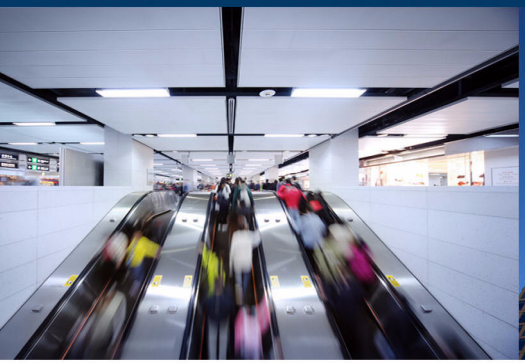
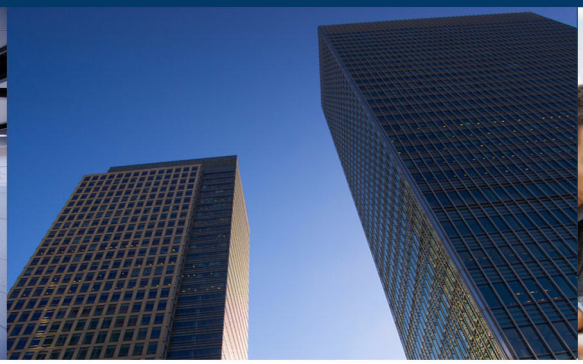
Edge™ v2
Device Management Guide

Products Covered

Edge™ v2

- MP-1035-CPE
- MP-1015-BS3
- MP-1025-BS3
- MP-1045-BS3
- MP-1055-BS3


Copyright

Trademarks

Edge™, Proxim® and the Proxim logo are the trademarks of Proxim Wireless Corporation. All other trademarks mentioned herein are the property of their respective owners.

Disclaimer

Proxim reserves the right to revise this publication and to make changes in content from time-to-time without obligation on the part of Proxim to provide notification of such revision or change. Proxim may make improvements or changes in the product(s) described in this guide at any time. When using these devices, basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons.

GPL License Note

Edge™ products include, in part, some free software that is developed by Free Software Foundation. A user is granted license to this software under the terms of either the GNU General Public License or GNU Lesser General Public License (See http://www.gnu.org/licenses/licenses.html). This license allows the user to freely copy, modify and redistribute this software and no other statement or documentation from us. To get a copy of this software, or for any other information, please contact our customer support team Telephone Support).

OpenSSL License Note

Edge™ products contains software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/) and that is subject to the following copyright and conditions:
Copyright (c) 1998-2016 The OpenSSL Project. All rights reserved.

The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to refer to, endorse, or promote the products or for any other purpose related to the products without prior written permission. For written permission, please contact openssl-core@openssl.org.
This software is provided by the OpenSSL Project “as is” and any expressed or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the OpenSSL Project or its contributors be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this software, even if advised of the possibility of such damage.

Edge™ v2 - Device Management Guide

Documentation Version: 2.0

P/N 765-00381, July 2022

Preface

About this Guide

This guide gives an overview of the device user interface and explains the step-by-step procedure to configure, manage and monitor the device by using Graphical User Interface.

Related Documents

For more information, please refer to the following additional documents available at Proxim support site http://support.proxim.com.

- **Quick Installation Guide (QIG)**: A quick reference guide that provides essential information for installing and configuring the device.
- **Software Configuration Guide:** A guide that provides software management information for Proxim devices.
- **Hardware Installation Guide**: A guide that provides a hardware overview and details about the installation procedures and hardware specifications.
- **CLI Guide**: A guide that provides essential information on how to configure, manage and monitor the device using the Command Line Interface.
- **Safety and Regulatory Guide**: A guide that provides essential information on the country specific safety and regulatory norms to be followed while installing the device.

Proxim recommends you to visit its support site http://support.proxim.com for regulatory information and latest product updates.

Management and Monitoring 1

1.1 Management and Monitoring

A Network Administrator can use the following interfaces to configure, manage and monitor the device.

- Proxim BlueConnect (Bluetooth)
- Graphical User Interface (GUI)
- Command Line Interface (CLI)
- Simple Network Management Protocol (SNMP)
- ProximVision® Advanced

For all the modes of operation (except Bluetooth), the IP address of the device should be configured. As each network is different, a suitable IP address on the network must be assigned to the device. This IP address helps to configure, manage and monitor the device by using GUI, SNMP, or Telnet/CLI.

For point-to-point and point-to-multipoint devices, the default IP Address is set to **static**. The pre-configured IP Address for BSU/End Point A is **169.254.128.132** and for SU/End Point B **169.254.128.131**.

You can assign **Static** or **Dynamic** IP address to the device. When you select Dynamic, the device obtains IP parameters automatically from Dynamic Host Configuration Protocol (DHCP) server during boot-up. If the device fails to obtain the IP address or there is no response from the DHCP server, the device falls back to the IP address 169.254.128.132. Select Static to manually configure IP parameters.

For IPv6 there are three modes; **Static**, **Dynamic,** and **Auto**.

By default, the device is set to **auto** mode. In this mode, the device uses Link-local IP Address created from Device MAC address by default. For Example: If DUT MAC is 04:f5:f4:00:11:05, then IPv6 Link-local IP address is fe80::6f5:f4ff:fe00:1105/64. The last 6 MAC address octets is used in Link-local.

1.1.1 Proxim BlueConnect

BuleConnect mobile app introduces remote management of a device or peripheral within a range of 15 meters using Bluetooth Low Energy (BLE) feature. The main purpose of this application is to enable the communication between a mobile device and any proxim device that supports BLE feature.

With BlueConnect app on your mobile device, you can:

- Retrieve data from nearby devices.
- Configure data to a nearby device.
- Monitor the link status of a device.
- Configure a device.
- Reset / reboot a device.

: Proxim BlueConnect is only applicable to Edge 1015 and 1025 series.

1.1.2 Graphical User Interface

GUI provides an easy way to configuration settings and retrieve network statistics from any computer on the network. You can access the GUI through either LAN device, a browser through an Internet connection, or through an Ethernet cable directly connected to your computer's Ethernet port.

For a secure communication between the device and the HTTP client, the device supports and maintains TLS 1.2 with a 256-bit encryption certificate. All communications are encrypted by using the server and the client-side certificate.

1.1.3 Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure, manage and monitor the device. The commands can be issued from the keyboard for real-time control, or from scripts that automate the configuration.

Access the CLI through the Ethernet interface by using a Telnet of SSH connection.

To login to the device:

- Verify that the computer has IP connectivity with the device (Ping 169.254.128.132),
- Use Telnet or SSH client (Telnet 169.254.128.132),
- Enter the username and password (By default, the username is **admin** for **Administrator** User, **monitor** for **Monitor** User and the password is **public** for both users).

To view the list of available commands, type Question Mark (?) at the command prompt.

For details on how to configure the device through CLI, refer to *Reference Guide* available on Proxim website at http://support.proxim.com.

: For devices with no serial port, the user can initialize, configure, manage and monitor the device through CLI commands via Telnet/SSH.

1.1.4 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is an application-layer protocol designed to facilitate the exchange of management information between the network devices. It is a part of the TCP/IP protocol and is most commonly used by the Network Administrators.

SNMP MIB (Management Information Base) is a collection of various network objects that you can access using a network-management protocol such as SNMP. The supported MIB files are available on Proxim website at http://support.proxim.com. You need to compile one or more of the MIBs into their SNMP program's database before you can manage the device by SNMP. You can open the MIB with any text editor, such as Microsoft Word, Notepad, or WordPad.

To access SNMP agent through MIB browser (for example NuDesign Pro 8.2) by using SNMP versions as V1, V2c, or V3, do the following:

- Select SNMP version.
- Provide device's IP address in the **Dest IP Address** box. The default IP address of the device is **169.254.128.132**.
- Provide the **Dest UDP Port**. By default, the port number is set to **161**.
- Provide the Read Community Password. By default, the password is **public**.
- Provide the Read/Write Community Password. By default, the password is **public**.

For details on how to configure the device through SNMP Interface, refer to *Reference Guide* available on Proxim website at http://support.proxim.com.

1.1.5 ProximVision® Advanced

ProximVision® Advanced is the state-of-the-art network management system to administer Proxim devices on the network.

ProximVision® Advanced offers the following network management and monitoring features:

- Network Management - Network Discovery, Geographical, and Logical Maps
- Fault Management - Event Logs and Alarms
- Performance Management - Statistics Collection and Analysis
- Security Management - User Provisioning

- Scheduled Bulk Operations and Task - Backup, Software Upgrade and Bulk SNMP Parameter Configuration
- Configuration Management - Device Configuration.

For details, refer to *ProximVision® Advanced Installation and Management Guide* available on Proxim website at http://support.proxim.com.

Proxim Blue Connect 2

: Proxim BlueConnect is only applicable to Edge 1015 and 1025 series.

2.1 Getting started

2.1.1 Downloading the app (For Android users)

To download BlueConnect app on your Android mobile device, do as follows:

1. Open **Google Play store** on your mobile and search for **"BlueConnect".**
2. Locate and select the app.
3. Tap **Install** to begin the download. The app will be installed automatically.
4. Tap on the **BlueConnect App** on your mobile to open it.

2.1.2 Downloading the app (For iphone (iOS) users)

To download BlueConnect app on your IOS mobile device, do as follows:

1. Open **App store** on your mobile and search for **"BlueConnect".**
2. Locate and select the app.
3. Tap **Install** to begin the download. The app will be installed automatically.
4. Tap on the **BlueConnect App** on your mobile to open it.

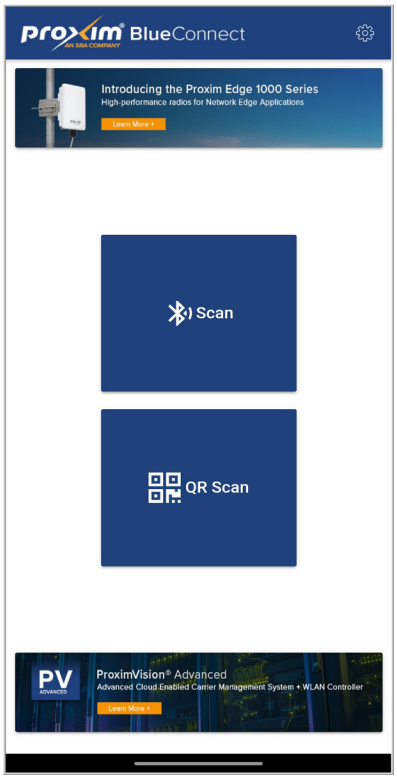
: Application will run on latest versions of Operating System given below:

Android device: *version 7 (Nougat), 8 (Oreo), 9 (Pie) and 10.*
Apple device: *iOS 10, 11, 12 and 13.*

Make sure to connect your mobile device to the internet (Mobile data / WiFi) before opening the application.

2.1.3 Home screen

Home screen displays two options - **Scan** and **QR Scan**. You can connect your mobile device to nearby Proxim devices with **Scan** option while the **QR Scan** is used to connect to a Proxim device by scanning its QR code. See figure below.



2.1.4 Settings

Change the language by selecting any of the following languages from the **Settings** option.

- English
- French
- Spanish
- Japanese
- Chinese

Tap **Settings** and select a language.

2.1.5 Connect to a device

Connect using scan feature

1. Tap **Scan** on the home screen**.** A pop-up appears on the screen asking permission to access the mobile location. Tap **Allow.**

2. A bluetooth permission pop-up appears on the screen. Tap **Yes** and then tap **OK** to turn **ON** buletooth. This will initiate the scanning process. After scanning, a screen appears as below showing the available Proxim devices.

3. Tap on a device from the scanned list that you want to connect with.
4. A pop-up with bluetooth pairing request appears on the screen. Enter the **PIN** and then tap **OK**. The default PIN is **123456**.
5. This may take upto few seconds to connect and load the data from the device. After loading the data successfully, the link status screen appears.

Connect using QR scan feature

1. Tap **QR Scan** on the home screen**.** A pop-up appears on the screen asking permission to take pictures and record videos. Tap **Allow**.
2. Point your phone's camera to the QR code on the device to capture it.
3. This may take upto few seconds to connect and load the data from the device. After successfully loading the data, the link status screen appears. See the Link status screen section below.

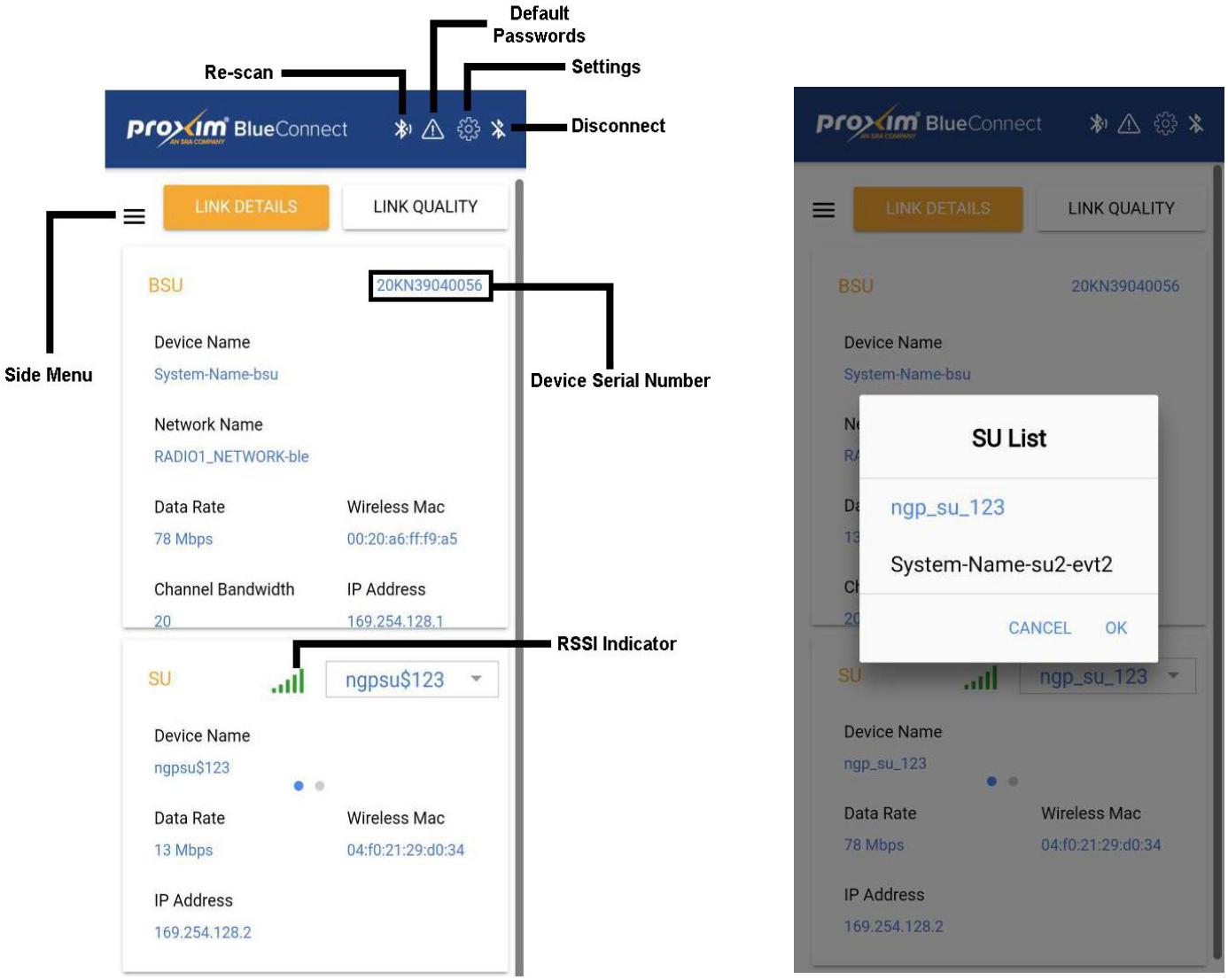
*If you see "**Please Wait Connecting...**" screen for longer than usual while trying to connect a device, go to your mobile bluetooth settings and then select "**Forget device**" option for that device ID. Perform re-scan in BlueConnect App to connect with the device.*

Make sure to connect only to BlueConnect app and disconnect all other bluetooth devices for better performance.

2.1.6 Link status screen

After you connect with a device, you can access the **Link Details** and **Link Quality** on the **Link Status Screen.** The link status screen contains the following features. See figure below.

- Default passwords
- Settings
- Disconnect
- Rescan
- Link details tab
- Link quality tab
- Side menu
- SU and BSU details
- RSSI indicator



A maximum of 8 devices can be paired with the mobile device. If you pair the 9th device, all the 8 devices will be un-paired automatically.

Allow all the app permission pop-up messages at first login after installing the BLE App.

2.1.7 Default passwords warning

The **"Default Passwords warning"** shows up if the connected device is still using default management passwords (BLE, WEB GUI, Telnet, SNMP)

2.1.8 Settings

Change the UI language by selecting a language from ***"Settings"*** . *The available languages are* ***English, Chinese, French, Japanese*** *and* ***Spanish.***

Tap ***Settings*** and then select a language from the list to apply it.

2.1.9 Disconnect

Disconnect from all the connected devices by tapping on **"Disconnect"** . This action will take you back to the home screen.

2.1.10 Rescan

Connect a new device without disconnecting the current device by tapping *on* **"Rescan"** . This will take you to the home screen, where you need to scan again for new devices to connect.

2.1.11 Link details

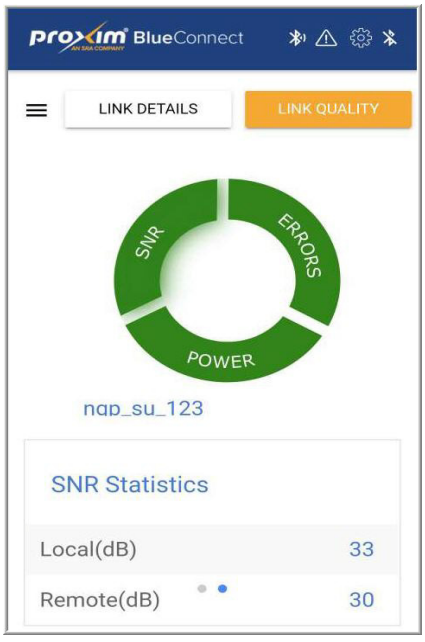
Link details tab displays the following information about **BSU / SU**.

- Device Name
- Device Serial Number
- Wireless MAC
- Data Rate
- IP Address
- Channel Bandwidth
- Network Name
- Device Serial Number

2.1.12 Link quality

Link quality tab displays the following information. See figure below.

- SNR
- Errors
- Power



:

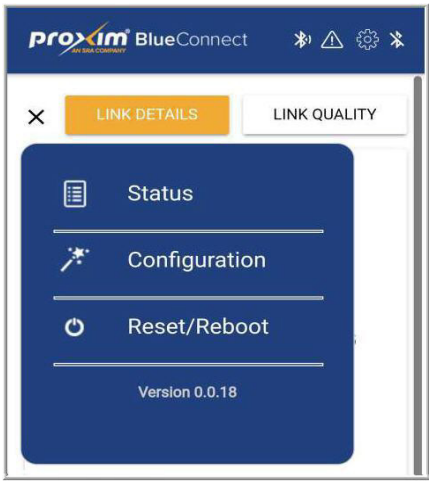
Link Quality displays the information only when the WORP link is established between BSU and SU. It shows empty values when the WORP link is not established.

When you connect to a BSU, the SU dropdown displays the available SU's for the user to select.

2.1.13 Side Menu

Side menu displays the following information. See figure below.

- Status
- Configuration
- Reset / Reboot



2.1.14 Status

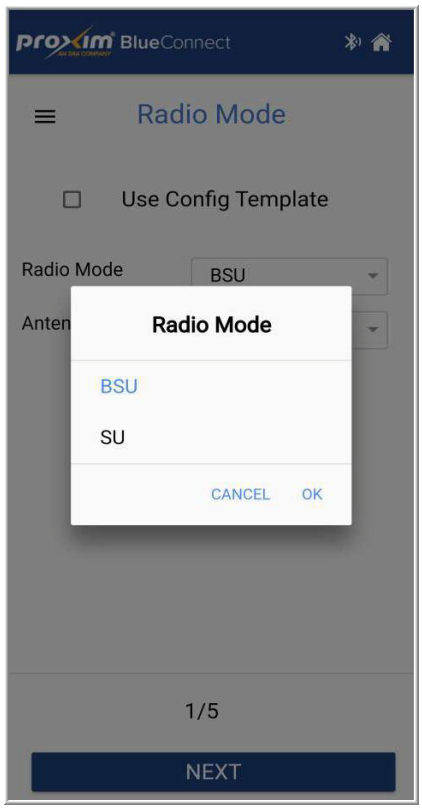
Check the Link Quality details by tapping on **Status**. This will take you to the **Link Status Screen**.

2.1.15 Configuration

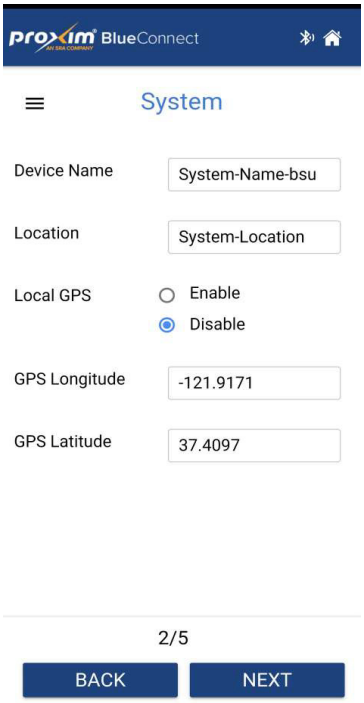
Tap ***Configuration*** and follow the step by step procedure to manage and monitor a device.

When the user taps ***Configuration***, the radio mode screen appears as below:

In the **Radio Mode** drop down, select BSU / SU, tap **OK** and then tap **Next.** *See figure below.*



The **System** screen appears as below.



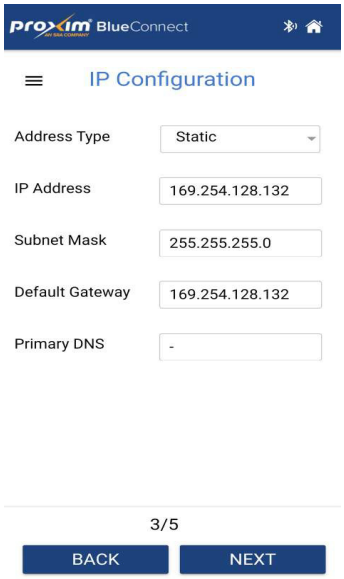
The system screen displays the ***Device Name***, ***Location*** and a provision to ***Enable / Disable*** the local GPS.

In the system screen, you can choose to either Enable the local GPS or disable it. Select **Enable** option if you want to get the GPS longitude and GPS latitude values of the mobile phone or tablet. Select **Disable** option to get the previously connected device parameters.

User can go to the previous screen by tapping on **Back** button.

Home and **"Rescan"** buttons are available at the top right hand corner of every screen in the configuration.

Configure the System screen and then tap ***Next***. The **IP Configuration** screen appears as shown below.



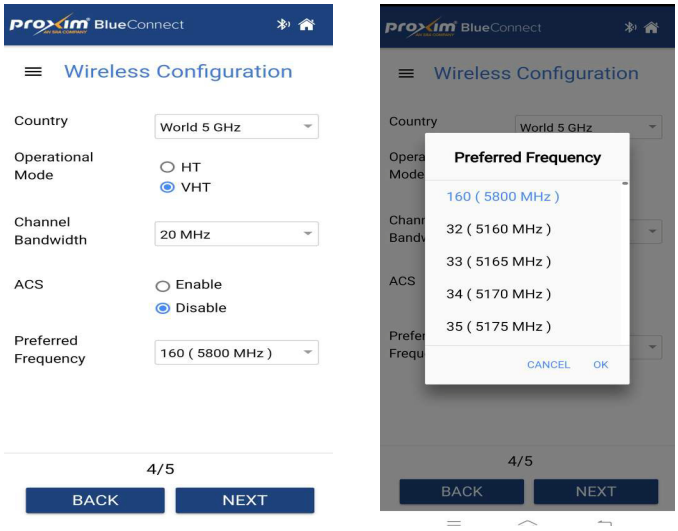
Enter the parameters such as **Address Type**, **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS.**

Address Type dropdown displays two options - ***Static*** and ***Dynamic***.

If you select **Static,** enter all the parameters such as **IP Address**, **Subnet Mask**, **Default Gateway** and **Primary DNS** manually.

If you select **Dynamic**, all required IP parameters will be retrieved by the device automatically. Tap ***NEXT*** *to continue.*

The **Wireless Configuration** screen appears as below.



Select **Country**, **Channel Bandwidth** and **Preferred Frequency**. Operational mode will be set to VHT by default.

Enable **Auto Channel Selection (ACS)** to fetch the channel automatically from the device.

Disable **ACS** if you want to select the preferred frequency from the drop down as shown in figure above and then tap **Next.**

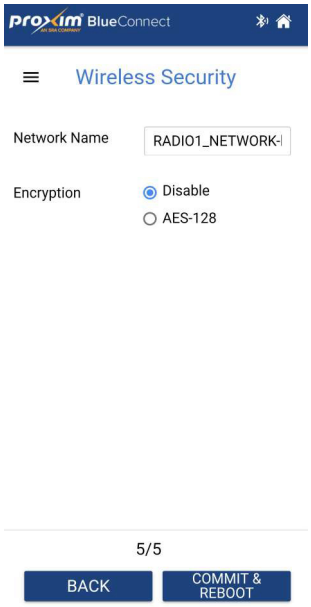
*When the user enables **ACS**, P**referred Frequency** option will not be visible.*

*Disable **ACS** option is available in SU mode.*

When the channel bandwidth is set to 80 MHz, only VHT option will be displayed in the operational mode.

When channel bandwidth is set to 20 or 40 MHz, both VHT and HT options are displayed in the operational mode.

Tap **Next.** The **Wireless Security** screen appears as shown below:



Enter the **Network Name** and select **AES 128** if you want encryption and tap ***Commit & Reboot*** *to apply the changes.*

*Encryption key length must be of **16 characters**.*

User can disable the Encryption if not required.

2.1.16 Reset/Reboot

Tap ***Reset / Reboot*** to apply the changes made.

Note: *After disconnecting the device from the application, you can connect the mobile app to the previously connected device directly after **Three** minutes by providing the pairing security key without scanning again.*

Accessing the Graphical User Interface 3

3.1 Accessing the Graphical User Interface

To access the Graphical User Interface (GUI), connect the device to a PC or a laptop and enter the default device IP address in the address bar (http://169.254.128.132). Alternatively, use ScanTool to access the device. See ScanTool for more details.

3.2 Logging In

Once the device connects to the network, the Windows Security page prompts the user to enter the username and the password.

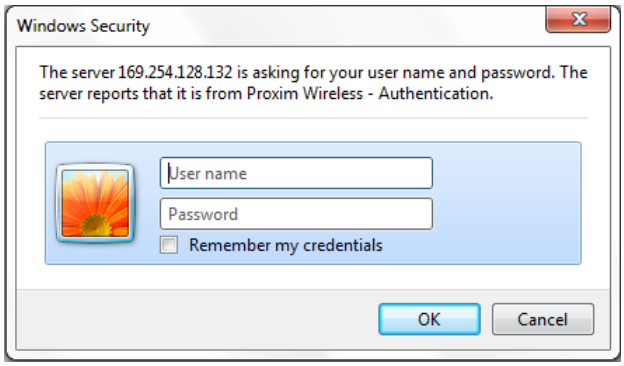


Figure 3-1 Login Screen

To login to the device:

1. Type a valid user name in the **Username** box. Based on the privilege level, three types of users are defined:
   - **Administrator:** Administrator user has access to all the features of the device. This user has the privilege to change his/her password and that of Monitor user. By default, the username is **admin**.
   - **Monitor**: Monitor user has only view access to all the features of the device and restricted from changing his/her password or run any of the test tools. However, this user is given the privilege to retrieve logs for debugging. By default, the username is **monitor**.
   - **Advanced**: Advanced user is identical to the administrator user, but has the privilege to change the advanced settings of the device. By default, the username is **advanced**.
2. Type the password in the **Password** box. By default, the password is **public** for all the users.

:

- *For security reasons, It is recommended to change the password after the first login. You can change the password from the Management tab in the GUI.*
- *Administrator and Advanced user share the same password; changing the administrator user password also changes the advanced user password.*

Graphical User Interface Overview 4

4.1 Graphical User Interface Overview

After logging in, the GUI title bar will display at the top of the browser screen, a navigation pane on the left, and a content pane in the center. The default page shown in the content pane is the **Setup Wizard** / **Summary**.

- **Home:** Click **Home** to return to the summary page which displays all the key performance parameters.
- **Commit:** Click **Commit** to save all changes made to the configuration parameters. Perform a device reboot after a successful Commit operation, if the reboot button blinks red.
- **Reboot:** Click **Reboot** for changes made in the configuration parameters to take effect. It is mandatory to save the changes before Reboot for changes to take effect.
- **ADVANCED**: Click Advanced to navigate from Simplified to Detailed Graphical User Interface.
- **BASIC GUI**: Click Basic GUI to navigate back to the simplified Graphical User Interface when logged as Admin.
- When directly logged in as Advanced user, it is not possible to switch between GUIs.
- **TEMPORARY COMMIT**: It allows users to temporarily apply the configuration on the device without storing it to database (or Flash memory). On reboot the device will reset to the old configuration. To retain the configuration use Commit. This feature is used to test configuration. In case of a link failure, the watchdog reboots the devices and comes-up with old configuration.

The Graphical User Interface refreshes every 5 seconds to update the page with most recent information.

:

- *Recommended browser is Firefox latest version.*
- *Recommended screen resolution is 1280 x 960 or higher.*

This feature is available only in Advanced User login.

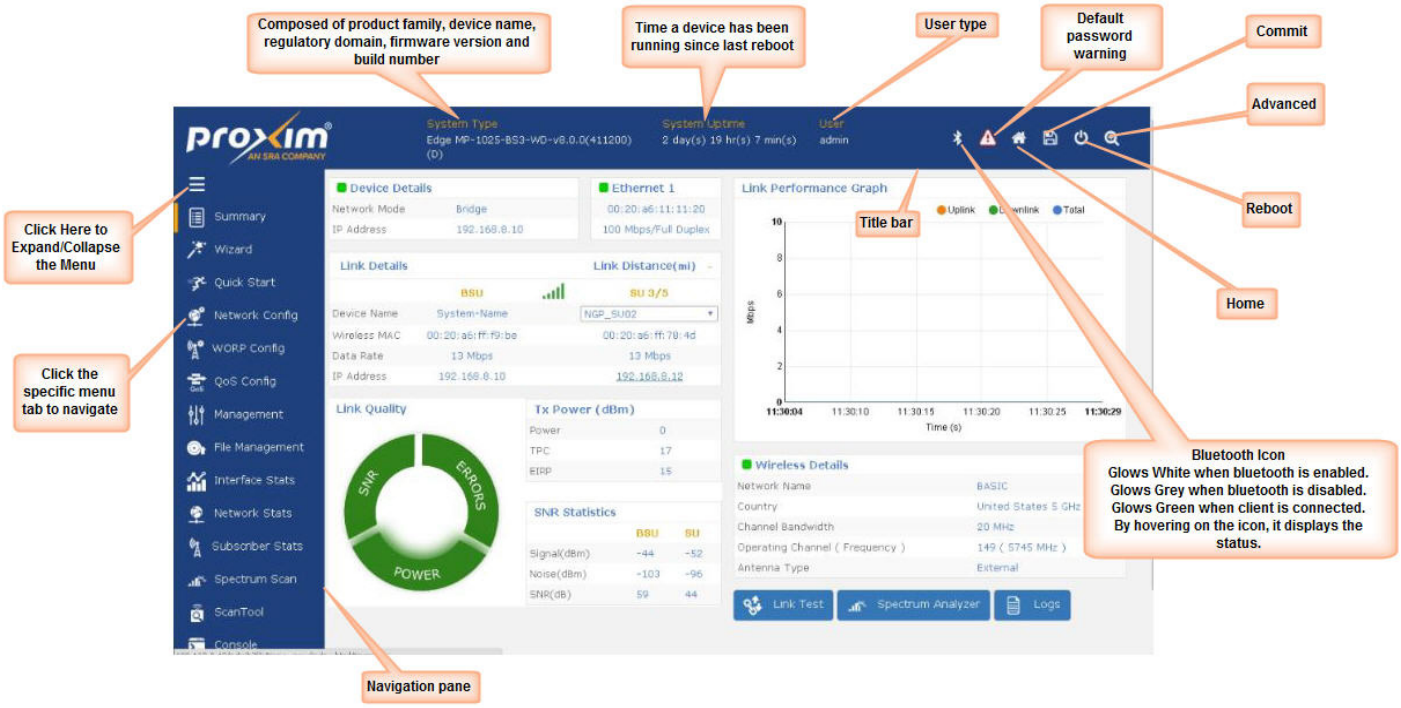


Figure 4-1 Graphical User Interface Overview (Admin User)

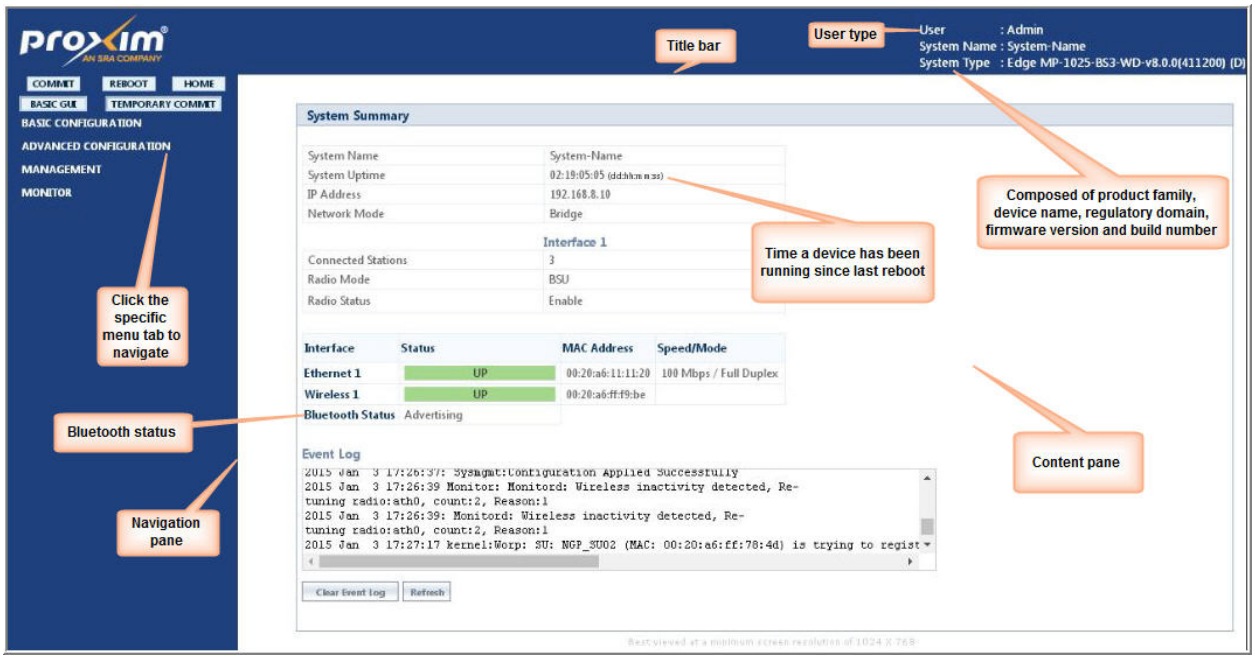


Figure 4-2 Graphical User Interface Overview (Advanced User)

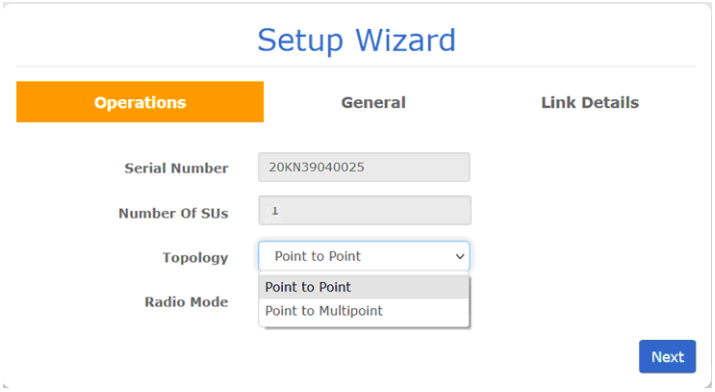
4.2 Device Setup

Wizard guides the user through initial device installation.

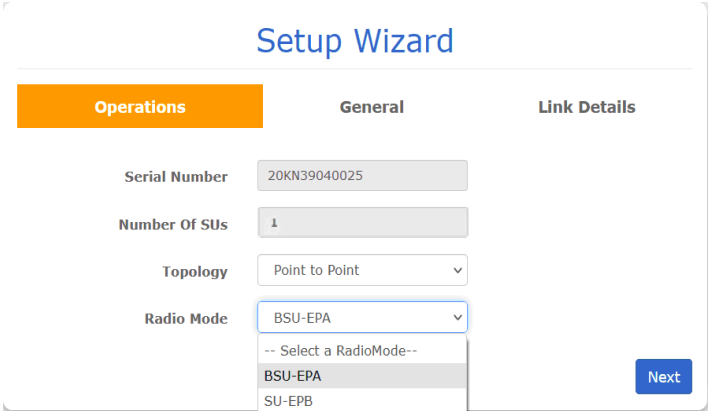
Click **Wizard** on the left navigation pane, configure the parameters and click **Finish** to complete the setup and reboot the device automatically. Parameters modified in the Wizard applies to the existing configuration of the device.

Wizard **Operations** tab controls device operational modes:

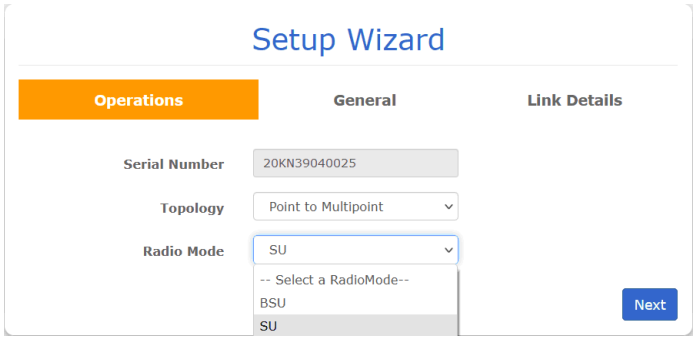
1. **Topology** option allows to select if the device will be used in **Point to Point** or **Point to Multipoint** mode. Default Topology setting is **Point to Point** mode.



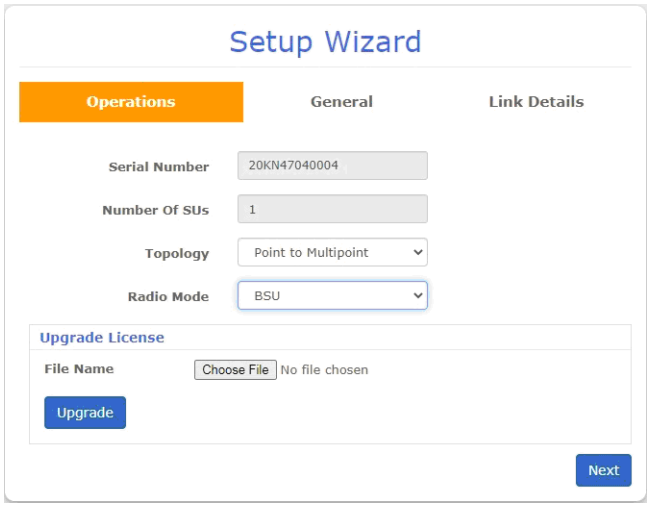
2. **Radio Mode** option allows to select if the device will be used in **Base Station (BSU)** or **Subscriber (SU)** mode. Default Radio Mode will be **BSU-EPA** if topology is set to Point to Point.

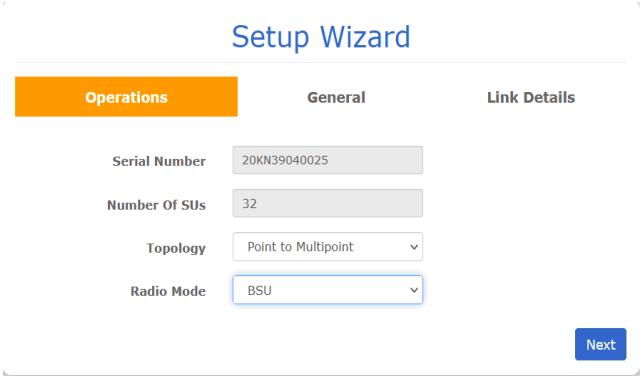


Default Radio Mode will be **SU** if topology is set to **Point to Multipoint**.



3. If Point to Multipoint / BSU are selected and supported Number of SUs is 1, then Upgrade License menu is displayed. It is then recommended to upgrade license to increase Number of SUs to 32.

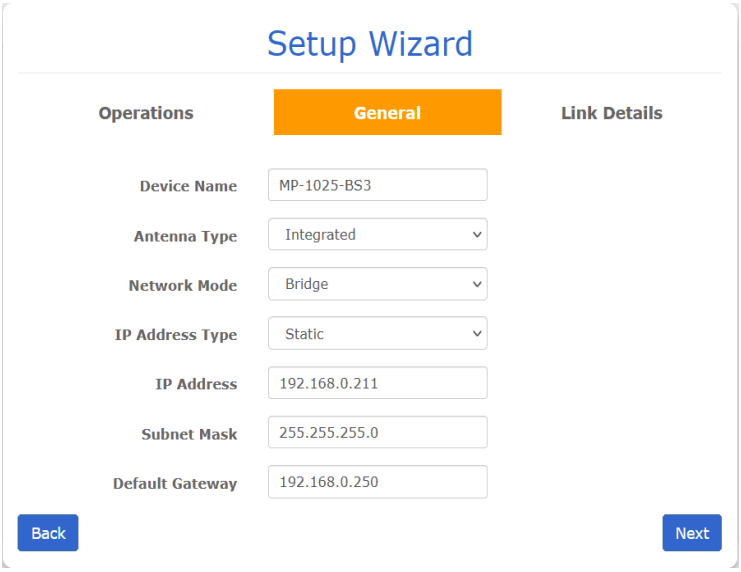




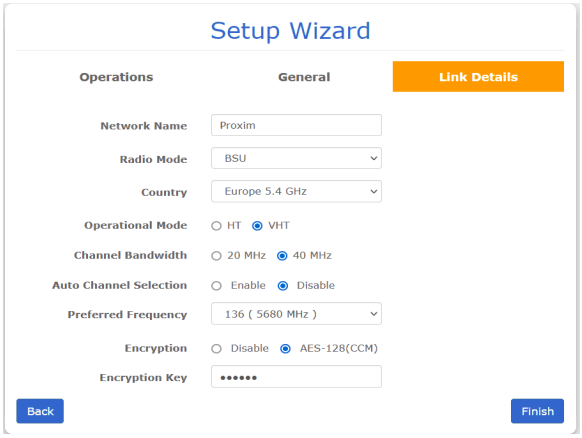
:

- *For Point to Point link, set one BS3 in "BSU-EPA" radio mode and one BS3 in "SU-EPB" radio mode*
- *For Point to Multipoint, set one BS3 in "BSU" radio mode (license upgrade is needed to support up to 32 subscribers), and set every other BS3 and CPE in "SU" radio mode*
- *Existing Edge v1 MP-10x5-BS3 supports all options: Point to Point / Point to Multipoint topologies and BSU / SU modes. It keeps Number of SUs to 32*
- *Existing Edge v1 MP-10x5-CPE only supports Point to Multipoint topology and SU mode.*
- *Existing Edge v1 QB-10x5-EPR only supports Point to Point topology and End Point A / End Point B modes.*

Wizard **General** tab controls device general configuration such as Device Name, Bridge or Routing mode and IP parameters.

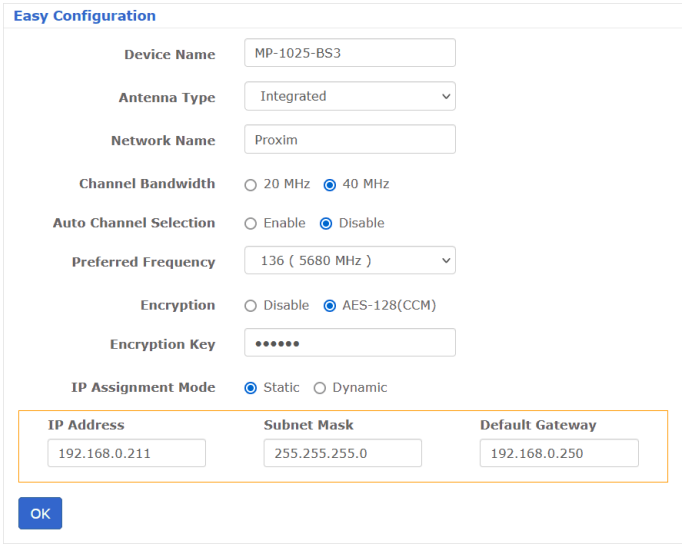


Wizard **Link Details** tab control device wireless configuration required to establish a link such as Radio Mode, Frequency information and Security encryption.



Quick Start consists of frequently used parameters. It is applicable only to selective devices.

Click Quick Start on the left navigation pane, configure the parameters and click **OK**. Perform **Commit** and **Reboot** to complete the setup.



4.3 File Management

File management tab enables the user to:

- Upgrade the firmware (Download the latest version of firmware from http://support.proxim.com).
- Retrieve Configuration in order to push it to similar devices.
- Retrieve Event Log, Debug log or License Info.
- Upgrade the certificate (SSL certificate).
- Upgrade the certificate authority.
- Reset the device to its factory default state.

:

- *For firmware upgrade, the file name should not contain any spaces or special characters.*
- *It is recommended to use Internet Explorer 8 or later.*
- *It is recommended not to navigate away from the screen, while firmware update is in progress.*
- *When the device is operational with factory default settings, there is no Config file present and hence it cannot be retrieved.*

For more details, refer File Management.

Device Management 5

5.1 System

To configure the device information, Inventory Management information, and licensed information navigate to **Management > System**.

5.1.1 Information

In the Information tab, view and configure the following parameters:

- **System Up-Time:** The operational time of the device since its last reboot.
- **System Description:** It includes device name, current version of the firmware and current build number.
- **System Name:** The name assigned to the device.
- **Contact:** The contact information (Email id, Phone number, and Location) of the person administering the device.
- **Email:** The email address of the person administering the device.
- **Phone Number:** The phone number of the person administering the device.
- **Location:** The location where the device is installed.
- **GPS Longitude/Latitude/Altitude:** The longitude/latitude/altitude at which the device is installed.
- **GPS Status Enable/Disable:** Enable this option to get the GPS status of the device.

:

- *Connect an External "Passive GPS Antenna" to get the GPS data after enabling the GPS status.*
- *GPS connectivity is only available with Edge 1015 and 1025 series.*

After configuring the required parameters, click **OK** and then **Commit.**

5.1.2 Inventory Management

To view the system inventory information, navigate to **Management** > **System Inventory Management**.

By default, the components information is auto-generated by the device. This information is standard and is used only for reference purpose. Click **Refresh**, to view the updated System Inventory Management information.

: Wireless Card 2 is applicable only to dual-radio device.

5.1.3 License Information

Licensing is one of the most important components in an enterprise class device which typically has a feature-based pricing model. Licensing allows the device to operate as intended and prevents anyone tempering with the device feature set.

To view the license information, navigate to **Management** > **System** > **License Information**.

: The Input bandwidth indicates the data received on the wireless interface and output bandwidth indicates the data sent on the wireless interface.

5.1.3.1 License Upgrade Procedure

To obtain additional bandwidth (larger channel, higher throughput limit), upgrade the License by retrieving the license information (**License Info** file with **.lic** extension) from the device. For more details, refer Retrieve from Device.

Contact Proxim Sales Representative to purchase a license upgrade. Refer to the Technical Note available on http://www.proxim.com/support to generate a unique license file for your device.

Upgrade the bandwidth using the license file (**.bin** extension) generated above. For more details, refer Upgrade License.

5.2 File Management

The **File Management** tab enables you to upgrade the firmware and configuration files on the device, and retrieve configuration and log files from the device through Hypertext Transfer Protocol (HTTP) and Trivial File Transfer Protocol (TFTP).

- HTTP file transfer can be performed with or without TLS enabled. HTTP file transfer with TLS requires enabling Secure Management and Transport Layer Security. HTTP file transfer by using TLS may take extra time.
- TFTP file transfer requires that a TFTP server is running and configured to point to the desired directory path to copy the retrieved file.

5.2.1 Upgrade Firmware

You can update the device with the latest firmware either through HTTP or TFTP.

:

- *Make sure that the firmware which you are loading is compatible with the device which is being upgraded.*
- *It is recommended to upgrade the remote end(s) first and then the local end.*

5.2.1.1 Update Firmware Using HTTP

To update the firmware using HTTP, follow the below steps:

1. Navigate to **Management** > **File Management** > **Upgrade Firmware > HTTP.**
2. In the HTTP screen, click **Choose File** to select the updated firmware file from the desired location.
3. To upgrade the device with new firmware click **Upgrade** and then reboot the device.

: The file name should not contain any spaces or special characters.

5.2.1.2 Update Firmware Using TFTP

To update the firmware using TFTP, follow the below steps:

1. Navigate to **Management** > **File Management** > **Upgrade Firmware > TFTP**.
2. Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.
3. Enter the name of the latest firmware file (including the file extension) in the **File Name** box that you want to load onto the device.
4. To upgrade the device with new firmware, click **Upgrade** and then reboot the device after the firmware upgrade has finished or click **Upgrade & Reboot**.

:

- *After upgrading the device with the new firmware, reboot the device; otherwise, the device will continue to run with the old firmware.*
- *It is recommended not to navigate away from the screen while the upgrade is in progress.*

5.2.2 Upgrade Configuration

You can upgrade the device with the latest configuration files either through HTTP or TFTP.

Configuration files retrieved from the other similar/compatible devices contains configuration parameters for the device apart from the below unique parameters that are excluded while retrieving the profile.

Unique parameters that are excluded during the creation of configuration profile are applied with the corresponding values of the target device.

These parameters will be set to default values until they are configured on the new device.

 : *Make sure that you retrieve the configuration file from a device of the same SKU.*

5.2.2.1 Configuration File Encryption

For enhanced security, the Edge will encrypt the configuration file.

In order to change the encryption key used by the devices, users need to configure the new encryption key in PV Advanced and apply the same on all the managed devices. For more details about modifying the encryption key refer **PV Advanced Installation & Management Guide** available at http://support.proxim.com.

NOTE:

- *Encryption key modification from PV Advanced is only supported for devices with Controller Mode enabled.*
- *When a device is reset to factory default, the user configured encryption key is also reset to factory default value. The device is updated with the Encryption Key configured in PV Advanced only after re-associating with it.*
- *Either unencrypted or encrypted config/config profile files can be loaded into devices if the device type and firmware version support configuration file encryption.*
- *Encrypted config/config profile files cannot be loaded into devices if the device type or firmware version do not support configuration file encryption.*
- *For devices supporting configuration file encryption, the config/config profile files retrieved from one device cannot be loaded into another device if different encryption keys are configured in the two devices.*

5.2.2.2 Upgrade Configuration Using HTTP

To update the device with configuration files using HTTP, follow the below steps:

1. Navigate to **Management** > **File Management** > **Upgrade Configuration > HTTP**.
2. In the HTTP screen, click **Choose File** to locate the configuration file. Select a Binary Configuration file or a Config Profile file. Make sure that the file name does not contain any space or special characters.
3. If you are upgrading the device with Binary Configuration file, click **Upgrade** and then **Reboot** the device.
4. If you are upgrading the device with Config Profile file, click **Upgrade** and then **Reboot** the device. If the configuration profile is not compatible, the device will rollback to its old configuration on reboot.
5. If you are upgrading the device with a Text-Based Configuration file, click **Upgrade** and then **Load**. Alternatively, click **Upgrade & Load** to perform both operations in a single step.

5.2.2.3 Update Configuration Using TFTP

To update the device with configuration files using TFTP, follow the below steps:

1. Navigate to **Management** > **File Management** > **Upgrade Configuration > TFTP**.
2. You can update the device with three types of configuration files; **Binary**, **Text Based**, and **Config Profile**. Select any one then;
   - Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.

- Enter the name of the Binary, Text Based, or Config Profile file (including the file extension) in the **File Name** box that you want to download onto the device.

3. If you are upgrading the device with Binary Configuration file, click **Upgrade** and then **Reboot** the device or click **Upgrade & Reboot**.
4. If you are upgrading the device with Text Based Configuration file, click **Upload** and then click **Apply**.
5. If you are upgrading the device with Config profile file, click **Upload** and then **Reboot** the device or click **Apply & Reboot**.

: It is recommended not to navigate away from the screen while the update is in progress.

5.2.3 Upgrade License

You can upgrade the license file on the device either through HTTP or TFTP. Refer License Upgrade Procedure for more details.

5.2.3.1 Upgrade License via HTTP

To upgrade the license using HTTP, do the following:

1. Navigate to **Management > File Management > Upgrade License > HTTP.**
2. Click **Choose File** to locate the license upgrade (**.bin**) file.
3. Click **Upgrade** and then **Reboot** the device.

5.2.3.2 Upgrade License via TFTP

To upgrade the license file using TFTP Server, do the following:

1. Navigate to **Management** > **File Management** > **Upgrade License > TFTP**.
2. Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.
3. Enter the name of the file (including the file extension) in the **File Name** box that you want to load onto the device.
4. Click **Upgrade** and then **Reboot** the device.

- *You can upgrade the license through CLI/Web Interface/SNMP.*
- *After license upgrade and device reboot, reconfigure the WORP input and output bandwidth limits as per the newly licensed values.*

5.2.4 Upgrade Certificate

Device comes with default SSL certificate. User can upload his own SSL certificate for secured access.

To upgrade the SSL certificate, follow the below steps:

1. Navigate to **File Management** > **Upgrade Certificate.**
2. Click **Browse** to locate the SSL certificate (**.pem**) file.
3. Click **Upgrade/Upgrade & Reboot** to update the SSL certificate on the device.
4. On Reboot, the device will be upgraded with the new SSL certificate.

Click **Reset** to make the device to come back to its default SSL certificate.

*: SSL certificate will be in **.pem** file format.*

5.2.5 Upgrade Certificate Authority

To upgrade the certificate authority, follow the below steps:

1. Navigate to **File Management** > **Upgrade Certificate Authority.**
2. Click **Browse** to locate the certificate authority file.
3. Click **Upgrade/Upgrade & Reboot** to update the certificate authority file on the device.
4. On Reboot, the device will be upgraded with the new certificate authority.

Click **Remove** to erase the certificate authority file from the device.

5.2.6 Retrieve from Device

The **Retrieve From Device** tab allows you to retrieve logs, config files, and license info from the device either through HTTP or TFTP.

5.2.6.1 Retrieve from Device using HTTP

To retrieve Configuration files, Event Logs and Text Based Templates from the device using HTTP, follow the below steps:

1. Navigate to **Management** > **File Management** > **Retrieve from Device > HTTP**.
2. Select the file type from the drop-down that you want to retrieve from the device. The file types may vary depending on your device. The File Types are; **Config, Event Log, Debug Log, Config Profile, License Info.**

   The Config Profile is used for replicating the configuration of a master device on to other similar devices by excluding **the below unique parameters**

   a. System Information (System Name, System Coordinates (GPS Longitude, GPS Latitude, GPS Altitude) and Contact Information (Contact, Email, Phone Number and Location))
   b. IP Configuration (Address Type (Static/Dynamic), Subnet Mask, Default Gateway IP Address and DNS)
   c. Ethernet Configuration (Speed & Tx Mode, Admin Status and Auto Shutdown)
   d. Wireless Configuration (Preferred Channel, Preferred Channel Offset and Antenna Gain)

   By default, System Information and IP Configuration parameters are excluded.

   After excluding the unique parameters, click **Create Profile** and then **Retrieve**. When you load the retrieved configuration profile file on target devices, the target devices will come up with the configuration of the master device except the excluded parameters. The excluded parameters are retained as configured on the target device.
3. Click **Retrieve** and right-click the **Download** link and select **Save Target As** or **Save Link As** to save the file to the desired location.


:

- *Config Profile is applicable only to the compatible devices.*
- *When the device is running with default factory settings, Binary Configuration file is not available and cannot be retrieved.*

5.2.6.2 Retrieve from Device using TFTP

To retrieve Configuration files, Event Logs and Text Based Templates from the device using TFTP, follow the below steps:

1. Navigate to **Management** > **File Management** > **Retrieve from Device > TFTP**.
2. Based on the IP mode, configure either IPv4 or IPv6 address as TFTP Server address.
3. Enter the name of the file (including the file extension) in the **File Name** box that you want to retrieve from the device.

4. Select the file type from the drop-down that you want to retrieve from the device. The file types may vary depending on your device. The File Types are; **Config, Event Log, Debug Log, Config Profile, License Info.**

   The Config Profile is used for replicating the configuration of a master device on to other similar devices by excluding the unique parameters like System information, IP configuration, Ethernet configuration, Wireless configuration based on the selection. By default, System Information and IP Configuration parameters are excluded.

   After excluding the unique parameters, click **Create Profile** and then **Retrieve**. When you load the retrieved configuration profile file on target devices, the target devices will come up with the configuration of the master device except the excluded parameters. The excluded parameters are retained as configured on the target device.

5. Click **Retrieve.** You can find the retrieved file in the TFTP Server folder.

- *Config Profile is applicable only to the compatible devices.*
- *When the device is running with default factory settings, Binary Configuration file is not available and cannot be retrieved.*
- *You can retrieve Event Logs only when they are generated by the device.*

5.3 Services

The **Services** feature allows you to configure the management interface (HTTP/HTTPS, Telnet/SSH, SNMP, and Logs) parameters that prevent unauthorized access to the device.

5.3.1 HTTP/HTTPS

Navigate to **Management** > **Services > HTTP/HTTPS** and configure the following parameters:

- **Admin Password or Monitor Password:** By default, the password is set to **public**.

  : Special characters like - = \ " ' ? / space are not allowed in the password.

- **HTTP:** When **enabled**, it allows the user to access the device through web interface. To prevent access to the device through web interface, select **Disable**.
- **HTTP Port:** It represents the HTTP port to manage the device through Web Interface. Preferred value is 80.
- **HTTPS:** When **enabled**, it allows the user to access the device through a web interface over secure socket Layer (HTTPS). To prevent access to the device through HTTPS, select **Disable**. The password configuration for HTTPS is same as configured for HTTP.
- **LANGUAGE:** It allows the user to select the following languages from the drop down as shown in the figure below:
  - English
  - Spanish
  - French

Select the desired language from the drop down and click **OK**, **Commit** and then **Reboot.**

: Multi-Language support is added for Admin User based on the following SKUs:

- **US SKU – English only**
- **WD SKU – User can opt between English, French and Spanish for UI**
- **CN SKU – Chinese only.**
- **JP SKU – Japanese only.**

The SKUs that are converted for WD using console commands will have the same options as WD SKU.

- **HIGH SECURE MODE:** It represents the Transport Layer Security, TLS 1.2 to provide secured communication.
- User can Enable the high secure mode to apply TLS 1.2 only. To Enable the high secure mode, Select **Enable** and then click **OK**.
- User can Disable the high secure mode to apply TLS 1.0 / 1.1 or 1.2 as per the browser settings. To Disable the high secure mode, select **Disable** and then click **OK.**

5.3.2 Telnet/SSH

In the Web Interface, navigate to **Management** > **Services > Telnet/SSH** and configure the following parameters:

- **Admin Password or Monitor Password:** By default, the password is set to **public**.

  
  : Special characters like - = \ " ' ? / space are not allowed in the password.

- **Telnet:** When **enabled**, it allows the user to access the device via telnet interface. To prevent access to the device through Telnet, select **Disable**.
- **Telnet Port:** The number of the port on the telnet interface. Preferred value is 23.
- **Telnet Sessions:** The number of Telnet sessions which controls the number of active Telnet connections.
- **SSH:** When **enabled**, it allows the user to access the device via SSH Interface. To prevent access to the device through SSH, select **Disable**.
- **SSH Port:** It represents the port to manage the device using Secure Shell. Preferred value is 22. Telnet Port and SSH Port should not be same.
- **SSH Sessions:** It represents the number of SSH sessions which controls the number of active SSH connections.

  
  : A total number of 3 CLI sessions are allowed therefore the sum of Telnet and SSH sessions cannot be more than 3. For example, when you configure the number of Telnet sessions as 2, the number of SSH sessions value can only be either 0 or 1.

After configuring the required parameters, click **OK**, **Commit** and then **Reboot.**

5.3.3 SNMP

Navigate to **Management** > **Services > SNMP** and configure the following parameters:

- **SNMP:** When **enabled**, it allows the user to access the device through SNMP Interface. To prevent access to the device through SNMP, select **Disable.**

  
  : Any change in the SNMP status will affect the Network Management System access.

- **Version:** The supported SNMP versions are **SNMPv1-v2c** and **SNMPv3**.
  - If you select the SNMP version as **SNMPv1-v2c**, configure the following parameters**:**
    - **Read Password:** It represents the read-only community string used in SNMP Protocol. It is sent along with each SNMP GET / WALK / GETNEXT / GETBULK request to allow or deny access to the device. This password should be same as read password set in the NMS or MIB browser. The default password is **public**.
    - **Read/Write Password:** It represents the read-only community string used in SNMP Protocol. It is sent along with each SNMP GET / WALK / GETNEXT / SET request to allow or deny access to the device. This password should be same as read-write password set in the NMS or MIB browser. The default password is **public**.
  - If you select the SNMP version as **SNMPv3**, configure the following parameters:
    - **Security Level:** The supported security levels for the device are **AuthNoPriv** and **AuthPriv**. Select AuthNoPriv for Extensible Authentication or AuthPriv for both Authentication and Privacy (Encryption).

- **Priv Protocol:** It represents the type of privacy (or encryption) protocol. Select the encryption standard as either AES-128 (Advanced Encryption Standard) or DES (Data Encryption Standard).
- **Priv Password:** It represents the pass key for the selected Privacy protocol. The default password is **public123**.
- **Auth Protocol:** It is a type of Authentication protocol. Select the encryption standard as either SHA (Secure Hash Algorithm) or MD5 (Message-Digest algorithm).
- **Auth Password:** It represents the pass key for the selected Authentication protocol. The default password is **public123**.

: Special characters like - = \ " ' ? / space are not allowed in the password.

- *Priv Protocol and Pric Password are applicable only when the security level is set to AuthPriv.*

After configuring the required parameters, click **OK**, **Commit** and then **Reboot.**

5.3.3.1 SNMP Trap Host Table

The SNMP Trap Host table allows you to add a maximum of 5 Trap server's IP address to which the SNMP traps will be delivered. By default, the SNMP traps are delivered to 169.254.128.133.

: You cannot delete the default SNMP Trap Host Table entry.

Add a new Entry or Edit existing entry in the SNMP Trap Host Table

To add new entries to the SNMP Trap Host Table, click **Add** and configure the following parameters:

- **IP Address**: Based on the IP mode, enter the IPv4 or IPv6 address of the Trap server to which SNMP traps will be delivered.
- **Comment**: Type comments, if any.
- **Entry Status**: Select the entry status as either **Enable** or **Disable**. If enabled, the device will send SNMP traps to the authenticated Trap Server.
- **Password:** Type the password to authenticate the Trap Server.

The following special characters are not allowed in the password:

-, =, \, ", ', ?, /, and space (Applicable only to SNMP v1-v2c.).

After configuring the required parameters, click **Add** and then **Commit**.

You can also edit the desired SNMP Trap Host Table existing entries.

- *IPv6 address should be the global IP address and not the link-local IP address.*
- Password is applicable to SNMP v1, SNMP v2c.

5.3.4 Logs

The device supports two types of log mechanisms:

1. **Event Log**: On the basis of configured event log priority, you can record and use all the log messages for analysis. These messages will remain in the system until cleared by the user.
2. **Syslog**: Syslog is similar to Event log except that it gets cleared on device reboot.

To configure Event log and Syslog priority, navigate to **Management** > **Services** > **Logs** and configure the following parameters:

- **Event Log Priority:** Configure the event log priority such as; **Emergency**, **Alert**, **Critical**, **Error**, **Warning**, **Notice**, **Info**, **Debug**. Please note that the priorities are listed in the order of their severity, where **Emergency** takes the highest severity and **Debug** the lowest. When the log priority is configured as high, all the logs with low priority are also logged. For example, if **Event Log Priority** is set to **Notice**, then the device will log all logs with priorities Notice, Warning, Error, Critical, Alert and Emergency.
- **System Status:** By default, **Syslog Status** is enabled and default priority is **Critical**.
- **Syslog Priority:** Configuration is same as Event Log Priority.

After configuring the required parameters, click **OK** and then **Commit**.

5.3.4.1 Configure a Remote Syslog host

Configure a syslog host (server) in order to forward syslog messages to it.

Follow the following steps to configure a remote syslog host:

1. Click **Add** in the **Logs** screen.
2. **IP Address**: Based on the IP mode, enter IPv4 or IPv6 address of the Syslog host.
3. **Host Port**: The port on which the Syslog host listens to the log messages sent by the device.
4. **Comments**: Types comments, if any.
5. Click **Add**.

For some reason, if the configured syslog host parameters are changed then you can edit it directly in the **Syslog Host Table** entry.

After doing the necessary changes, click **OK** followed by **Commit**.

:

- *You can configure only one syslog host.*
- *IPv6 address should be the global IP address and not the link-local IP address.*
- *Configure the correct port number on which the Syslog host is running. Choice of port number must be in line with the standards for port number assignments defined by Internet Assigned Numbers Authority (IANA).*

5.4 Simple Network Time Protocol (SNTP)

SNTP allows you to synchronize the date and time of the device with the configured time servers.

The SNTP Client when enabled on the device(s), sends an NTP (Network Time Protocol) request to the configured time servers. Upon receiving the NTP response, it decodes the response and sets the received date and time on the device after adjusting the time zone and day light saving.

In case the time servers are not available, then users also have the option to manually set the date and time on the device.

To synchronize the device time with time servers or manually set the time, navigate to **Management > SNTP** and configure the following parameters

- **Enable SNTP Status:** Select this parameter to enable SNTP Client on the device. If enabled, the SNTP Client tries to synchronize the device time with the configured time servers.
- **Primary Server IP Address / Domain Name or Secondary Server IP Address / Domain Name:** Enter the host name, or the IP address based on IP modes (**IPv4 only** or **IPv4 and IPv6**) of the primary or secondary SNTP time server. The SNTP Client tries to synchronize device time with the configured primary server time. If the primary server is not reachable, then SNTP client tries to synchronize device time with the secondary server time.

- *When you configure a host name instead of an IP address, ensure that you configure DNS server IP on the device.*
- *IPv6 address should be the global IP address and not the link-local IP address.*

- **Time Zone:** Configure the time zone from the available list. This configured time zone is considered before setting the time, received from the time servers, on the device.
- **Day Light Saving Time:** Configure the Day Light Saving time from the available list. This configured Day Light Saving time is considered before setting the time, received from the time servers, on the device.
- **ReSync Interval:** Once the time is synchronized, the SNTP Client tries to resynchronize with the time servers after every set time interval.
- **Sync Status:** Specifies the SNTP Client sync status when it tries to ReSync again with the time servers. The status is as follows:
  - **Disabled**: The SNTP client will not synchronize the time with the time servers and displays the status as Disabled.
  - **Synchronizing**: The SNTP client is in the process of synchronizing time with the time servers.
  - **Synchronized**: The SNTP client has synchronized time with the time servers.
- **Current Date/Time:** Specifies the system current date and time.
  - If SNTP is not enabled, the current date and time are automatically generated by the local system.
  - If SNTP is enabled, it displays the time, that the device has obtained from the SNTP server.
- **Manual Time Configuration:** Manually set the time if the SNTP Client is disabled on the device or the time servers are not available on the network.

- *Reboot does not retain Manual Time Configuration. Set the time again after every reboot.*
- *It is recommended to periodically check and adjust the time since the device may lag behind the actual time with the Manual Time Configuration.*

Click **OK** and **Commit**, to save the configured parameters.

5.5 Access Control

The **Access Control** tab enables you to control the device management access through specified host(s). You can specify a maximum of five hosts to control device management access.

Navigate to **Management > Access Control**, configure the parameters. Click **OK** and **Reboot** the device, if you have changed the values in the Access Control Table.

Add or Edit Host(s) to Management Access Control Table

To add a host to the Management Access Control Table, do the following:

1. Click **Add** in the **Management Access Control** screen.
2. **IP Address**: Based on the IP mode, configure either IPv4 or IPv6 address of the host that controls the device management access.
3. **Entry Status:** By default, the entry status is enabled meaning which the specified host can control the device management access. Edit the status to **Disable**, if you do not want the host to control the device management access.
4. Click **Add**.

You can also edit the desired host entries.

After configuration, click **OK, Commit** and then **Reboot**.

- *If MAC ACL is enabled, configure at least one entry in the Management Access Table with the IP address of the PC or the management station to manage the device.*
- *To manage the Access Point device, you can add a maximum of five system IP addresses.*
- *You can add new entries only when the Access Table status is enabled.*

5.6 Reset to Factory

The 'Reset to Factory' feature allows you to reset the device to factory default state. When this operation is performed, the device will reboot automatically and operates with the factory default configuration.

To reset the device to factory defaults, navigate to **Management** > **Reset To Factory**. Click **OK** for the device to restart with the default factory configuration.

5.7 Interface Statistics

To view the Ethernet and Wireless Interface Statistics, navigate to **Monitor > Interface Statistics** and click **Ethernet 1 or Wireless 1** depending on the interfaces supported by your device. The following points explains the Statistics parameters:

- **MTU:** The Maximum Transmission Unit of the data packet received or sent on the Ethernet or wireless interface. Ethernet MTU size varies from 1500 to 9216 bytes depending on the MTU configuration.
  Wireless MTU size varies from 350 to 11000 bytes depending on the WORP MTU (or Super Frame) configuration.
- **MAC Address:** The MAC address at the Ethernet or wireless protocol layer.
- **Operational Status:** The current operational state of the Ethernet or wireless interface.
- **In Octets:** The total number of octets received on the Ethernet or wireless interface.
- **In Unicast Packets:** The number of subnetwork-unicast packets delivered to the higher level protocol.
- **In Non-unicast Packets:** The number of non-unicast subnetwork packets delivered to the higher level protocol.
- **In Errors:** The number of inbound packets which contains errors and which are restricted from delivery.
- **Out Octets:** The total number of octets transmitted out from the Ethernet or wireless interface.
- **Out Packets:** The total number of packets requested by the higher level protocol and transmitted to the non-unicast address.
- **Out Discards:** The number of error-free outbound packets, chosen to be discarded to prevent them from being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
- **Out Errors:** The number of outbound packets that are not transmitted because of errors.
- **Retunes:** The number of times the radio is re-tuned for better performance of the device.
- **Max Tx Power:** It indicates the maximum power that the radio can radiate.
- **SNR Statistics:** It represents the ratio of signal strength to noise at the antenna ports.
  - **Antenna:** It specifies the antenna ports which varies depending on the product.
  - **Status:** It specifies the status of the antenna ports. **ON/OFF** indicates that the antenna port is either enable or disable.
- **Rx Error Details**
  - **Decrypt Errors:** It is applicable only if security is enabled. It indicates the number of received packets that failed to decrypt.
  - **CRC Errors:** It is the number of received packets with invalid CRC.
  - **PHY Errors:** It is the total Rx PHY Errors. It indicates the interference in the wireless medium.

Click **Refresh**, to view the updated Ethernet or Wireless statistics. Click **Clear**, to delete the Ethernet or Wireless statistics.

5.8 System

System tab enables you to view LED/RSSI Display.

: System is applicable only to point-to-point and point-to-multipoint devices.

5.8.1 RSSI LED Behavior

When the link establishes, the Received Signal Strength Indicator (RSSI) LED's on the scaling mask glows. RSSI LED's indicates the strength of the link signal. A Higher number of glowing LED's better is the signal strength. To view RSSI, navigate to **Monitor > System**.

The output from the LED's during antenna alignment is variable according to SNR ranges and number of glowing LED's as given in the following table.

SNR Range	Number of Glowing LED
1 – 12	1
13– 18	2
19 – 24	3
25 – 30	4
More the 30	5

: If the configured wireless MAC address of the SU is registered with the BSU, then the LEDs will glow based on the RSSI value else all the 5 LEDs will blink.

5.9 Logs

Logs provides a record of events on the system.

- For administrator and monitor user, go to the **Summary** page and click the **Logs** link to open the system log information.
- For advanced user, go to the **Monitor > Logs** section and click **Event Log/Debug Log/Syslog.**

Click **Refresh** to update the display with the most recent information. Click **Clear** to clear the system logs. The messages are cleared and moved to the backup file leaving the log files empty.

5.9.1 Event Log

Event Logs track all the events that occur during the operation of the device and display the time the event occurred, event type, and the name of the event, error, or any event message. Based on the priority, the event details are logged and can be used for any reference or troubleshooting.

The maximum size of the event log file is 65 KB. If the file size exceeds 65 KB, then all the log messages are moved to a backup file and only the recent 100 lines are displayed in the log file. When the size of the log file exceeds again then it overwrites the backup file.

:

- *The recent event logs are stored in the flash memory.*
- *Log messages can be stored in the log file approximately up to 6 days with logging interval of 5 minutes.*
- *The current and the backed up event logs are stored in the flash memory and can be retrieved even after device reboot.*

5.9.2 Debug Log

Debug Log helps you to debug issues related to important features of the device. Currently, this feature supports only DDRS and DFS. This feature helps the engineering team analyze the issues and provide a faster solution. This feature should be used only in consultation with the Proxim Customer Support team. Once logging is enabled, the Debug Log file can be retrieved via HTTP or TFTP.

To enable Debug Log, navigate to **Monitor > Logs > Debug Log**.

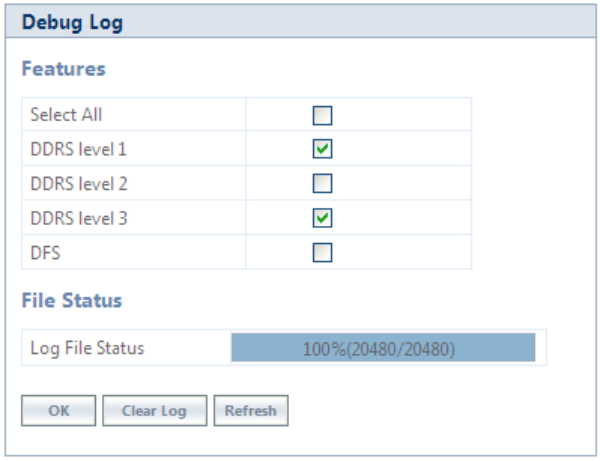


Figure 5-1 Debug Log

Features: Select the appropriate features to be logged. The available features are **Select All, DDRS Level 1, DDRS Level 2, DDRS Level 3** and **DFS**.

File Status: It displays the current size of the Debug Log file.

After selecting the parameters, click **OK**.

To delete the **Debug Log**, click **Clear Log**. To get the updated status of the **Debug Log** File, click **Refresh.**

: Debug log is applicable only to point-to-point and point-to-multipoint devices.

5.9.3 Syslog

When you enable the **Syslog** Status in a device, the Syslog Log Section displays all the Syslog events generated by the device. Syslog messages will be shown based on the configured Log and Priority levels.

-

Tools 6

6.1 ScanTool

Proxim ScanTool is a software utility that runs on Microsoft Windows machine.

By using ScanTool, a user can,

- Scan Proxim devices connected to the local network
- Obtain device IP address
- Modify device IP Configuration parameters (IP Address, Address Type, Gateway, etc)
- Launch the device Graphical User Interface.

:

- *ScanTool v5.1 scans devices based on IPv4 or IPv6 address.*
- *IPv6 is supported only by ScanTool v3.0.1 and higher versions.*
- *Network Adapter in ScanTool supports up to 16 virtual or real interfaces.*
- *Disable Windows Firewall (or add an exception) for ScanTool to function or to detect the radio.*

6.1.1 Initializing the device by using ScanTool

To scan and locate the devices on a network by using ScanTool, do the following:

1. Power on, or reset the device.
2. To download Proxim ScanTool, log on to Proxim support site at http://support.proxim.com and search for ScanTool with (Answer ID 1735). Upon successful download, double-click the icon to start the ScanTool.
3. If there are more than one network adapter installed on the computer, then the user will be prompted to select the ethernet adapter for scanning Proxim devices. Select an adapter and click **OK**.

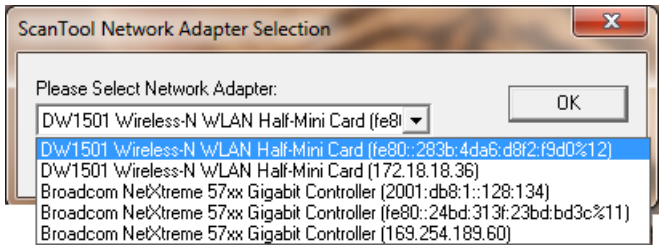


Figure 6-1 ScanTool Network Adapter Selection

4. The following **Scan List** screen appears, which displays all devices that are connected to the selected adapter.

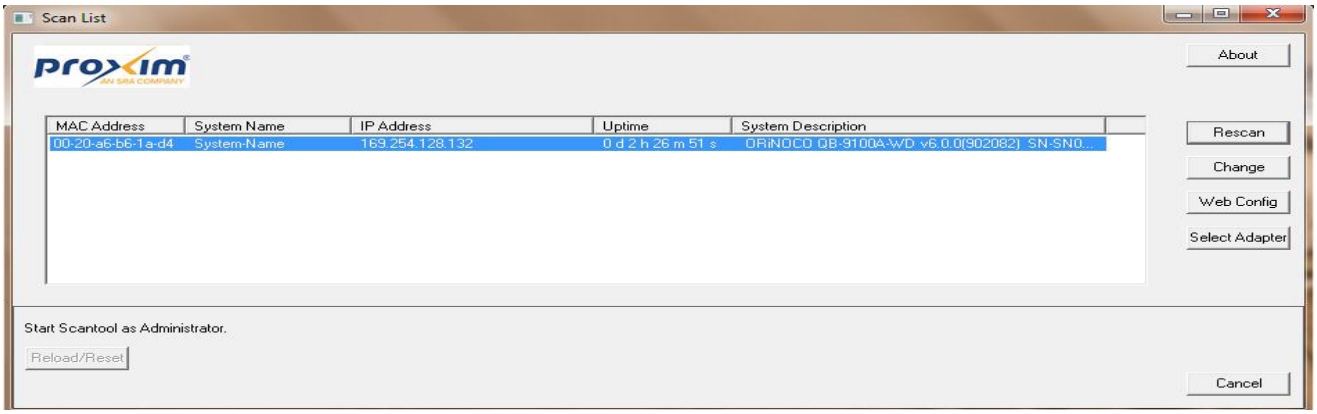


Figure 6-2 Scan List - Scanned Devices

This screen contains MAC Address, System Name, IP Address, Uptime, and System Description (comprises of device description, firmware version, serial number, and bootloader version).

5. Click **Select Adapter**, to change adapter settings.
6. From the list, identify and select the MAC address of the device that needs to be initialized, and click **Web Config** to log on to the Graphical User Interface.

*: If the device does not appear in the Scan List, click **Rescan** in the **Scan List** screen. If the device still does not appear in the list, see Troubleshooting. Note that after rebooting the device, it may take up to five minutes for the device to appear in the Scan List.*

6.1.2 Modifying the IP Address of the Device using ScanTool

To modify the IP address of a device using ScanTool, select the device from the scan list and click **Change**. A **Change** screen appears as shown in the following figure.

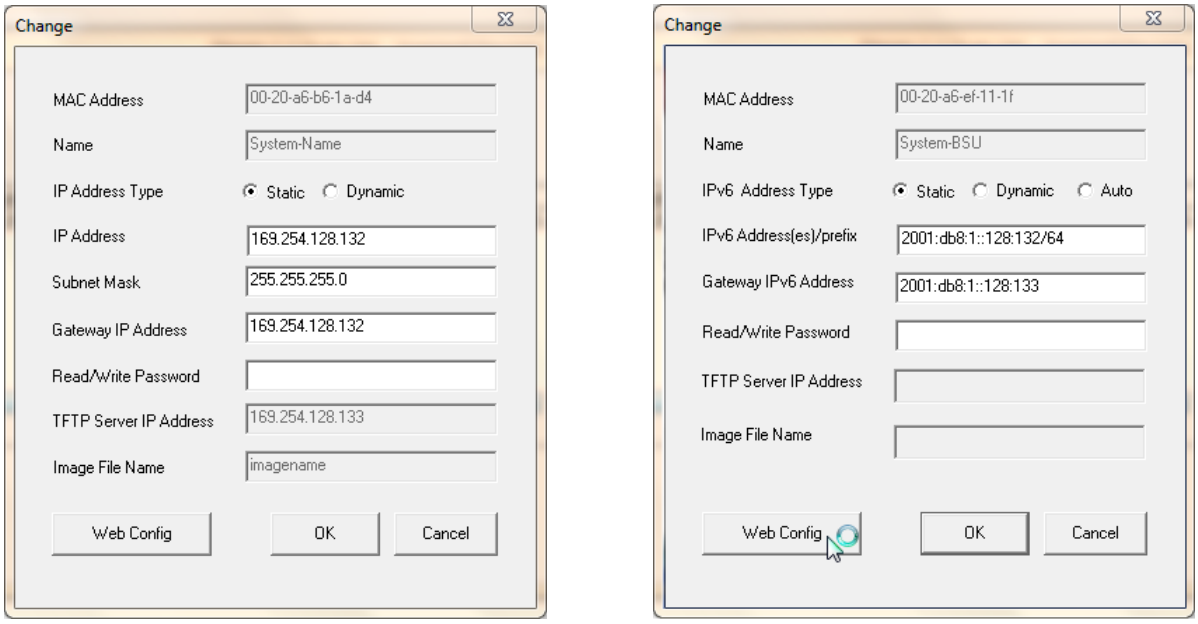


Figure 6-3 Modifying Device IP Address (IPv4 and IPv6)

The system automatically populates the **MAC Address**, **System Name**, **TFTP Server IP Address** and **Image File Name** of the device.

Assigning the IP Address

1. Select the **IP Address Type** as **static/dynamic** for IPv4 and as **static/dynamic/auto** for IPv6.
   - **Static**: When set to static, the **IP Address**, **Subnet Mask**, and the **Gateway IP Address** of the device can be manually changed.
   - **Dynamic**: When set to dynamic, the **IP Address**, **Subnet Mask**, and the **Gateway IP Address** is dynamically generated by the DHCP server.
   - **Auto**: When set to auto, the IPv6 address is calculated by the device using the router advertisement messages.
2. Enter the SNMP Read/Write password in the **Read/Write Password** box. By default, it is **public**.
3. Click **OK** to save the details. The device automatically reboots.

To log on to the Graphical User Interface, click **Web Configuration**. For details, refer Logging In.

6.2 Channel Planning and Link Tools

The tools required to monitor the device by using Graphical User Interface are as following:

- Spectrum Analyzer
- Radio Link Test Tool

6.2.1 Spectrum Analyzer

The Spectrum Analyzer actively scans the spectrum to report on interference sources that may impact link performance. This tool is not a replacement for the commercial Spectrum Analyzers as this is only intended to help with channel selection and diagnose performance issues.

This tool helps to scan the user configured bandwidth to identify the other devices operating on different channels. The analyzer will also display the frequencies and the level of signal is detected.

:

- ***When the Spectrum Analyzer starts, the wireless link, if established, is terminated and re-established after the scan is completed.***
- ***As the wireless link is down during spectrum analysis, the remote device cannot be accessed. Hence, if Spectrum Analyzer is started on a remote device, the results will not be available until spectrum scan is completed and wireless link gets re-established.***

To scan the configured frequency domain, do the following:

- For admin and monitor user, go to the **Summary** page and click the **Spectrum Analyzer** link or go to the **Spectrum Scan** tab on the left navigation pane.
- For advanced user, navigate to **Monitor > Tools** section and click the **Spectrum Analyzer.**

The following screen appears:

Figure 6-4 Spectrum Analyzer (Admin and Monitor User)

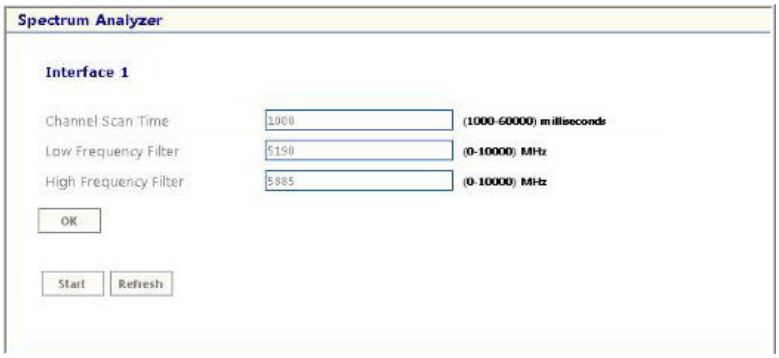


Figure 6-5 Spectrum Analyzer

For single radio devices, no tabs are displayed at the top of the screen for admin user and for spectrum analyzer advanced user, only **Interface 1** tab will be displayed.

Spectrum Analyzer consists of the following:

- **Channel Scan Time**: Enter the time (ranging from 1000 to 60000 milliseconds) to scan each channel.
- **Low Frequency Filter & High Frequency Filter**: Enter the start and stop frequency filter values to limit the number of channels to scan.

Click **OK** and then click **Start** to continuously scan all the available channels within the vicinity of the device.

The Spectrum Analyzer plots the channel utilization and Avg. SNR for each channel. Channel utilization is calculated as ratio of counter values (Medium found free) / (Medium Tested for Free) and Avg. SNR is calculated as ratio of (Sum of RSSI values of frames received) / (Number of Frames received). The newest data shows up on the right and scrolls to the left over time. The user can scroll through the graph for the specific values of each parameter at that specified place.

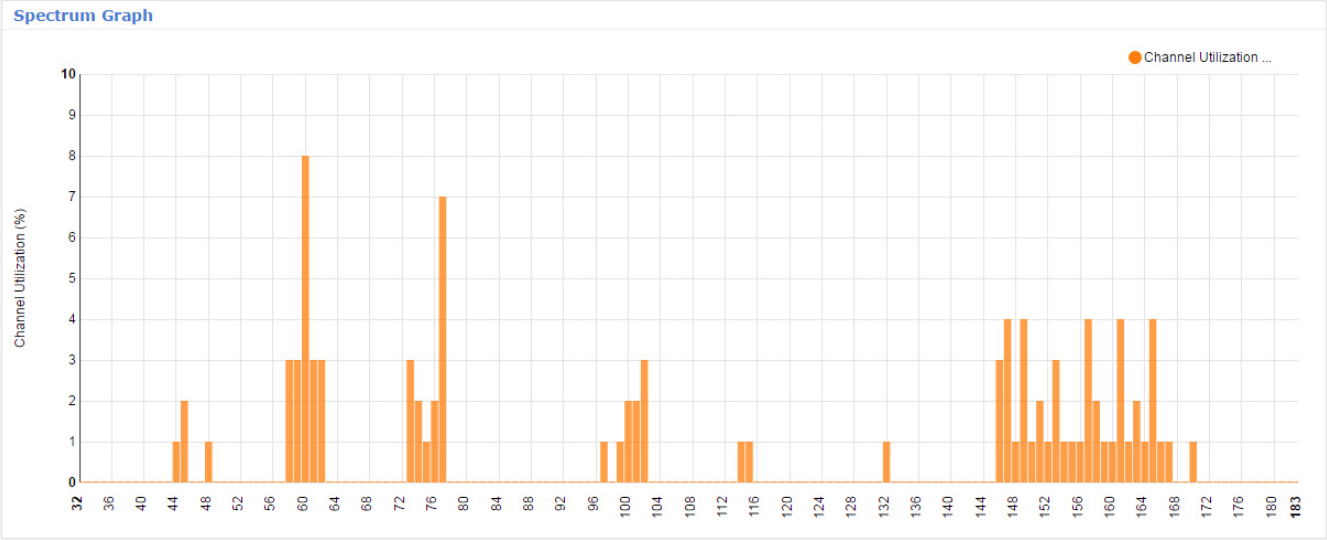


Figure 6-6 Spectrum Graph (Admin and Monitor User)

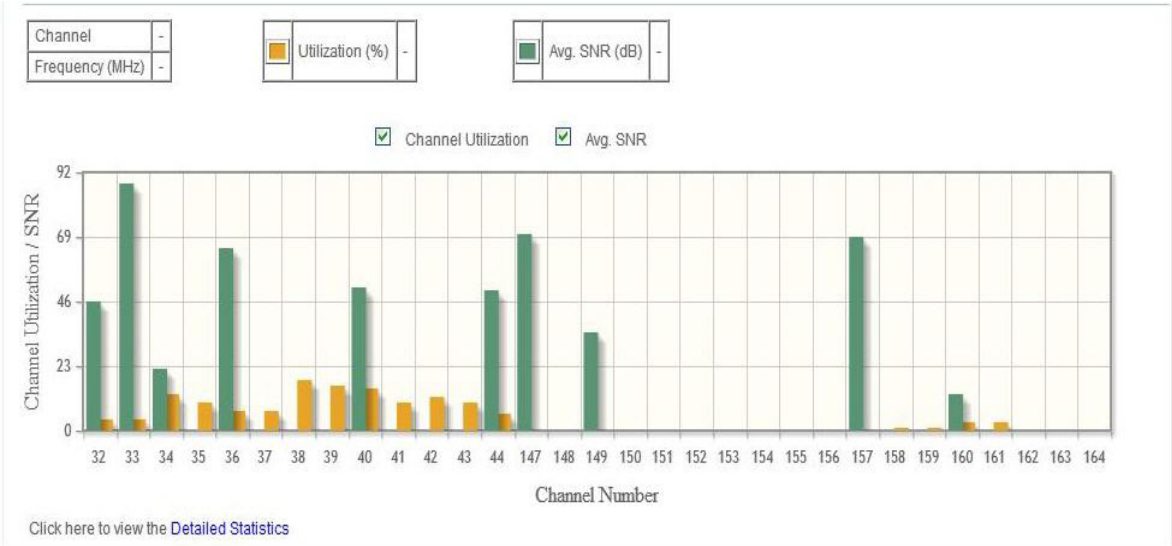
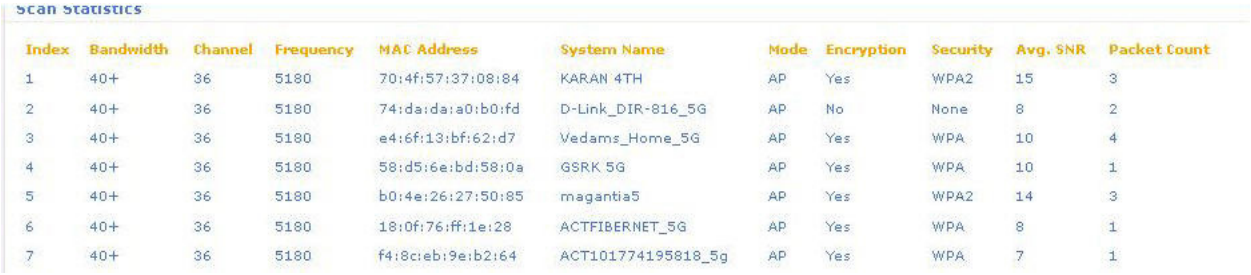


Figure 6-7 Spectrum Graph (Advanced User)

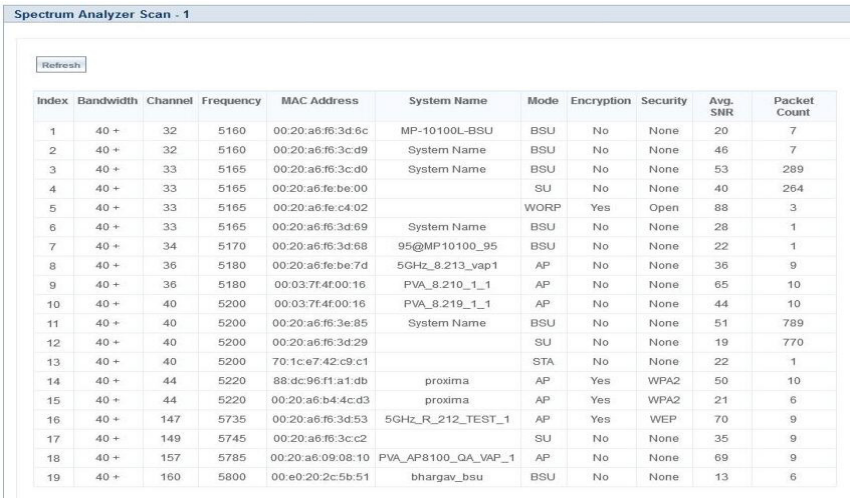
Spectrum Analyzer displays the detected device information such as Bandwidth, Channel number, Frequency, MAC Address, System Name, Mode (End Point A, AP, SU, STA), Encryption, Security, Avg. SNR, and Packet count.



Scan Statistics

Index	Bandwidth	Channel	Frequency	MAC Address	System Name	Mode	Encryption	Security	Avg. SNR	Packet Count
1	40+	36	5180	70:4f:57:37:08:84	KARAN 4TH	AP	Yes	WPA2	15	3
2	40+	36	5180	74:da:da:a0:b0:fd	D-Link_DIR-816_5G	AP	No	None	8	2
3	40+	36	5180	e4:6f:13:bf:62:d7	Vedams_Home_5G	AP	Yes	WPA	10	4
4	40+	36	5180	58:d5:6e:bd:58:0a	GSRK 5G	AP	Yes	WPA	10	1
5	40+	36	5180	b0:4e:26:27:50:85	magantia5	AP	Yes	WPA2	14	3
6	40+	36	5180	18:0f:76:ff:1e:28	ACTFIBERNET_5G	AP	Yes	WPA	8	1
7	40+	36	5180	f4:8c:eb:9e:b2:64	ACT101774195818_5g	AP	Yes	WPA	7	1

Figure 6-8 Spectrum Analyzer - Scan Statistics (Admin and Monitor User)



Spectrum Analyzer Scan - 1

Refresh

Index	Bandwidth	Channel	Frequency	MAC Address	System Name	Mode	Encryption	Security	Avg. SNR	Packet Count
1	40 +	32	5160	00:20:a6:f6:3d:6c	MP-10100L-BSU	BSU	No	None	20	7
2	40 +	32	5160	00:20:a6:f6:3c:d9	System Name	BSU	No	None	46	7
3	40 +	33	5165	00:20:a6:f6:3c:d0	System Name	BSU	No	None	53	289
4	40 +	33	5165	00:20:a6:fe:be:00		SU	No	None	40	264
5	40 +	33	5165	00:20:a6:fe:c4:02		WORP	Yes	Open	88	3
6	40 +	33	5165	00:20:a6:f6:3d:69	System Name	BSU	No	None	28	1
7	40 +	34	5170	00:20:a6:f6:3d:68	95@MP10100_95	BSU	No	None	22	1
8	40 +	36	5180	00:20:a6:fe:be:7d	5GHz_8.213_vap1	AP	No	None	36	9
9	40 +	36	5180	00:03:7f:4f:00:16	PVA_8.210_1_1	AP	No	None	65	10
10	40 +	40	5200	00:03:7f:4f:00:16	PVA_8.219_1_1	AP	No	None	44	10
11	40 +	40	5200	00:20:a6:f6:3e:85	System Name	BSU	No	None	51	789
12	40 +	40	5200	00:20:a6:f6:3d:29		SU	No	None	19	770
13	40 +	40	5200	70:1c:e7:42:c9:c1		STA	No	None	22	1
14	40 +	44	5220	88:dc:96:f1:a1:db	proxima	AP	Yes	WPA2	50	10
15	40 +	44	5220	00:20:a6:b4:4c:d3	proxima	AP	Yes	WPA2	21	6
16	40 +	147	5735	00:20:a6:f6:3d:53	5GHz_R_212_TEST_1	AP	Yes	WEP	70	9
17	40 +	149	5745	00:20:a6:f6:3c:c2		SU	No	None	35	9
18	40 +	157	5785	00:20:a6:09:08:10	PVA_AP8100_QA_VAP_1	AP	No	None	69	9
19	40 +	160	5800	00:e0:20:2c:5b:51	bhargav_bsu	BSU	No	None	13	6

Figure 6-9 Spectrum Analyzer - Scan Statistics (Advanced User)

The device information displayed in **Advance** Scanning mode are described and tabulated below.

Parameter	Description
Bandwidth	This parameter displays Bandwidth of the detected device.
Channel Number	This parameter displays the channel number on which the detected device is operating.
Frequency	This parameter displays the frequency in which the device is detected.
MAC Address	This parameter displays the MAC Address of the detected device.
System Name	This parameter displays either the Device Name or the SSID of the detected device.
Mode	This parameter displays the Mode of the detected device. • **BSU**: Base Station Unit • **SU**: Subscriber Unit • **AP**: Access Point • **STA**: Station
Encryption	This parameter indicates whether encryption is enabled on the detected device.
SNR	This parameter displays the Average Signal-to-Noise Ratio (SNR) value of the detected device in the scanned channel.

Parameter	Description
Packet Count	This parameter displays the Packet Count for the detected device.

- *Only an Admin / Advanced user can use Spectrum Analyzer to scan the spectrum. However, the Monitor user can only view the last scanned results.*
- *The total duration of scan depends on the number of channels available and channel scan time.*
- *While scanning, Spectrum Analyzer does not consider channel offset.*
- *Spectrum Analyzer detects only 802.11 modulated signals.*
- *A minor variation in Spectrum Analyzer results can be expected due to the following reasons: variation in the radio properties between various device models and Satellite Density Configuration.*
- *The frequencies are scanned based on the configured Scan Bandwidth slice starting from the lower edge of the frequency filter, and displays the results captured at that particular instance.*

6.2.2 Radio Link Test Tool

When there is a performance issue in the network, it is necessary to identify if the issue is related to wireless link or due to any network parameters. Using the Radio Link Test (RLT) tool, you can measure and diagnose the performance issues in the wireless link.

At MAC level, this tool internally generates traffic between the two radios, monitors the traffic, and generates a test report. This test report helps to analyze the performance of the wireless link and other related issues, such as, interference, lower throughput, and wireless errors.

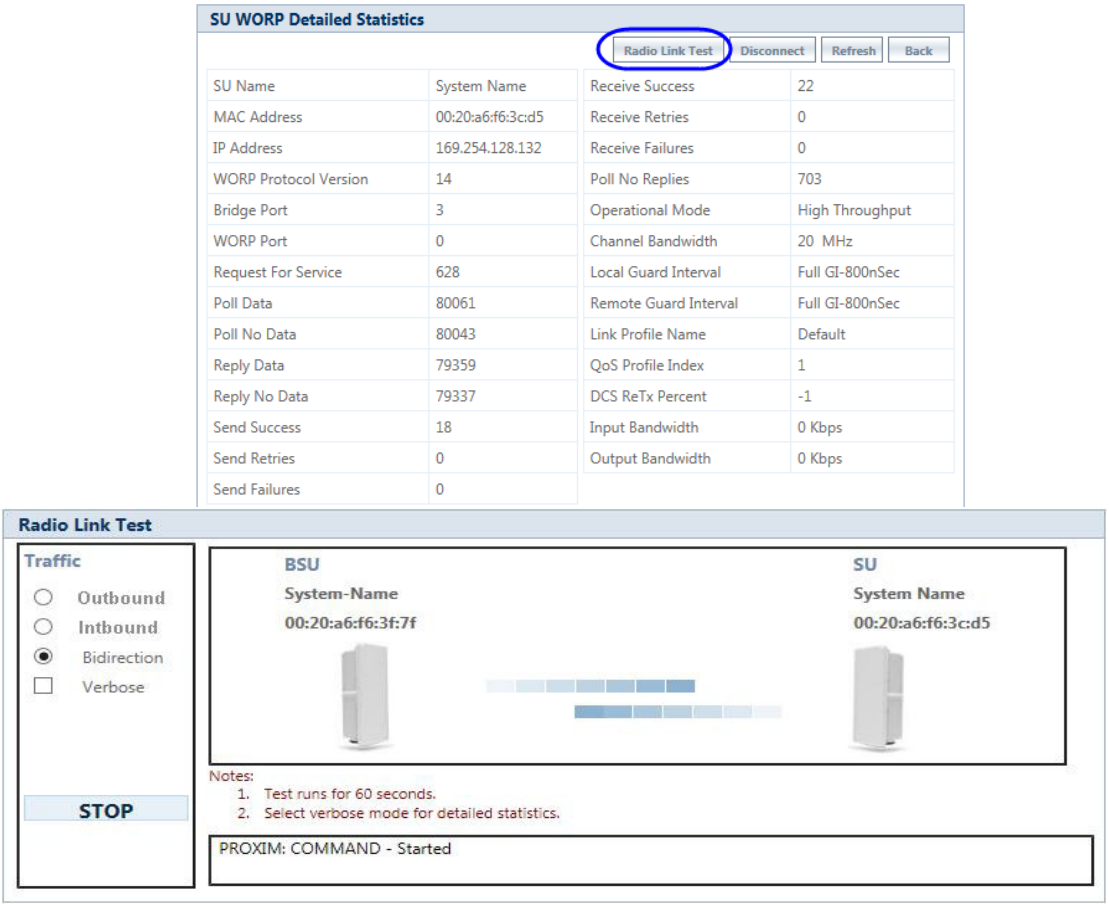
Especially for the static link establishment, this is very helpful to check the link between the two radios when installing for the first time or if any performance issues are noticed after the installation. If the link between the radios is of expected quality, then there is no issue with the wireless link. In case, if there is any issue due to wireless parameters, the link may need some tuning in configuration such as channel, Data Rate, Tx power or distance between the radios. In spite of all the testing and tuning, if the performance still fails to improve, then it may be due to installation related issues such as antenna alignment or the physical path. In the worst case, it may be a hardware related issue.

- *This is not a replacement for other wireless performance measuring tools and should be used in conjunction with other tools like Iperf or any other commercial tools.*
- *It is recommended to use this tool with caution on live networks as it will be generating internal traffic which may impact the network performance.*
- *Radio Link test is an experimental feature and will be improved in future releases.*
- *This tool can be accessed through web interface, console commands, and CLI.*
- *Both ends of a link cannot simultaneously run this test.*

- For administrator and monitor user, go to the **Summary** page and click **Link Test** to access Radio Link Test
- For advanced user, go to the **Monitor > Statistics > Interface > Link Statistics > Details** and click **Radio Link Test.**

Select the required type of traffic from the given options namely **Outbound**, **Inbound**, and **Bidirection**. Select **Verbose** along with any one of the traffic options to get a detailed test report. Next, click the **Start** button.

Alternatively, use the **rlt** commands to run the radio link test tool through **Console**. Type the required rlt command and click **Execute,** for example "rlt -t". To run the Radio Link Test tool through Command Line Interface (CLI), refer the *'Reference Guide'* for details.

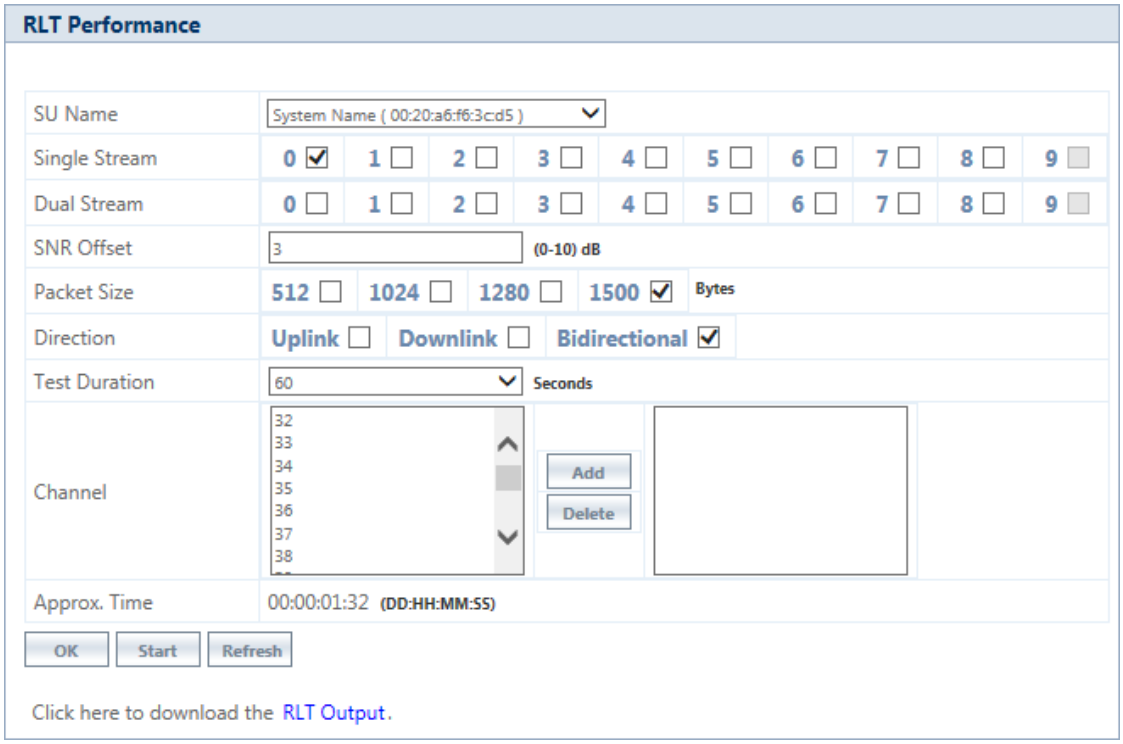


6.3 Radio Link Test Performance

Radio Link Test performance tool allows testing radio link with different transmission/network parameters such as Packet Size, Direction, Channels and different modulation rates.

: ***RLT Performance*** *option is available only on* ***BSU*** *in* ***Advanced*** *User Mode. The RLT test gets aborted if the link is down during the test procedure.*

If **Stop** button is clicked during the test procedure, the test continues running for Test Duration (until the current testing is done), and stops thereafter. After the test procedure, the default configuration is restored without any link failure. It is recommended to Disable ACS on BSU and Enable ACS on SU, before the test procedure.



Tabulated below are the RLT Performance parameters.

Parameter	Description
SU Name	Select the Subscriber Unit with which Radio Link Test should be done.
MCS Index (Single Stream / Dual Stream)	Select **Single Stream** or **Dual Stream** or **both**. • **Single Stream**: Select **Single**, for reliability and longer range. (Default:0) • **Dual Stream**: Select **Dual**, for higher throughput.
SNR Offset	This is an Offset/Threshold to be added to the **Minimum Required SNR** for calculating the supported data rates. (Default value: 3 dB)
Packet Size	Size of packet used for the test (Default value: 1500 Bytes)
Direction	Direction of the traffic (Downlink/Uplink/Bidirectional). (Default: Bidirectional)
Test Duration	Time duration for which the Radio Link Test is performed (Default: 60 seconds)
Channel	This parameter allows the user to select and operate in a preferred channel.
Approx. Time	The approximate estimated time required for the RLT performance test to complete.

: When multiple choices are selected for one Parameter, multiple tests are run, one for each instance of the parameter.i.e. if both Downlink, Uplink and Bidirectional are selected, then three sets of test are run. One with uplink packet only, one with downlink packet only and one with both uplink and downlink packet simultaneously.

Click **RLT Output** to see the following table.

```
SU/EPB System Name: AES_SU                          Channel Bandwidth : 80 MHz
MAC Address: 00:20:a6:fe:bd:f7                      Guard Interval    : Short GI

<--  : Uplink Throughput (BSU/EPA <-- SU/EPB)       Rate/Throughput in Kbps
-->  : Downlink Throughput (BSU/EPA --> SU/EPB)     Packet Size in Bytes
<==> : Bidirection Throughput (BSU/EPA <==> SU/EPB)
```

Channel : 60
Unsupported MCS index : -

Packet Size		Local SNR		Remote SNR		512			1024			1280			1500		
MCS	Rate	A1	A2	A1	A2	<--	-->	<==>	<--	-->	<==>	<--	-->	<==>	<--	-->	<==>
0	32500	65	65	67	65	28349	28319	15716	29744	29751	15624	29999	29880	14765	23552	23552	12351
1	65000	68	67	68	65	54528	54521	38237	57196	57182	39008	57685	57660	37780	57982	57987	36545
2	97500	66	66	69	66	78887	78837	54106	82711	82666	54850	83410	83414	55417	83929	83897	55532
3	130000	65	65	68	65	101462	101367	77684	106443	106351	82002	107328	107303	79196	108029	107949	79983
4	195000	64	65	68	64	141464	142101	96334	149094	149017	105967	150509	150492	103410	151440	151402	104369
5	260000	63	63	66	64	160854	176393	110956	176236	185518	111516	179772	187346	110338	181550	188367	116185
6	292500	62	62	66	62	171262	215763	183817	193236	226922	219164	198992	228522	221256	200692	230539	219988
7	325000	59	61	63	59	235445	235024	179559	247680	247515	193368	249677	249964	197716	251075	250989	198895
8	390000	56	58	59	56	267403	271426	264284	284075	284942	291214	286818	287784	293534	288610	289506	295549
9	433300	53	54	55	53	305724	304247	301361	322255	321327	303616	325345	324752	312975	327213	326673	321955
10	65000	65	65	69	66	54367	54349	38893	57017	57030	38949	57503	57522	37376	57800	57788	35518
11	130000	68	66	70	67	100931	100829	78629	105859	105772	80208	106744	106657	78604	107437	107373	80468
12	195000	67	65	70	66	139837	140927	99791	147759	147909	98605	149166	149351	103229	150055	150163	100490
13	260000	66	65	69	66	171351	173946	106523	183302	183884	106004	185229	185633	106636	186311	186761	107950
14	390000	65	65	68	65	269495	267791	275838	283445	282411	291335	286209	285262	294137	287784	287045	292371
15	520000	64	64	67	65	156567	272268	222625	189008	342683	288913	201128	334299	294530	156661	337692	296303
16	585000	62	63	65	62	183410	390637	295266	174308	415099	320582	175573	407718	338918	169681	426658	342286
17	650000	59	61	64	59	348528	347181	293339	426285	427550	411223	438065	440345	410740	444017	446775	420338
18	780000	56	58	60	56	343135	368242	357335	427284	464109	488485	441592	484220	503565	451439	489853	513324
19	866700	53	54	55	53	382995	367958	445011	472776	379258	585934	487686	485183	598388	493282	373984	608620

6.4 Console Commands

The Console Commands feature helps Proxim Technical Support team to debug field issues.

6.5 Wireless Site Survey

This feature scans all the available channels according to the current Channel Bandwidth and collects information about all BSU or End point A configured with the same network name as SU or End Point B.

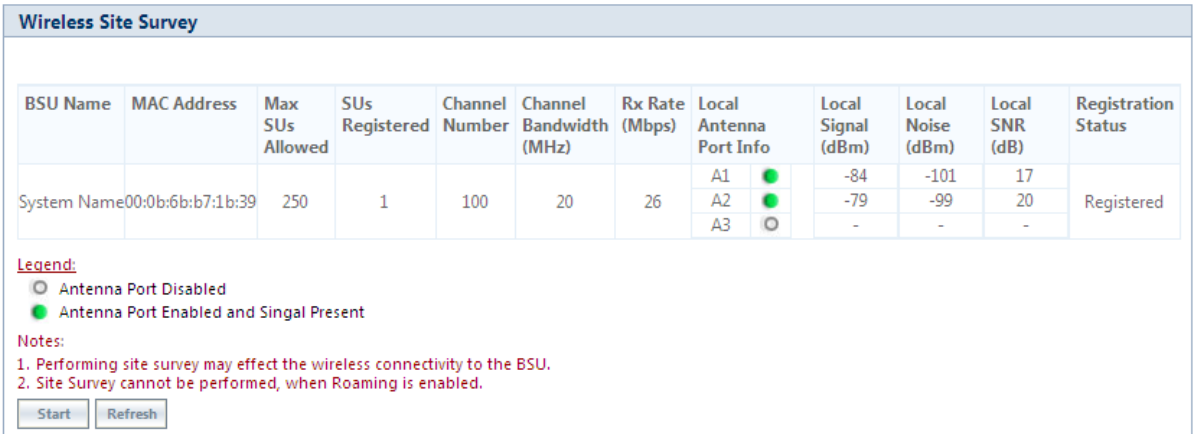


Figure 6-10 Wireless Site Survey - SU Mode

To initialize the survey process, click **Start**. This process list the details of all the available BSU or End Point A. To stop the site survey process, click Stop.

During the scan process, click **Refresh** to view the latest discovered BSU/End Point A.

- *Site Survey cannot be performed, when Roaming is enabled.*
- *Applicable only to a device in SU or End Point B mode.*

6.6 sFlow®

Proxim point-to-multipoint and point-to-point devices support sFlow® technology, developed by InMon Corporation. The sFlow® technology provides the ability to measure network traffic on all interfaces simultaneously by collecting, storing, and analyzing traffic data.

Depicted below is the sFlow architecture that consists of a sFlow Agent and a sFlow Receiver.

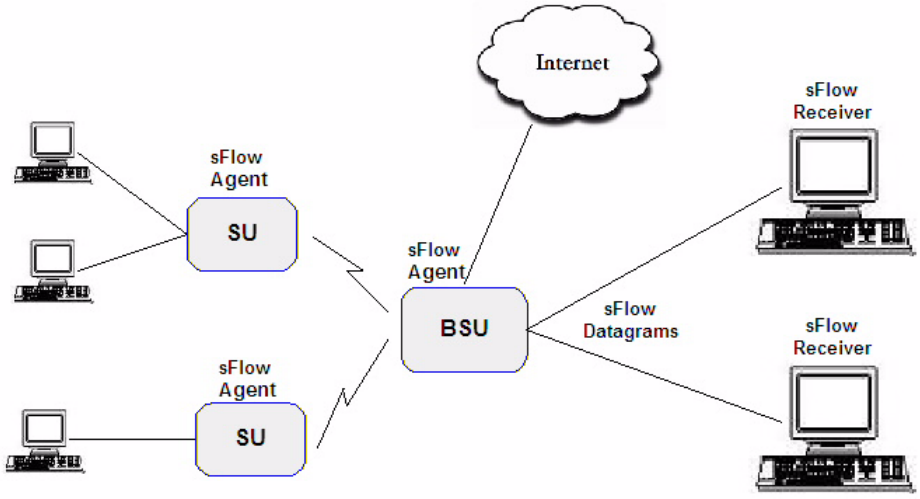


Figure 6-11 sFlow Architecture - An Example with a BSU and SUs

The **sFlow Agent**, which is running on devices, captures traffic information received on all the Ethernet interfaces, and sends sampled packets to the **sFlow Receiver** for analysis.

The sampling mechanism used to sample data are as follows:

- **Packet Flow Sampling**: In this sampling, the data packets received on the Ethernet interface of the device are sampled based on a counter. With each packet received, the counter is decremented. When the counter reaches zero, the packet is packaged and sent to the sFlow Receiver for analysis. These packets are referred to as Packet Flow Samples.
- **Counter Polling Sampling**: In this sampling, the sFlow Agent sends counters periodically to the sFlow Receiver based on the set polling interval. If polling interval is set to 5 seconds then the sFlow Agent sends counters to sFlow Receiver every 5 seconds. These packets are referred to as Counter Polling Samples.

The Packet Flow Samples and Counter Polling Samples are collectively sent to the sFlow Receiver as sFlow Datagrams. It is possible to enable either or both types of sampling.

sFlow Sampling effects the system performance and hence care must be taken in configuring the sFlow parameters.

To configure sFlow, navigate to **MONITOR** > **Tools** > **sFlow**. Following information is displayed about the sFlow Agent:

- **Version**: The version comprises the following information:
  1. **sFlow MIB Version**: Indicates the agent's MIB version. The MIB specifies how the agent extracts and bundles sampled data, and the sFlow receiver must support the agent's MIB. For example, if the sFlow MIB version is 1.3, the sFlow Receiver's version must also be at least 1.3.
  2. **Organization**: Specifies the organization implementing sFlow Agent functionality on the device. For example Proxim Wireless Corp.
  3. **Revision**: Specifies the sFlow Agent version. For example v6.4.
- **Address Type**: Specifies the protocol version for IP addresses.
- **Agent Address**: Specifies the sFlow Agent's IP address.

sFlow Receiver Configuration

The Receiver Configuration page allows you to configure sFlow Receiver(s), which receives samples from all agents on the network, combines and analyzes the samples to produce a report of network activity.

To configure sFlow Receiver do the following:

- **Index:** Represents the Receiver index number. Please note that the number of indexes depends on the Ethernet interfaces your device supports.
- **Owner:** Enter a string, which uniquely identifies the sFlow Receiver.
- **Timeout:** The sFlow Agent sends sampled packets to the specified sFlow Receiver till it reaches zero. At zero, all the Receiver parameters are set to default values.
- **Max Datagram Size:** Enter the maximum size of a sFlow datagram (in bytes), which the Receiver can receive, in the Max Datagram Size box.
- **Address Type:** The address type supported by sFlow Receiver is ipv4, which is by default selected.

  : Currently it supports only IPv4.

- **Receiver Address:** Enter the sFlow Receiver's IP address in the Receiver Address box.
- **Receiver Port:** By default, the sFlow Receiver listens to the sFlow datagrams on 6343 port.
- **Datagram Version:** The sFlow datagram version used is 5.

Click **Apply**, to save the sFlow Receiver configuration parameters.

Once the Receiver configurations are done, either Packet Flow sampling or Counter Polling Sampling or both can be started.

:

- *Enabling sampling effects the system performance and hence care should be taken in setting the right values for Timeout and Max Datagram Size.*
- *When the Owner string is cleared, the Flow Sampling and Counter Polling stops.*

Sampling Configuration

To configure and start packet flow sampling, do the following:

1. From the **Receiver Index** drop-down box, select the receiver index number associated with the sFlow Receiver to which the sFlow Agent should send the sFlow Datagrams.

   : If device has two Ethernet interfaces, then configure different Receiver indexes for each of the interface.

2. Type a value in the **Packet Sampling Rate** box. This value determines the number of packets the sFlow Agent samples from the total number of packets passing through the Ethernet interface of the device.
3. Type a value in the **Maximum Header Size** box, to set the amount of data (in bytes) to be included in the sFlow datagram. The sFlow Agent samples the specified number of bytes. For example, if you set the Maximum Header Size to 100, the sFlow Agent places the first 100 bytes of every sampled frame in the datagram. The value should match the size of the frame and packet header so that the entire header is forwarded.
4. Next, click **Apply** to start packet flow sampling. Once it starts, the **Timeout** parameter in sFlow Receiver Configuration keeps decrementing till it reaches a zero value. On reaching zero, the corresponding Receiver and Sampling values are set to default values.

- *Enabling sFlow packet sampling effects the system performance, and hence care must be taken when choosing the right value for Packet Sampling Rate and Maximum Header Size.*
- *Receiver Index for packet Sampling table and Counter Polling table should be same for each Ethernet interface.*

Counter Polling Configuration

To configure and start Counter Polling sampling, do the following:

1. From the **Receiver Index** drop-down box, choose the receiver index number associated with the sFlow Receiver to which the sFlow Agent sends the counters.

: If Packet Flow Sampling is already configured and running, then you should configure the Receiver index same as configured in the Packet Flow Sampling for each Ethernet interface.

2. Set the polling interval by typing a value in the **Interval** box. Lets say, the polling interval is set to 30 seconds. So for every 30 seconds, the counters are collected and send to the sFlow Receiver. The valid range for polling interval is 0 to 2^{31} - 1 seconds.
3. Next, click **Apply** to start Counter Polling Sampling. Once it starts, the **Timeout** parameter in sFlow Receiver Configuration keeps decrementing till it reaches a zero value. On reaching zero, the corresponding Receiver and Counter Polling values are set to default values.

- *Enabling sFlow counter sampling effects the system performance, and hence care must be taken when choosing the right value sampling interval.*
- *Receiver Index for packet Sampling table and Counter Polling table should be same for each Ethernet interface.*
- *If a sampling starts and there is already another sampling running then we consider the time out value of the current/already running sampling.*

CLI Commands 7

CLI commands mapped with SNMP are given in the following table.

MIB Name	CLI Command
PROXIM-MIB.systemContact	configure management system-information contact
PROXIM-MIB.sysContactEmail	configure management system-information email
PROXIM-MIB.sysContactPhoneNumber	configure management system-information phone-number
PROXIM-MIB.sysLocationName	configure management system-information location
PROXIM-MIB.sysGPSLongitude	configure management system-information gps-longitude
PROXIM-MIB.sysGPSLatitude	configure management system-information gps-latitude
PROXIM-MIB.sysGPSAltitude	configure management system-information gps-altitude
PROXIM-MIB.systemName	configure management system-information system-name
PROXIM-MIB.sysMgmtCfgRestore	configure management system-information restore
PROXIM-MIB.sysMgmtFactoryReset	configure management system-information factory-reset
PROXIM-MIB.sysMgmtCommand	configure management system-information sys-mgmt-command
PROXIM-MIB.tftpSrvInetAddress	configure management tftp server-ip
PROXIM-MIB.tftpFileName	configure management tftp file-name
PROXIM-MIB.tftpFileType	configure management tftp file-type
PROXIM-MIB.sysMgmtCfgProfileExcludeParam	configure management tftp cfgprof-exclude-param
PROXIM-MIB.sysMgmtCfgProfileCreate	configure management tftp cfgprof-create
PROXIM-MIB.sysMgmtCfgProfileApply	configure management tftp cfgprof-apply-and-reboot
PROXIM-MIB.allIntAccessControl	configure management access-ctrl all-access-ctrl
PROXIM-MIB.httpAccessControl	configure management access-ctrl http-ctrl
PROXIM-MIB.httpsAccessControl	configure management access-ctrl https-ctrl
PROXIM-MIB.snmpAccessControl	configure management access-ctrl snmp-ctrl
PROXIM-MIB.telnetAccessControl	configure management access-ctrl telnet-ctrl
PROXIM-MIB.sshAccessControl	configure management access-ctrl ssh-ctrl
PROXIM-MIB.mgmtSnmpTrapHostTableInetAddress	configure management trap-host-table rowedit ipaddress
PROXIM-MIB.mgmtSnmpTrapHostTablePassword	configure management trap-host-table rowedit password
PROXIM-MIB.mgmtSnmpTrapHostTableComment	configure management trap-host-table rowedit comment
PROXIM-MIB.mgmtSnmpTrapHostTableEntryStatus	configure management trap-host-table rowedit entry-status
PROXIM-MIB.mgmtSnmpTrapHostTableEntryStatus	configure management trap-host-table rowadd entry-status
PROXIM-MIB.mgmtSnmpTrapHostTableInetAddress	configure management trap-host-table rowadd ipaddress
PROXIM-MIB.mgmtSnmpTrapHostTablePassword	configure management trap-host-table rowadd password
PROXIM-MIB.mgmtSnmpTrapHostTableComment	configure management trap-host-table rowadd comment
PROXIM-MIB.mgmtAccessTableStatus	configure management access-tbl-status
PROXIM-MIB.mgmtAccessTableEntryStatus	configure management access-table rowadd entry-status

MIB Name	CLI Command
PROXIM-MIB.mgmtAccessTableInetAddress	configure management access-table rowadd ipaddress
PROXIM-MIB.mgmtAccessTableInetAddress	configure management access-table rowedit ipaddress
PROXIM-MIB.mgmtAccessTableEntryStatus	configure management access-table rowedit entry-status
PROXIM-MIB.mgmtSnmpReadPassword	configure management snmp read-password
PROXIM-MIB.mgmtSnmpReadWritePassword	configure management snmp read-write-password
PROXIM-MIB.telnetPassword	configure management telnet password
PROXIM-MIB.telnetPort	configure management telnet port
PROXIM-MIB.telnetSessions	configure management telnet sessions
PROXIM-MIB.telnetSecondaryUserPassword	configure management telnet monitor-user-passwd
PROXIM-MIB.httpPassword	configure management http password
PROXIM-MIB.httpPort	configure management http port
PROXIM-MIB.httpSecondaryUserPassword	configure management http monitor-user-passwd
PROXIM-MIB.sshPort	configure management ssh port
PROXIM-MIB.sshSessions	configure management ssh sessions
PROXIM-MIB.autoConfigRecoveryStatus	configure management auto-config-recovery status
PROXIM-MIB.autoConfigRecoveryDelay	configure management auto-config-recovery recovery-delay
PROXIM-MIB.mgmtSnmpVersion	configure management snmp snmp-version
PROXIM-MIB.mgmtSnmpV3SecurityLevel	configure management snmp v3-security-level
PROXIM-MIB.mgmtSnmpV3AuthProtocol	configure management snmp v3-auth-protocol
PROXIM-MIB.mgmtSnmpV3AuthPassword	configure management snmp v3-auth-password
PROXIM-MIB.mgmtSnmpV3PrivProtocol	configure management snmp v3-priv-protocol
PROXIM-MIB.mgmtSnmpV3PrivPassword	configure management snmp v3-priv-password
PROXIM-MIB.syslogStatus	configure management syslog status
PROXIM-MIB.syslogPriority	configure management syslog priority
PROXIM-MIB.syslogReset	configure management syslog reset
PROXIM-MIB.syslogHostTableEntryStatus	configure management syslog host-table rowadd entry-status
PROXIM-MIB.syslogHostInetAddress	configure management syslog host-table rowadd ipaddress
PROXIM-MIB.syslogHostPort	configure management syslog host-table rowadd port
PROXIM-MIB.syslogHostComment	configure management syslog host-table rowadd comment
PROXIM-MIB.syslogHostInetAddress	configure management syslog host-table rowedit ipaddress
PROXIM-MIB.syslogHostPort	configure management syslog host-table rowedit port
PROXIM-MIB.syslogHostComment	configure management syslog host-table rowedit comment
PROXIM-MIB.syslogHostTableEntryStatus	configure management syslog host-table rowedit entry-status
PROXIM-MIB.eventLogReset	configure management eventlog reset
PROXIM-MIB.eventLogPriority	configure management eventlog priority
PROXIM-MIB.debugLogBitMask	configure monitor debuglog enable

MIB Name	CLI Command
PROXIM-MIB.debugLogBitMask	configure monitor debuglog disable
PROXIM-MIB.debugLogReset	configure monitor debuglog clear-log
PROXIM-MIB.sntpStatus	configure monitor sntp sntp-status
PROXIM-MIB.sntpPrimaryServerInetAddress	configure monitor sntp primary-server-name
PROXIM-MIB.sntpSecondaryServerInetAddress	configure monitor sntp secondary-server-name
PROXIM-MIB.sntpTimeZone	configure monitor sntp time-zone
PROXIM-MIB.sntpDayLightSavingTime	configure monitor sntp day-light-savingtime
PROXIM-MIB.sntpReSyncInterval	configure monitor sntp re-sync-interval
PROXIM-MIB.sntpCurrentDateAndTime	configure monitor sntp current-date-time
PROXIM-MIB.tempLoggingInterval	configure monitor temperature interval
PROXIM-MIB.tempLogReset	configure monitor temperature reset
PROXIM-MIB.highTempThreshold	configure monitor temperature high-threshold
PROXIM-MIB.lowTempThreshold	configure monitor temperature low-threshold
PROXIM-MIB.worpSiteSurveyOperationStatus	configure monitor site-survey-tbl rowedit status
SFLOW-MIB.sFlowRcvrOwner	configure monitor sflow receiver-table rowedit owner
SFLOW-MIB.sFlowRcvrTimeout	configure monitor sflow receiver-table rowedit timeout
SFLOW-MIB.sFlowRcvrMaximumDatagramSize	configure monitor sflow receiver-table rowedit max-datagram-size
SFLOW-MIB.sFlowRcvrAddress	configure monitor sflow receiver-table rowedit address
SFLOW-MIB.sFlowRcvrPort	configure monitor sflow receiver-table rowedit port
SFLOW-MIB.sFlowFsReceiver	configure monitor sflow sampling-table rowedit receiver-indx
SFLOW-MIB.sFlowFsPacketSamplingRate	configure monitor sflow sampling-table rowedit packet-samp-rate
SFLOW-MIB.sFlowFsMaximumHeaderSize	configure monitor sflow sampling-table rowedit max-header-size
SFLOW-MIB.sFlowCpReceiver	configure monitor sflow polling-table rowedit receiver-indx
SFLOW-MIB.sFlowCpInterval	configure monitor sflow polling-table rowedit interval
PROXIM-MIB.wirelessIf5GHzStatsStatus	configure monitor wireless-stats interface wireless-stats-status
PROXIM-MIB.worpSiteSurveyBaseDisconnect	configure monitor bsu-link-stats interface rowedit bsu-disconnect
PROXIM-MIB.wirelessIfWORPStaStatsStationDisconnect	configure monitor su-link-stats interface rowedit su-disconnect
PROXIM-MIB.wirelessIfStaDisassociate	configure monitor station-disassociate
PROXIM-MIB.filteringCtrl	configure filtering global-filter-control
PROXIM-MIB.intraBSSFiltering	configure filtering intra-bss
PROXIM-MIB.etherProtocolFilteringCtrl	configure filtering protocol filter-control
PROXIM-MIB.etherProtocolFilteringType	configure filtering protocol filter-type
PROXIM-MIB.etherProtocolFilterTableStatus	configure filtering protocol protocol-table rowadd entry-status
PROXIM-MIB.etherProtocolFilterProtocolName	configure filtering protocol protocol-table rowadd protocol-name
PROXIM-MIB.etherProtocolFilterProtocolNumber	configure filtering protocol protocol-table rowadd protocol-number
PROXIM-MIB.etherprotocolFilterStatus	configure filtering protocol protocol-table rowadd filter-status

MIB Name	CLI Command
PROXIM-MIB.etherProtocolFilterProtocolName	configure filtering protocol protocol-table rowedit protocol-name
PROXIM-MIB.etherProtocolFilterProtocolNumber	configure filtering protocol protocol-table rowedit protocol-number
PROXIM-MIB.etherprotocolFilterStatus	configure filtering protocol protocol-table rowedit filter-status
PROXIM-MIB.etherProtocolFilterTableStatus	configure filtering protocol protocol-table rowedit entry-status
PROXIM-MIB.staticMACAddrFilterTableEntryStatus	configure filtering staticmac rowadd entry-status
PROXIM-MIB.staticMACAddrFilterWiredMACAddress	configure filtering staticmac rowadd wired-mac-address
PROXIM-MIB.staticMACAddrFilterWiredMACMask	configure filtering staticmac rowadd wired-mac-mask
PROXIM-MIB.staticMACAddrFilterWirelessMACAddress	configure filtering staticmac rowadd wireless-mac-address
PROXIM-MIB.staticMACAddrFilterWirelessMACMask	configure filtering staticmac rowadd wireless-mac-mask
PROXIM-MIB.staticMACAddrFilterComment	configure filtering staticmac rowadd filter-comment
PROXIM-MIB.staticMACAddrFilterTableEntryStatus	configure filtering staticmac rowedit entry-status
PROXIM-MIB.advancedFilterProtocolName	configure filtering advanced rowedit protocol-name
PROXIM-MIB.advancedFilterDirection	configure filtering advanced rowedit direction
PROXIM-MIB.advancedFilterTableEntryStatus	configure filtering advanced rowedit entry-status
PROXIM-MIB.tcpudpPortFilterCtrl	configure filtering tcpudp port-filter-ctrl
PROXIM-MIB.tcpudpPortFilterTableEntryStatus	configure filtering tcpudp tcpudp-table rowadd entry-status
PROXIM-MIB.tcpudpPortFilterProtocolName	configure filtering tcpudp tcpudp-table rowadd protocol-name
PROXIM-MIB.tcpudpPortFilterPortNumber	configure filtering tcpudp tcpudp-table rowadd port-number
PROXIM-MIB.tcpudpPortFilterPortType	configure filtering tcpudp tcpudp-table rowadd port-type
PROXIM-MIB.tcpudpPortFilterInterface	configure filtering tcpudp tcpudp-table rowadd interface
PROXIM-MIB.tcpudpPortFilterProtocolName	configure filtering tcpudp tcpudp-table rowedit protocol-name
PROXIM-MIB.tcpudpPortFilterPortNumber	configure filtering tcpudp tcpudp-table rowedit port-number
PROXIM-MIB.tcpudpPortFilterPortType	configure filtering tcpudp tcpudp-table rowedit port-type
PROXIM-MIB.tcpudpPortFilterInterface	configure filtering tcpudp tcpudp-table rowedit interface
PROXIM-MIB.tcpudpPortFilterTableEntryStatus	configure filtering tcpudp tcpudp-table rowedit entry-status
PROXIM-MIB.worpIntraCellBlockingStatus	configure filtering worp-intracell intracell-status
PROXIM-MIB.worpIntraCellBlockingMACTableEntryStatus	configure filtering worp-intracell mac-table rowadd entry-status
PROXIM-MIB.worpIntraCellBlockingMACAddress	configure filtering worp-intracell mac-table rowadd mac-address
PROXIM-MIB.worpIntraCellBlockingGroupID1	configure filtering worp-intracell mac-table rowadd group-id1
PROXIM-MIB.worpIntraCellBlockingGroupID2	configure filtering worp-intracell mac-table rowadd group-id2
PROXIM-MIB.worpIntraCellBlockingGroupID3	configure filtering worp-intracell mac-table rowadd group-id3
PROXIM-MIB.worpIntraCellBlockingGroupID4	configure filtering worp-intracell mac-table rowadd group-id4
PROXIM-MIB.worpIntraCellBlockingGroupID5	configure filtering worp-intracell mac-table rowadd group-id5
PROXIM-MIB.worpIntraCellBlockingGroupID6	configure filtering worp-intracell mac-table rowadd group-id6
PROXIM-MIB.worpIntraCellBlockingGroupID7	configure filtering worp-intracell mac-table rowadd group-id7
PROXIM-MIB.worpIntraCellBlockingGroupID8	configure filtering worp-intracell mac-table rowadd group-id8

MIB Name	CLI Command
PROXIM-MIB.worpIntraCellBlockingGroupID9	configure filtering worp-intracell mac-table rowadd group-id9
PROXIM-MIB.worpIntraCellBlockingGroupID10	configure filtering worp-intracell mac-table rowadd group-id10
PROXIM-MIB.worpIntraCellBlockingGroupID11	configure filtering worp-intracell mac-table rowadd group-id11
PROXIM-MIB.worpIntraCellBlockingGroupID12	configure filtering worp-intracell mac-table rowadd group-id12
PROXIM-MIB.worpIntraCellBlockingGroupID13	configure filtering worp-intracell mac-table rowadd group-id13
PROXIM-MIB.worpIntraCellBlockingGroupID14	configure filtering worp-intracell mac-table rowadd group-id14
PROXIM-MIB.worpIntraCellBlockingGroupID15	configure filtering worp-intracell mac-table rowadd group-id15
PROXIM-MIB.worpIntraCellBlockingGroupID16	configure filtering worp-intracell mac-table rowadd group-id16
PROXIM-MIB.worpIntraCellBlockingMACAddress	configure filtering worp-intracell mac-table rowedit mac-address
PROXIM-MIB.worpIntraCellBlockingGroupID1	configure filtering worp-intracell mac-table rowedit group-id1
PROXIM-MIB.worpIntraCellBlockingGroupID2	configure filtering worp-intracell mac-table rowedit group-id2
PROXIM-MIB.worpIntraCellBlockingGroupID3	configure filtering worp-intracell mac-table rowedit group-id3
PROXIM-MIB.worpIntraCellBlockingGroupID4	configure filtering worp-intracell mac-table rowedit group-id4
PROXIM-MIB.worpIntraCellBlockingGroupID5	configure filtering worp-intracell mac-table rowedit group-id5
PROXIM-MIB.worpIntraCellBlockingGroupID6	configure filtering worp-intracell mac-table rowedit group-id6
PROXIM-MIB.worpIntraCellBlockingGroupID7	configure filtering worp-intracell mac-table rowedit group-id7
PROXIM-MIB.worpIntraCellBlockingGroupID8	configure filtering worp-intracell mac-table rowedit group-id8
PROXIM-MIB.worpIntraCellBlockingGroupID9	configure filtering worp-intracell mac-table rowedit group-id9
PROXIM-MIB.worpIntraCellBlockingGroupID10	configure filtering worp-intracell mac-table rowedit group-id10
PROXIM-MIB.worpIntraCellBlockingGroupID11	configure filtering worp-intracell mac-table rowedit group-id11
PROXIM-MIB.worpIntraCellBlockingGroupID12	configure filtering worp-intracell mac-table rowedit group-id12
PROXIM-MIB.worpIntraCellBlockingGroupID13	configure filtering worp-intracell mac-table rowedit group-id13
PROXIM-MIB.worpIntraCellBlockingGroupID14	configure filtering worp-intracell mac-table rowedit group-id14
PROXIM-MIB.worpIntraCellBlockingGroupID15	configure filtering worp-intracell mac-table rowedit group-id15
PROXIM-MIB.worpIntraCellBlockingGroupID16	configure filtering worp-intracell mac-table rowedit group-id16
PROXIM-MIB.worpIntraCellBlockingMACTableEntryStatus	configure filtering worp-intracell mac-table rowedit entry-status
PROXIM-MIB.worpIntraCellBlockingGroupName	configure filtering worp-intracell group-table rowedit group-name
PROXIM-MIB.worpIntraCellBlockingGroupTableEntryStatus	configure filtering worp-intracell group-table rowedit entry-status
PROXIM-MIB.securityGatewayStatus	configure filtering security-gateway status
PROXIM-MIB.securityGatewayMacAddress	configure filtering security-gateway macaddress
PROXIM-MIB.stpFrameForwardStatus	configure filtering stp-frame-status
PROXIM-MIB.stormMulticastThreshold	configure filtering storm-threshold rowedit multicast-threshold
PROXIM-MIB.stormBroadcastThreshold	configure filtering storm-threshold rowedit broadcast-threshold
PROXIM-MIB.packetForwardingStatus	configure filtering packet-forwarding status
PROXIM-MIB.packetForwardingMACAddress	configure filtering packet-forwarding forwarding-tbl rowedit gateway-mac-addr

MIB Name	CLI Command
PROXIM-MIB.packetForwardingPortName	configure filtering packet-forwarding forwarding-tbl rowedit uplink-port-name
PROXIM-MIB.vlanStatus	configure vlan vlan-status
PROXIM-MIB.radiusVLANStatus	configure vlan radius-vlan-status
PROXIM-MIB.mgmtVLANIdentifier	configure vlan mgmt-vlan-id
PROXIM-MIB.mgmtVLANPriority	configure vlan mgmt-vlan-priority
PROXIM-MIB.qinqStatus	configure vlan double-vlan-status
PROXIM-MIB.tagProtocolID	configure vlan service-vlan-tpid
PROXIM-MIB.serviceProviderVLANID	configure vlan service-vlan-id
PROXIM-MIB.serviceProviderVLANPriority	configure vlan service-vlan-priority
PROXIM-MIB.vlanMode	configure vlan config-table rowedit vlan-mode
PROXIM-MIB.accessVLANId	configure vlan config-table rowedit access-vlan-id
PROXIM-MIB.accessVLANPriority	configure vlan config-table rowedit access-vlan-priority
PROXIM-MIB.untaggedFrames	configure vlan config-table rowedit untagged-frames
PROXIM-MIB.portVLANID	configure vlan config-table rowedit port-vlan-id
PROXIM-MIB.portVLANPriority	configure vlan config-table rowedit port-vlan-priority
PROXIM-MIB.allowUntaggedMgmtAccess	configure vlan config-table rowedit allow-untagged-mgmt-access
PROXIM-MIB.vlanEthTrunkTableEntryStatus	configure vlan trunk-table rowadd secondary-index entry-status
PROXIM-MIB.ethVLANTrunkId	configure vlan trunk-table rowadd secondary-index trunk-id
PROXIM-MIB.ethVLANTrunkId	configure vlan trunk-table rowedit secondary-index trunk-id
PROXIM-MIB.vlanEthTrunkTableEntryStatus	configure vlan trunk-table rowedit secondary-index entry-status
PROXIM-MIB.wirelessSecurityCfgEntryStatus	configure security security-profile rowadd entry-status
PROXIM-MIB.wirelessSecurityCfgprofileName	configure security security-profile rowadd profile-name
PROXIM-MIB.wirelessSecurityCfgAuthenticationMode	configure security security-profile rowadd authentication-mode
PROXIM-MIB.wirelessSecurityCfgKey1	configure security security-profile rowadd key1
PROXIM-MIB.wirelessSecurityCfgdot1xWepKeyLength	configure security security-profile rowadd dot1x-wepkey-length
PROXIM-MIB.wirelessSecurityCfgEncryptionType	configure security security-profile rowadd encryption-type
PROXIM-MIB.wirelessSecurityCfgPSK	configure security security-profile rowadd psk
PROXIM-MIB.wirelessSecurityCfgRekeyingInterval	configure security security-profile rowadd rekey-interval
PROXIM-MIB.wirelessSecurityCfgKeyIndex	configure security security-profile rowadd key-index
PROXIM-MIB.wirelessSecurityCfgNetworkSecret	configure security security-profile rowadd network-secret
PROXIM-MIB.wirelessSecurityCfgKey2	configure security security-profile rowadd key2
PROXIM-MIB.wirelessSecurityCfgKey3	configure security security-profile rowadd key3
PROXIM-MIB.wirelessSecurityCfgKey4	configure security security-profile rowadd key4
PROXIM-MIB.wirelessSecurityCfgprofileName	configure security security-profile rowedit profile-name
PROXIM-MIB.wirelessSecurityCfgAuthenticationMode	configure security security-profile rowedit authentication-mode
PROXIM-MIB.wirelessSecurityCfgKey1	configure security security-profile rowedit key1

MIB Name	CLI Command
PROXIM-MIB.wirelessSecurityCfgdot1xWepKeyLength	configure security security-profile rowedit dot1x-wepkey-length
PROXIM-MIB.wirelessSecurityCfgEncryptionType	configure security security-profile rowedit encryption-type
PROXIM-MIB.wirelessSecurityCfgPSK	configure security security-profile rowedit psk
PROXIM-MIB.wirelessSecurityCfgRekeyingInterval	configure security security-profile rowedit rekey-interval
PROXIM-MIB.wirelessSecurityCfgEntryStatus	configure security security-profile rowedit entry-status
PROXIM-MIB.wirelessSecurityCfgNetworkSecret	configure security security-profile rowedit network-secret
PROXIM-MIB.wirelessSecurityCfgKey2	configure security security-profile rowedit key2
PROXIM-MIB.wirelessSecurityCfgKey3	configure security security-profile rowedit key3
PROXIM-MIB.wirelessSecurityCfgKey4	configure security security-profile rowedit key4
PROXIM-MIB.wirelessSecurityCfgKeyIndex	configure security security-profile rowedit key-index
PROXIM-MIB.wirelessSecurityProfileGroupType	configure security security-profile rowadd sec-profile-group-type
PROXIM-MIB.wirelessSecurityProfileGroupType	configure security security-profile rowedit sec-profile-group-type
PROXIM-MIB.wirelessIfPropertiesRadioStatus	configure wireless properties radio radio-status
PROXIM-MIB.wirelessIfOperationalMode	configure wireless properties radio operational-mode
PROXIM-MIB.wirelessIfCurrentChannelBandwidth	configure wireless properties radio current-bandwidth
PROXIM-MIB.wirelessIfChannelOffset	configure wireless properties radio channel-offset
PROXIM-MIB.wirelessIfAutoChannelSelection	configure wireless properties radio auto-channel-selection
PROXIM-MIB.wirelessIfCurrentOperatingChannel	configure wireless properties radio configured-channel
PROXIM-MIB.wirelessIfAutoRateSelection	configure wireless properties radio auto-rate-selection
PROXIM-MIB.wirelessIfTransmittedRate	configure wireless properties radio transmit-rate
PROXIM-MIB.wirelessIfVAPRTSThreshold	configure wireless properties radio rts-threshold
PROXIM-MIB.wirelessIfVAPBeaconInterval	configure wireless properties radio beacon-interval
PROXIM-MIB.wirelessIfTPC	configure wireless properties radio tpc
PROXIM-MIB.wirelessIfCellSize	configure wireless properties radio cellsize
PROXIM-MIB.wirelessIfMaxEIRP	configure wireless properties radio max-eirp
PROXIM-MIB.wirelessIfTMPDCSStatus	configure wireless properties radio dcs-status
PROXIM-MIB.wirelessIfDCSReTxThreshold	configure wireless properties radio dcs-retx-thrld
PROXIM-MIB.wirelessIfDCSBadlinkThreshold	configure wireless properties radio dcs-badlink-thrld
PROXIM-MIB.wirelessIfDTIM	configure wireless properties radio dtim
PROXIM-MIB.wirelessIfAntennaGain	configure wireless properties radio antenna-gain
PROXIM-MIB.wirelessIfSatelliteDensity	configure wireless properties radio satellite-density
PROXIM-MIB.wirelessIfSensitivity	configure wireless properties radio sensitivity
PROXIM-MIB.wirelessIfWindowLength	configure wireless properties radio window-length
PROXIM-MIB.wirelessIfLowRSSIThreshold	configure wireless properties radio rssi-threshold
PROXIM-MIB.wirelessIfLowRSSICheckTime	configure wireless properties radio rssi-check-time
PROXIM-MIB.wirelessIfHighPowerMode	configure wireless properties radio high-power-mode

MIB Name	CLI Command
PROXIM-MIB.wirelessIfAckTimeout	configure wireless properties radio ack-timeout
PROXIM-MIB.wirelessIfDDRSMinReqSNR	configure wireless ddrs snr-table radio rowedit min-req-snr
PROXIM-MIB.wirelessIfDDRSMaxOptimalSNR	configure wireless ddrs snr-table radio rowedit max-opt-snr
PROXIM-MIB.wirelessIfRoamingStatus	configure wireless roaming radio roaming-status
PROXIM-MIB.wirelessIfRoamingDownlinkBuffering	configure wireless roaming radio downlink-buffering
PROXIM-MIB.wirelessIfRoamingLinkProfileIndex	configure wireless roaming radio roaming-link-profile-index
PROXIM-MIB.wirelessIfRoamingAnnouncePeriod	configure wireless roaming radio announce-period
PROXIM-MIB.wirelessIfRoamingMaximumPacketsPerBurst	configure wireless roaming radio max-pkts-per-burst
PROXIM-MIB.wirelessIfRoamingVLANId	configure wireless roaming radio roam-vlan-id
PROXIM-MIB.wirelessIfRoamingSlowRxSNRThrld	configure wireless roaming radio slow-roam-rx-snr-thrld
PROXIM-MIB.wirelessIfRoamingFastRxSNRThrld	configure wireless roaming radio fast-roam-rx-snr-thrld
PROXIM-MIB.wirelessIfRoamingToggleOffset	configure wireless roaming radio roam-toggle-offset
PROXIM-MIB.wirelessIfRoamingChannelEntryStatus	configure wireless roaming roaming-channel-table radio rowadd entry-status
PROXIM-MIB.wirelessIfRoamingChannel	configure wireless roaming roaming-channel-table radio rowadd channel
PROXIM-MIB.wirelessIfRoamingChannel	configure wireless roaming roaming-channel-table radio rowedit channel
PROXIM-MIB.wirelessIfRoamingChannelEntryStatus	configure wireless roaming roaming-channel-table radio rowedit entry-status
PROXIM-MIB.wirelessIfWhiteChanEntryStatus	configure wireless white-channel-list radio rowedit entry-status
PROXIM-MIB.wirelessIfChannelWaitTime	configure wireless dfs radio channel-wait-time
PROXIM-MIB.wirelessIfDfsNumSatWithRadarForFreqSwitch	configure wireless dfs radio sus-reporting-radar
PROXIM-MIB.wirelessIfDfsStatus	configure wireless dfs radio dfs-status
PROXIM-MIB.wirelessIfForcePreferredChannel	configure wireless dfs radio force-preferred-channel
PROXIM-MIB.wirelessIf11nPropertiesAMPDUStatus	configure wireless mimo radio ampdu-status
PROXIM-MIB.wirelessIf11nPropertiesAMPDUMaxNumFrames	configure wireless mimo radio ampdu-max-frames
PROXIM-MIB.wirelessIf11nPropertiesAMPDUMaxFrameSize	configure wireless mimo radio ampdu-max-frame-size
PROXIM-MIB.wirelessIf11nPropertiesAMSDUStatus	configure wireless mimo radio amsdu-status
PROXIM-MIB.wirelessIf11nPropertiesFrequencyExtension	configure wirelessmimoradio frequency-extension
PROXIM-MIB.wirelessIf11nPropertiesGuardInterval	configure wireless mimo radio guard-interval
PROXIM-MIB.wirelessIf11nPropertiesRxAntennas	configure wireless mimo radio rx-antennas
PROXIM-MIB.wirelessIfVAPType	configure wireless vap index secondary-index type
PROXIM-MIB.wirelessIfVAPSSID	configure wireless vap index secondary-index ssid
PROXIM-MIB.wirelessIfVAPBroadcastSSID	configure wireless vap index secondary-index broadcast-ssid
PROXIM-MIB.wirelessIfVAPFragmentationThreshold	configure wireless vap index secondary-index fragmentation
PROXIM-MIB.wirelessIfVAPRadiusProfileName	configure wireless vap index secondary-index radius-name
PROXIM-MIB.wirelessIfVAPVLANID	configure wireless vap index secondary-index vlan-id

MIB Name	CLI Command
PROXIM-MIB.wirelessIfVAPVLANPriority	configure wireless vap index secondary-index vlan-priority
PROXIM-MIB.wirelessIfVAPQoSProfileName	configure wireless vap index secondary-index qos-name
PROXIM-MIB.wirelessIfVAPMACACLStatus	configure wireless vap index secondary-index macacl-status
PROXIM-MIB.wirelessIfVAPRadiusMACACLStatus	configure wireless vap index secondary-index radius-macacl-status
PROXIM-MIB.wirelessIfVAPRadiusAccStatus	configure wireless vap index secondary-index radius-acc-status
PROXIM-MIB.wirelessIfVAPStatus	configure wireless vap index secondary-index status
PROXIM-MIB.wirelessIfVAPSecurityProfileIndex	configure wireless vap index secondary-index security-profile-index
PROXIM-MIB.wirelessIfVAPRadiusProfileIndex	configure wireless vap index secondary-index radius-profile-index
PROXIM-MIB.wirelessIfVAPMulticastLegacyRate	configure wireless vap index secondary-index multicast-legacy-rate
PROXIM-MIB.wirelessIfVAPMaxStations	configure wireless vap index secondary-index max-stations
PROXIM-MIB.wirelessIfVAPIqueMe	configure wireless vap index secondary-index iqme
PROXIM-MIB.wirelessIfVAPStream	configure wireless vap index secondary-index data-stream
PROXIM-MIB.wirelessIfInActivityTimerInSeconds	configure wireless wireless-timer radio wireless-inactive-timer
PROXIM-MIB.wirelessIfWORPBaseStationName	configure wireless worp radio bsu-name
PROXIM-MIB.wirelessIfWORPBaseStationName	configure wireless worp radio endpointa-name
PROXIM-MIB.wirelessIfWORPSecBaseStationName	configure wireless worp radio secondary-bsu-name
PROXIM-MIB.wirelessIfWORPBaseSwitchInterval	configure wireless worp radio bsu-switch-interval
PROXIM-MIB.wirelessIfWORPNetworkName	configure wireless worp radio network-name
PROXIM-MIB.wirelessIfWORPMaxSatellites	configure wireless worp radio max-sus
PROXIM-MIB.wirelessIfWORPMaxTimedOutSatellites	configure wireless worp radio poll-backoff-on-timeout
PROXIM-MIB.wirelessIfWORPErrorCountThreshold.1	configure wireless worp radio error-count-threshold
PROXIM-MIB.wirelessIfWORPRSSIDropThreshold.1	configure wireless worp radio rssi-drop-threshold
PROXIM-MIB.wirelessIfWORPMTU	configure wireless worp radio worp-mtu
PROXIM-MIB.wirelessIfWORPSuperPacketing	configure wireless worp radio super-frame
PROXIM-MIB.wirelessIfWORPSleepMode	configure wireless worp radio sleep-mode
PROXIM-MIB.wirelessIfWORPMultiFrameBursting	configure wireless worp radio multi-frame-burst
PROXIM-MIB.wirelessIfWORPRegistrationTimeout	configure wireless worp radio registration-timeout
PROXIM-MIB.wirelessIfWORPRetries	configure wireless worp radio retry-count
PROXIM-MIB.wirelessIfWORPTimeoutOffset	configure wireless worp radio timeout-offset
PROXIM-MIB.wirelessIfWORPInputBandwidthLimit	configure wireless worp radio input-bandwidth-limit
PROXIM-MIB.wirelessIfWORPOutputBandwidthLimit	configure wireless worp radio output-bandwidth-limit
PROXIM-MIB.wirelessIfWORPSecurityProfileIndex	configure wireless worp radio security-profile-index
PROXIM-MIB.wirelessIfWORPRadiusProfileIndex	configure wireless worp radio radius-profile-index
PROXIM-MIB.wirelessIfWORPMACACLStatus	configure wireless worp radio mac-acl
PROXIM-MIB.wirelessIfWORPRadiusMACACLStatus	configure wireless worp radio radius-mac-acl
PROXIM-MIB.wirelessIfWORPBandwidthLimitType	configure wireless worp radio bandwidth-limit-type

MIB Name	CLI Command
PROXIM-MIB.wirelessIfWORPAutoMultiFrameBursting	configure wireless worp radio auto-multi-frame-burst
PROXIM-MIB.wirelessIfWORPSyncStatus	configure wireless worp radio sync-status
PROXIM-MIB.wirelessIfWORPSyncDLTimeFrame	configure wireless worp radio downlink-time-frame
PROXIM-MIB.wirelessIfWORPSyncULTimeFrame	configure wireless worp radio uplink-time-frame
PROXIM-MIB.wirelessIfWORPSyncDLSubSlots	configure wireless worp radio downlink-sub-slots
PROXIM-MIB.wirelessIfWORPSyncULSubSlots	configure wireless worp radio uplink-sub-slots
PROXIM-MIB.wirelessIfWORPSyncInterFrameDelay	configure wireless worp radio inter-frame-delay
PROXIM-MIB.wirelessIfWORPSyncIntraFrameDelay	configure wireless worp radio intra-frame-delay
PROXIM-MIB.wirelessIfWORPSyncOffset	configure wireless worp radio sync-offset
PROXIM-MIB.wirelessIfWORPSyncStopIfNoGPS	configure wireless worp radio stop-if-no-gps
PROXIM-MIB.wirelessIfWORPSyncCompatibility	configure wireless worp radio sync-compatibility
PROXIM-MIB.wirelessIfWORPSyncDLRatio	configure wireless worp radio sync-dl-ratio
PROXIM-MIB.wirelessIfWORPSyncMaxDistance	configure wireless worp radio sync-max-distance
PROXIM-MIB.wirelessIfWORPSyncControlSlots	configure wireless worp radio sync-control-slots
PROXIM-MIB.wirelessIfWORPSyncGPSSource	configure wireless worp radio sync-gps-source
PROXIM-MIB.wirelessIfWORPProfilePeerTableEntryStatus	configure wireless profile-peer-list radio rowadd entrystatus
PROXIM-MIB.wirelessIfWORPProfilePeerMACAddress	configure wireless profile-peer-list radio rowadd wireless-mac-address
PROXIM-MIB.wirelessIfWORPProfilePeerDeviceName	configure wireless profile-peer-list radio rowadd device-name
PROXIM-MIB.wirelessIfWORPProfilePeerProfileIndex	configure wireless profile-peer-list radio rowadd link-profile-index
PROXIM-MIB.wirelessIfWORPProfilePeerQoSIndex	configure wireless profile-peer-list radio rowadd qos-class-index
PROXIM-MIB.wirelessIfWORPProfilePeerMACAddress	configure wireless profile-peer-list radio rowedit wireless-mac-address
PROXIM-MIB.wirelessIfWORPProfilePeerDeviceName	configure wireless profile-peer-list radio rowedit device-name
PROXIM-MIB.wirelessIfWORPProfilePeerProfileIndex	configure wireless profile-peer-list radio rowedit link-profile-index
PROXIM-MIB.wirelessIfWORPProfilePeerQoSIndex	configure wireless profile-peer-list radio rowedit qos-class-index
PROXIM-MIB.wirelessIfWORPProfilePeerTableEntryStatus	configure wireless profile-peer-list radio rowedit entrystatus-end
PROXIM-MIB.linkProfileTableEntryStatus	configure wireless link-profiles radio rowadd entrystatus
PROXIM-MIB.linkProfileName	configure wireless link-profiles radio rowadd profile-name
PROXIM-MIB.linkProfileDDRSStatus	configure wireless link-profiles radio rowadd ddrs-status
PROXIM-MIB.linkProfileDDRSMinDataRate	configure wireless link-profiles radio rowadd ddrs-min-data-rate
PROXIM-MIB.linkProfileDDRSMaxDataRate	configure wireless link-profiles radio rowadd ddrs-max-data-rate
PROXIM-MIB.linkProfileDDRSLowerSNRCorrection	configure wireless link-profiles radio rowadd ddrs-low-snr-correction
PROXIM-MIB.linkProfileDDRSUpperSNRCorrection	configure wireless link-profiles radio rowadd ddrs-upper-snr-correction
PROXIM-MIB.linkProfileDDRSRateIncrRTXThrld	configure wireless link-profiles radio rowadd ddrs-rate-incr-rtx-thrld
PROXIM-MIB.linkProfileDDRSRateDecrRTXThrld	configure wireless link-profiles radio rowadd ddrs-rate-decr-rtx-thrld
PROXIM-MIB.linkProfileDDRSChainBalThrld	configure wireless link-profiles radio rowadd ddrs-chain-bal-thrld
PROXIM-MIB.linkProfileDDRSRateBackOffInt	configure wireless link-profiles radio rowadd ddrs-back-off-interval

MIB Name	CLI Command
PROXIM-MIB.linkProfileDDRSRateBlacklistInt	configure wireless link-profiles radio rowadd ddrs-blacklist-interval
PROXIM-MIB.linkProfileDDRSRateStableInt	configure wireless link-profiles radio rowadd ddrs-stable-interval
PROXIM-MIB.linkProfileATPCStatus	configure wireless link-profiles radio rowadd atpc-status
PROXIM-MIB.linkProfileATPCUpperMargin	configure wireless link-profiles radio rowadd atpc-upper-margin
PROXIM-MIB.linkProfileATPCLowerMargin	configure wireless link-profiles radio rowadd atpc-lower-margin
PROXIM-MIB.linkProfileTPC	configure wireless link-profiles radio rowadd tpc
PROXIM-MIB.linkProfileTxRate	configure wireless link-profiles radio rowadd tx-rate
PROXIM-MIB.linkProfileDataStreams	configure wireless link-profiles radio rowadd data-streams
PROXIM-MIB.linkProfileAutoTxAntStatus	configure wireless link-profiles radio rowadd auto-tx-antenna-status
PROXIM-MIB.linkProfileTxAntChainMask	configure wireless link-profiles radio rowadd tx-antenna-chainmask
PROXIM-MIB.linkProfileName	configure wireless link-profiles radio rowedit profile-name
PROXIM-MIB.linkProfileDDRSStatus	configure wireless link-profiles radio rowedit ddrs-status
PROXIM-MIB.linkProfileDDRSMinDataRate	configure wireless link-profiles radio rowedit ddrs-min-data-rate
PROXIM-MIB.linkProfileDDRSMaxDataRate	configure wireless link-profiles radio rowedit ddrs-max-data-rate
PROXIM-MIB.linkProfileDDRSLowerSNRCorrection	configure wireless link-profiles radio rowedit ddrs-low-snr-correction
PROXIM-MIB.linkProfileDDRSUpperSNRCorrection	configure wireless link-profiles radio rowedit ddrs-upper-snr-correction
PROXIM-MIB.linkProfileDDRSRateIncrRTXThrld	configure wireless link-profiles radio rowedit ddrs-rate-incr-rtx-thrld
PROXIM-MIB.linkProfileDDRSRateDecrRTXThrld	configure wireless link-profiles radio rowedit ddrs-rate-decr-rtx-thrld
PROXIM-MIB.linkProfileDDRSChainBalThrld	configure wireless link-profiles radio rowedit ddrs-chain-bal-thrld
PROXIM-MIB.linkProfileDDRSRateBackOffInt	configure wireless link-profiles radio rowedit ddrs-back-off-interval
PROXIM-MIB.linkProfileDDRSRateBlacklistInt	configure wireless link-profiles radio rowedit ddrs-blacklist-interval
PROXIM-MIB.linkProfileDDRSRateStableInt	configure wireless link-profiles radio rowedit ddrs-stable-interval
PROXIM-MIB.linkProfileATPCStatus	configure wireless link-profiles radio rowedit atpc-status
PROXIM-MIB.linkProfileATPCUpperMargin	configure wireless link-profiles radio rowedit atpc-upper-margin
PROXIM-MIB.linkProfileATPCLowerMargin	configure wireless link-profiles radio rowedit atpc-lower-margin
PROXIM-MIB.linkProfileTPC	configure wireless link-profiles radio rowedit tpc
PROXIM-MIB.linkProfileTxRate	configure wireless link-profiles radio rowedit tx-rate
PROXIM-MIB.linkProfileDataStreams	configure wireless link-profiles radio rowedit data-streams
PROXIM-MIB.linkProfileAutoTxAntStatus	configure wireless link-profiles radio rowedit auto-tx-antenna-status
PROXIM-MIB.linkProfileTxAntChainMask	configure wireless link-profiles radio rowedit tx-antenna-chainmask
PROXIM-MIB.linkProfileTableEntryStatus	configure wireless link-profiles radio rowedit entrystatus
PROXIM-MIB.qosProfileName	configure ap-qos profile-table rowedit profile-name
PROXIM-MIB.qosProfileTablePolicyName	configure ap-qos profile-table rowedit policy-name
PROXIM-MIB.qosProfileEDCAProfileName	configure ap-qos profile-table rowedit edca-profile-name
PROXIM-MIB.qosProfileTableQoSNACKStatus	configure ap-qos profile-table rowedit nack-status
PROXIM-MIB.qoSPolicyPriorityMapping	configure ap-qos policy-table rowedit secondary-index priority-mapping

MIB Name	CLI Command
PROXIM-MIB.qoSPolicyMarkingStatus	configure ap-qos policy-table rowedit secondary-index marking-status
PROXIM-MIB.qoSPolicyTableEntryStatus	configure ap-qos policy-table rowedit secondary-index entry-status
PROXIM-MIB.wirelessQoSEDCATableProfileName	configure ap-qos edca-table rowedit secondary-index profile-name
PROXIM-MIB.wirelessQoSEDCATableCWmin	configure ap-qos edca-table rowedit secondary-index sta-cwmin
PROXIM-MIB.wirelessQoSEDCATableCWmax	configure ap-qos edca-table rowedit secondary-index sta-cwmax
PROXIM-MIB.wirelessQoSEDCATableAIFSN	configure ap-qos edca-table rowedit secondary-index sta-aifsn
PROXIM-MIB.wirelessQoSEDCATableTXOP	configure ap-qos edca-table rowedit secondary-index sta-txop
PROXIM-MIB.wirelessQoSEDCATableACM	configure ap-qos edca-table rowedit secondary-index sta-acm
PROXIM-MIB.wirelessQoSEDCATableAPCWmin	configure ap-qos edca-table rowedit secondary-index ap-cwmin
PROXIM-MIB.wirelessQoSEDCATableAPCWmax	configure ap-qos edca-table rowedit secondary-index ap-cwmax
PROXIM-MIB.wirelessQoSEDCATableAPAIFSN	configure ap-qos edca-table rowedit secondary-index ap-aifsn
PROXIM-MIB.wirelessQoSEDCATableAPTXOP	configure ap-qos edca-table rowedit secondary-index ap-txop
PROXIM-MIB.wirelessQoSEDCATableAPACM	configure ap-qos edca-table rowedit secondary-index ap-acm
PROXIM-MIB.l2l3QoSDot1Priority	configure ap-qos dot1p-mapping-table rowedit dot1d-priority dot1p-priority
PROXIM-MIB.l2l3QoSDSCPPriorityLowerLimit	configure ap-qos ipdscp-mapping-tble rowedit ipdscp lower-limit
PROXIM-MIB.l2l3QoSDSCPPriorityUpperLimit	configure ap-qos ipdscp-mapping-tble rowedit ipdscp upper-limit
PROXIM-MIB.netIpCfgIPAddress	configure network ip ethernet-ip-table rowedit ipaddress
PROXIM-MIB.netIpCfgSubnetMask	configure network ip ethernet-ip-table rowedit mask
PROXIM-MIB.netIpCfgAddressType	configure network ip ethernet-ip-table rowedit address-type
PROXIM-MIB.netIpWirelessCfgIPAddress	configure network ip wireless-ip-table rowedit ip
PROXIM-MIB.netIpWirelessCfgSubnetMask	configure network ip wireless-ip-table rowedit mask
PROXIM-MIB.netIpWirelessCfgAddrType	configure network ip wireless-ip-table rowedit address-type
PROXIM-MIB.netIpWirelessCfgPPPoESecInetAddress	configure network ip wireless-ip-table rowedit pppoe-secip
PROXIM-MIB.netIpWirelessCfgPPPoESecMask	configure network ip wireless-ip-table rowedit pppoe-secmask
PROXIM-MIB.netCfgAllIntfDefaultRouterAddr	configure network ip default-gateway
PROXIM-MIB.netCfgDefaultGatewayInetAddress	configure network ip default-gatewayv6
PROXIM-MIB.netIpCfgIPMode.1	configure network ip ip-mode
PROXIM-MIB.netIpCfgInetAddress	configure network ipethernet-ipv6-table rowedit ipv6address
PROXIM-MIB.netIpCfgInetAddressType	configure network ip ethernet-ipv6-table rowedit v6address-type
PROXIM-MIB.netCfgClearIntfStats	configure network clear-interface-stats
PROXIM-MIB.netCfgPrimaryDNSInetAddress	configure network primary-dns-ip
PROXIM-MIB.netCfgSecondaryDNSInetAddress	configure network secondary-dns-ip
PROXIM-MIB.netCfgDNSProxyStatus	configure network dns-proxy-status
PROXIM-MIB.hotspotStatus	configure network hotspot hotspot-status
PROXIM-MIB.hotspotWebRedirect	configure network hotspot hotspot-webredirect
PROXIM-MIB.hotspotNASId	configure network hotspot hotspot-nasid

MIB Name	CLI Command
PROXIM-MIB.hotspotUAMSecret	configure network hotspot hotspot-uamsecret
PROXIM-MIB.hotspotADMUSR	configure network hotspot hotspot-adminuser
PROXIM-MIB.hotspotADMPWD	configure network hotspot hotspot-adminpassword
PROXIM-MIB.hotspotSessionTimeout	configure network hotspot hotspot-sessiontimeout
PROXIM-MIB.hotspotPrimaryRadiusServer	configure network hotspot hotspot-primaryradius
PROXIM-MIB.hotspotSecondaryRadiusServer	configure network hotspot hotspot-secondaryradius
PROXIM-MIB.hotspotRadiusSharedSecret	configure network hotspot hotspot-radiusshared
PROXIM-MIB.hotspotWallGardenTableEntryStatus	configure network hotspot hotspot-wallgarden-tbl rowadd entry-status
PROXIM-MIB.hotspotWallGardenDomain	configure network hotspot hotspot-wallgarden-tbl rowadd hotspot-domain
PROXIM-MIB.hotspotWallGardenTableEntryStatus	configure network hotspot hotspot-wallgarden-tbl rowedit entry-status
PROXIM-MIB.hotspotWallGardenDomain	configure network hotspot hotspot-wallgarden-tbl rowedit hotspot-domain
PROXIM-MIB.hotspotLanPoolStartIPAddress	configure network hotspot hotspot-lanpool-tbl rowedit hotspot-lanpoolstartip
PROXIM-MIB.hotspotLanPoolEndIPAddress	configure network hotspot hotspot-lanpool-tbl rowedit hotspot-lanpoolendip
PROXIM-MIB.natStatus	configure network nat nat-status
PROXIM-MIB.natPortBindingStatus	configure network nat port-bind-status
PROXIM-MIB.natDynamicStartPort	configure network nat dynamic-start-port
PROXIM-MIB.natDynamicEndPort	configure network nat dynamic-end-port
PROXIM-MIB.natStaticPortBindTableEntryStatus	configure network nat port-bind-table rowadd entry-status
PROXIM-MIB.natStaticPortBindLocalAddr	configure network nat port-bind-table rowadd local-address
PROXIM-MIB.natStaticPortBindPortType	configure network nat port-bind-table rowadd port-type
PROXIM-MIB.natStaticPortBindStartPortNum	configure network nat port-bind-table rowadd start-portnumber
PROXIM-MIB.natStaticPortBindEndPortNum	configure network nat port-bind-table rowadd end-portnumber
PROXIM-MIB.natStaticPortBindTableEntryStatus	configure network nat port-bind-table rowedit entry-status
PROXIM-MIB.ripConfigStatus	configure network rip status
PROXIM-MIB.ripInterfaceStatus	configure network rip config-table rowedit status
PROXIM-MIB.ripInterfaceAuthType	configure network rip config-table rowedit authentication-type
PROXIM-MIB.ripInterfaceAuthKey	configure network rip config-table rowedit authentication-key
PROXIM-MIB.ripInterfaceVersionNum	configure network rip config-table rowedit version-number
PROXIM-MIB.ripReceiveOnly	configure network rip config-table rowedit receive-only
PROXIM-MIB.tunnelingStatus	configure network tunneling tunneling-status
PROXIM-MIB.tunnelConfigTableEntryStatus	configure network tunneling tunneling-table rowadd entry-status
PROXIM-MIB.tunnelConfigName	configure network tunneling tunneling-table rowadd config-name
PROXIM-MIB.tunnelConfigEncapMethod	configure network tunneling tunneling-table rowadd encap-method

MIB Name	CLI Command
PROXIM-MIB.tunnelConfigVirtualIPAddress	configure network tunneling tunneling-table rowadd virtual-ip
PROXIM-MIB.tunnelConfigLocalIPAddress	configure network tunneling tunneling-table rowadd local-ip
PROXIM-MIB.tunnelConfigRemoteIPAddress	configure network tunneling tunneling-table rowadd remote-ip
PROXIM-MIB.tunnelConfigTTL	configure network tunneling tunneling-table rowadd ttl
PROXIM-MIB.tunnelConfigTableEntryStatus	configure network tunneling tunneling-table rowedit entry-status
PROXIM-MIB.pppoeStatus	configure network pppoe status
PROXIM-MIB.pppoeAuthProtocol	configure network pppoe authentication-protocol
PROXIM-MIB.pppoeLcpEchoInterval	configure network pppoe lcp-echo-interval
PROXIM-MIB.pppoeLcpEchoFailure	configure network pppoe lcp-echo-failure
PROXIM-MIB.pppoePreferredServiceName	configure network pppoe preferred-service-name
PROXIM-MIB.pppoeAccessConcentratorName	configure network pppoe access-concentrator-name
PROXIM-MIB.pppoeUserName	configure network pppoe user-name
PROXIM-MIB.pppoePassword	configure network pppoe password
PROXIM-MIB.pppoeSessionRestart	configure network pppoe session-restart
PROXIM-MIB.pppoeMPPEStatus	configure network pppoe mppe-status
PROXIM-MIB.pppoeMPPEStateless	configure network pppoe stateless-encrypt-mode
PROXIM-MIB.pppoeMPPEKeyLength	configure network pppoe mppe-key-length
PROXIM-MIB.netLinkAvlCheckStatus	configure network link-availability status
PROXIM-MIB.netLinkAvlPollingTime	configure network link-availability polling-time
PROXIM-MIB.netLinkAvlOfflinePollingTime	configure network link-availability offline-polling-time
PROXIM-MIB.netLinkAvlPollingRetries	configure network link-availability polling-retries
PROXIM-MIB.netLinkAvlServerEntryStatus	configure network link-availability link-availability-tbl rowadd entry-status
PROXIM-MIB.netLinkAvlServerInetAddress	configure network link-availability link-availability-tbl rowadd inet-address
PROXIM-MIB.netLinkAvlServerComment	configure network link-availability link-availability-tbl rowadd comment
PROXIM-MIB.netLinkAvlServerEntryStatus	configure network link-availability link-availability-tbl rowedit entry-status
PROXIM-MIB.netLinkAvlServerInetAddress	configure network link-availability link-availability-tbl rowedit inet-address
PROXIM-MIB.netLinkAvlServerComment	configure network link-availability link-availability-tbl rowedit comment
PROXIM-MIB.netIpStaticRouteTableEntryStatus	configure network static-routes static-route-table rowedit entry-status
PROXIM-MIB.netIpStaticRouteTableEntryStatus	configure network static-routes static-route-table rowadd entry-status
PROXIM-MIB.netIpStaticRouteDestAddr	configure network static-routes static-route-table rowadd destination-address
PROXIM-MIB.netIpStaticRouteMask	configure network static-routes static-route-table rowadd route-mask

MIB Name	CLI Command
PROXIM-MIB.netIpStaticRouteNextHop	configure network static-routes static-route-table rowadd route-next-hop
PROXIM-MIB.netIpStaticRouteMetric	configure network static-routes static-route-table rowadd metric
PROXIM-MIB.netCfgStaticRouteStatus	configure network static-routes static-route-status
PROXIM-MIB.macaclOperationType.1	configure security macacl operation-type
PROXIM-MIB.macaclAddrTableEntryStatus	configure security macacl address-table rowadd secondary-index entry-status
PROXIM-MIB.macaclAddrTableMACAddress	configure security macacl address-table rowadd secondary-index mac-address
PROXIM-MIB.macaclAddrComment	configure security macacl address-table rowadd secondary-index comment
PROXIM-MIB.macaclAddrTableMACAddress	configure security macacl address-table rowedit secondary-index mac-address
PROXIM-MIB.macaclAddrComment	configure security macacl address-table rowedit secondary-index comment
PROXIM-MIB.macaclAddrTableEntryStatus	configure security macacl address-table rowedit secondary-index entry-status
PROXIM-MIB.radiusSrvInetADDR	configure security radius server-table rowedit secondary-index ipaddress
PROXIM-MIB.radiusSrvServerPort	configure security radius server-table rowedit secondary-index port
PROXIM-MIB.radiusSrvProfileServerSharedSecret	configure security radius server-table rowedit secondary-index shared-secret
PROXIM-MIB.radiusSrvProfileTableEntryStatus	configure security radius server-table rowedit secondary-index entry-status
PROXIM-MIB.radiusSupProfileName	configure security radius supported-table rowedit profile-name
PROXIM-MIB.radiusSupProfileMaxReTransmissions	configure security radius supported-table rowedit max-retransmissions
PROXIM-MIB.radiusSupProfileMsgResponseTime	configure security radius supported-table rowedit msg-response-time
PROXIM-MIB.radiusSupProfileReAuthenticationPeriod	configure security radius supported-table rowedit re-authentication
PROXIM-MIB.radiusSupProfileTableEntryStatus	configure security radius supported-table rowedit entry-status
PROXIM-MIB.sysMgmtCfgCommit	configure commit
PROXIM-MIB.sysMgmtReboot	configure reboot
PROXIM-MIB.dhcpServerStatus	configure dhcp server-status
PROXIM-MIB.dhcpMaxLeasePeriod	configure dhcp max-lease-time
PROXIM-MIB.dhcpServerNetMask	configure dhcp server-interface-table rowedit net-mask
PROXIM-MIB.dhcpServerDefaultGateway	configure dhcp server-interface-table rowedit default-gateway
PROXIM-MIB.dhcpServerPrimaryDNS	configure dhcp server-interface-table rowedit primary-dns
PROXIM-MIB.dhcpServerSecondaryDNS	configure dhcp server-interface-table rowedit secondary-dns
PROXIM-MIB.dhcpServerDefaultLeasePeriod	configure dhcp server-interface-table rowedit default-leasetime
PROXIM-MIB.dhcpServerIfTableComment	configure dhcp server-interface-table rowedit comment
PROXIM-MIB.dhcpServerIfTableEntryStatus	configure dhcp server-interface-table rowedit entry-status

MIB Name	CLI Command
PROXIM-MIB.dhcpServerIpPoolTableEntryStatus	configure dhcp server-ippool-table rowadd entry-status
PROXIM-MIB.dhcpServerIpPoolInterface	configure dhcp server-ippool-table rowadd interface-type
PROXIM-MIB.dhcpServerIpPoolStartIpAddress	configure dhcp server-ippool-table rowadd start-ipaddress
PROXIM-MIB.dhcpServerIpPoolEndIpAddress	configure dhcp server-ippool-table rowadd end-ipaddress
PROXIM-MIB.dhcpServerIpPoolInterface	configure dhcp server-ippool-table rowedit interface-type
PROXIM-MIB.dhcpServerIpPoolStartIpAddress	configure dhcp server-ippool-table rowedit start-ipaddress
PROXIM-MIB.dhcpServerIpPoolEndIpAddress	configure dhcp server-ippool-table rowedit end-ipaddress
PROXIM-MIB.dhcpServerIpPoolTableEntryStatus	configure dhcp server-ippool-table rowedit entry-status
PROXIM-MIB.dhcpRelayServerTableEntryStatus	configure dhcp dhcp-relay server-table rowadd entry-status
PROXIM-MIB.dhcpRelayServerIpAddress	configure dhcp dhcp-relay server-table rowadd ipaddress
PROXIM-MIB.dhcpRelayServerIpAddress	configure dhcp dhcp-relay server-table rowedit ipaddress
PROXIM-MIB.dhcpRelayServerTableEntryStatus	configure dhcp dhcp-relay server-table rowedit entry-status
PROXIM-MIB.ethernetIfTxModeAndSpeed	configure ethernet rowedit txmodeandspeed
PROXIM-MIB.ethernetIfAdminStatus	configure ethernet rowedit eth-admin-status
PROXIM-MIB.ethernetIfAutoShutDown	configure ethernet rowedit ethernet-autoshutdown
PROXIM-MIB.sysTypeMode	configure radio-mode interface radio-mode
PROXIM-MIB.sysTypeFreqDomainOrCountryCode	configure system-configure radio frequency-domain
PROXIM-MIB.sysConfMaxMTUSupport	configure system-configure max-mtu
PROXIM-MIB.sysPacketForwardingMode	configure system-configure network-mode
PROXIM-MIB.sysMgmtMode	configure system-configure controller-status
PROXIM-MIB.sysApplicationType	configure system-configure application-type
PROXIM-MIB.sysLEDStackStatus	configure system-configure led-display led-status
PROXIM-MIB.sysLEDStackSUMACAddr	configure system-configure led-display su-wirless-mac-adrs
PROXIM-MIB.sysDeliverPowerOverEthernet	configure system-configure deliver-power-over-ethernet
PROXIM-MIB.worpQoSPIRMacTableEntryStatus	configure worp-qos pir-mac-list rowadd entry-status
PROXIM-MIB.worpQoSPIRMacAddr	configure worp-qos pir-mac-list rowadd mac-address
PROXIM-MIB.worpQoSPIRMacMask	configure worp-qos pir-mac-list rowadd mac-mask
PROXIM-MIB.worpQoSPIRMacComment	configure worp-qos pir-mac-list rowadd comment
PROXIM-MIB.worpQoSPIRMacAddr	configure worp-qos pir-mac-list rowedit mac-address
PROXIM-MIB.worpQoSPIRMacMask	configure worp-qos pir-mac-list rowedit mac-mask
PROXIM-MIB.worpQoSPIRMacComment	configure worp-qos pir-mac-list rowedit comment
PROXIM-MIB.worpQoSPIRMacTableEntryStatus	configure worp-qos pir-mac-list rowedit entry-status
PROXIM-MIB.worpQoSPIRIPTableEntryStatus	configure worp-qos pir-ip-list rowadd entry-status
PROXIM-MIB.worpQoSPIRIPAddr	configure worp-qos pir-ip-list rowadd ip-address
PROXIM-MIB.worpQoSPIRIPSubMask	configure worp-qos pir-ip-list rowadd subnet-mask
PROXIM-MIB.worpQoSPIRIPComment	configure worp-qos pir-ip-list rowadd comment

MIB Name	CLI Command
PROXIM-MIB.worpQoSPIRIPAddr	configure worp-qos pir-ip-list rowedit ip-address
PROXIM-MIB.worpQoSPIRIPSubMask	configure worp-qos pir-ip-list rowedit subnet-mask
PROXIM-MIB.worpQoSPIRIPComment	configure worp-qos pir-ip-list rowedit comment
PROXIM-MIB.worpQoSPIRIPTableEntryStatus	configure worp-qos pir-ip-list rowedit entry-status
PROXIM-MIB.worpQoSPIRPortTableEntryStatus	configure worp-qos pir-port-list rowadd entry-status
PROXIM-MIB.worpQoSPIRStartPort	configure worp-qos pir-port-list rowadd start-port
PROXIM-MIB.worpQoSPIREndPort	configure worp-qos pir-port-list rowadd end-port
PROXIM-MIB.worpQoSPIRPortComment	configure worp-qos pir-port-list rowadd comment
PROXIM-MIB.worpQoSPIRStartPort	configure worp-qos pir-port-list rowedit start-port
PROXIM-MIB.worpQoSPIREndPort	configure worp-qos pir-port-list rowedit end-port
PROXIM-MIB.worpQoSPIRPortComment	configure worp-qos pir-port-list rowedit comment
PROXIM-MIB.worpQoSPIRPortTableEntryStatus	configure worp-qos pir-port-list rowedit entry-status
PROXIM-MIB.worpQoSPIRMapSrcMacIndexList	configure worp-qos pir-map-list rowedit src-mac-index-list
PROXIM-MIB.worpQoSPIRMapDstMacIndexList	configure worp-qos pir-map-list rowedit dst-mac-index-list
PROXIM-MIB.worpQoSPIRMapSrcIpAddrIndexList	configure worp-qos pir-map-list rowedit src-ip-index-list
PROXIM-MIB.worpQoSPIRMapDstIpAddrIndexList	configure worp-qos pir-map-list rowedit dst-ip-index-list
PROXIM-MIB.worpQoSPIRMapSrcPortIndexList	configure worp-qos pir-map-list rowedit src-port-index-list
PROXIM-MIB.worpQoSPIRMapDstPortIndexList	configure worp-qos pir-map-list rowedit dst-port-index-list
PROXIM-MIB.worpQoSPIRTableEntryStatus	configure worp-qos pir-list rowadd entry-status
PROXIM-MIB.worpQoSPIRRuleName	configure worp-qos pir-list rowadd pir-name
PROXIM-MIB.worpQoSPIRIPToSLow	configure worp-qos pir-list rowadd tos-low
PROXIM-MIB.worpQoSPIRIPToSHigh	configure worp-qos pir-list rowadd tos-high
PROXIM-MIB.worpQoSPIRIPToSMask	configure worp-qos pir-list rowadd tos-mask
PROXIM-MIB.worpQoSPIRIPProtocolIds	configure worp-qos pir-list rowadd protocol-ids
PROXIM-MIB.worpQoSPIREtherPriorityLow	configure worp-qos pir-list rowadd ether-priority-low
PROXIM-MIB.worpQoSPIREtherPriorityHigh	configure worp-qos pir-list rowadd ether-priority-high
PROXIM-MIB.worpQoSPIRVlanId	configure worp-qos pir-list rowadd vlan-id
PROXIM-MIB.worpQoSPIREtherType	configure worp-qos pir-list rowadd ether-type
PROXIM-MIB.worpQoSPIREtherValue	configure worp-qos pir-list rowadd ether-value
PROXIM-MIB.worpQoSPIRRuleBitMask	configure worp-qos pir-list rowadd rule-bit-mask
PROXIM-MIB.worpQoSPIRPPPoEEncapsulation	configure worp-qos pir-list rowadd pppoe-encapsulation
PROXIM-MIB.worpQoSPIRPPPoEProtocolId	configure worp-qos pir-list rowadd pppoe-protocol-id
PROXIM-MIB.worpQoSPIRRuleBitMask	configure worp-qos pir-list rowadd tos-rule
PROXIM-MIB.worpQoSPIRRuleBitMask	configure worp-qos pir-list rowadd ether-priority-rule
PROXIM-MIB.worpQoSPIRRuleBitMask	configure worp-qos pir-list rowadd vlan-rule
PROXIM-MIB.worpQoSPIRRuleBitMask	configure worp-qos pir-list rowadd ether-type-rule

MIB Name	CLI Command
PROXIM-MIB.worpQoSPIRRuleName	configure worp-qos pir-list rowedit pir-name
PROXIM-MIB.worpQoSPIRIPToSLow	configure worp-qos pir-list rowedit tos-low
PROXIM-MIB.worpQoSPIRIPToSHigh	configure worp-qos pir-list rowedit tos-high
PROXIM-MIB.worpQoSPIRIPToSMask	configure worp-qos pir-list rowedit tos-mask
PROXIM-MIB.worpQoSPIRIPProtocolIds	configure worp-qos pir-list rowedit protocol-ids
PROXIM-MIB.worpQoSPIREtherPriorityLow	configure worp-qos pir-list rowedit ether-priority-low
PROXIM-MIB.worpQoSPIREtherPriorityHigh	configure worp-qos pir-list rowedit ether-priority-high
PROXIM-MIB.worpQoSPIRVlanId	configure worp-qos pir-list rowedit vlan-id
PROXIM-MIB.worpQoSPIREtherType	configure worp-qos pir-list rowedit ether-type
PROXIM-MIB.worpQoSPIREtherValue	configure worp-qos pir-list rowedit ether-value
PROXIM-MIB.worpQoSPIRPPPoEEncapsulation	configure worp-qos pir-list rowedit pppoe-encapsulation
PROXIM-MIB.worpQoSPIRPPPoEProtocolId	configure worp-qos pir-list rowedit pppoe-protocol-id
PROXIM-MIB.worpQoSPIRRuleBitMask	configure worp-qos pir-list rowedit rule-bit-mask
PROXIM-MIB.worpQoSPIRTableEntryStatus	configure worp-qos pir-list rowedit entry-status
PROXIM-MIB.worpQoSSFClassTableEntryStatus	configure worp-qos sfc-list rowadd entry-status
PROXIM-MIB.worpQoSSFClassName	configure worp-qos sfc-list rowadd sfc-name
PROXIM-MIB.worpQoSSFClassSchedularType	configure worp-qos sfc-list rowadd schedular-type
PROXIM-MIB.worpQoSSFClassDirection	configure worp-qos sfc-list rowadd traffic-direction
PROXIM-MIB.worpQoSSFClassMIR	configure worp-qos sfc-list rowadd mir
PROXIM-MIB.worpQoSSFClassCIR	configure worp-qos sfc-list rowadd cir
PROXIM-MIB.worpQoSSFClassMaxLatency	configure worp-qos sfc-list rowadd max-latency
PROXIM-MIB.worpQoSSFClassTolerableJitter	configure worp-qos sfc-list rowadd tolerable-jitter
PROXIM-MIB.worpQoSSFClassTrafficPriority	configure worp-qos sfc-list rowadd traffic-priority
PROXIM-MIB.worpQoSSFClassNumOfMesgInBurst	configure worp-qos sfc-list rowadd max-msg-inburst
PROXIM-MIB.worpQoSSFClassMaxDemand	configure worp-qos sfc-list rowadd max-demand
PROXIM-MIB.worpQoSSFClassName	configure worp-qos sfc-list rowedit sfc-name
PROXIM-MIB.worpQoSSFClassSchedularType	configure worp-qos sfc-list rowedit schedular-type
PROXIM-MIB.worpQoSSFClassDirection	configure worp-qos sfc-list rowedit traffic-direction
PROXIM-MIB.worpQoSSFClassMIR	configure worp-qos sfc-list rowedit mir
PROXIM-MIB.worpQoSSFClassCIR	configure worp-qos sfc-list rowedit cir
PROXIM-MIB.worpQoSSFClassMaxLatency	configure worp-qos sfc-list rowedit max-latency
PROXIM-MIB.worpQoSSFClassTolerableJitter	configure worp-qos sfc-list rowedit tolerable-jitter
PROXIM-MIB.worpQoSSFClassTrafficPriority	configure worp-qos sfc-list rowedit traffic-priority
PROXIM-MIB.worpQoSSFClassNumOfMesgInBurst	configure worp-qos sfc-list rowedit max-msg-inburst
PROXIM-MIB.worpQoSSFClassMaxDemand	configure worp-qos sfc-list rowedit max-demand
PROXIM-MIB.worpQoSSFClassTableEntryStatus	configure worp-qos sfc-list rowedit entry-status

MIB Name	CLI Command
PROXIM-MIB.worpQoSClassTableEntryStatus	configure worp-qos class-list rowadd sfc-index pir-index entry-status
PROXIM-MIB.worpQoSClassSFCValue	configure worp-qos class-list rowadd sfc-index pir-index sfc-value
PROXIM-MIB.worpQoSClassPIRValue	configure worp-qos class-list rowadd sfc-index pir-index pir-value
PROXIM-MIB.worpQoSClassName	configure worp-qos class-list rowadd sfc-index pir-index class-name
PROXIM-MIB.worpQoSClassPriority	configure worp-qos class-list rowadd sfc-index pir-index pir-priority
PROXIM-MIB.worpQoSClassName	configure worp-qos class-list rowedit sfc-index pir-index class-name
PROXIM-MIB.worpQoSClassPriority	configure worp-qos class-list rowedit sfc-index pir-index pir-priority
PROXIM-MIB.worpQoSClassTableEntryStatus	configure worp-qos class-list rowedit sfc-index pir-index entry-status
PROXIM-MIB.worpQoSDefaultClass	configure worp-qos default-class
PROXIM-MIB.worpQoSL2BroadcastClass	configure worp-qos l2-broadcast-class
PROXIM-MIB.worpQoSConfiguration	configure worp-qos qos-config
PROXIM-MIB.igmpSnoopingGlobalStatus	configure igmp igmp-status
PROXIM-MIB.igmpMembershipAgingTimer	configure igmp member-aging-timer
PROXIM-MIB.igmpRouterPortAgingTimer	configure igmp port-aging-timer
PROXIM-MIB.igmpForcedFlood	configure igmp forced-flood
PROXIM-MIB.passpointProfileTableIndex	NA
PROXIM-MIB.passpointProfileName	NA
PROXIM-MIB.passpointProfileAccessNetworkType	NA
PROXIM-MIB.passpointProfileDomainName	NA
PROXIM-MIB.passpointProfileRealmList	NA
PROXIM-MIB.passpointProfileRoamingConsotiumListLen1	NA
PROXIM-MIB.passpointProfileRoamingConsotiumList1	NA
PROXIM-MIB.passpointProfile3GPPCellularNetworkCode1	NA
PROXIM-MIB.passpointProfileTableEntryStatus	NA
PROXIM-MIB.lldpStatus	configure lldp lldp-status
PROXIM-MIB.lldpTransmitInterval	configure lldp transmit-interval
PROXIM-MIB.lldpHoldTimeMultiplier	configure lldp hold-time-multiplier
PROXIM-MIB.httpsTLS1dot2only	configure management https high-secure-mode

Bootloader CLI and ScanTool A

The Bootloader CLI is a minimal subset of the normal CLI that is used to perform initial configuration of the device. The Bootloader CLI is available when the device embedded software is not running.

This interface is only accessible through the serial interface, and used when:

- The device does not contain a software image.
- An existing image is corrupted.
- An automatic (default) download of image over TFTP has failed.

The Bootloader CLI provides the ability to configure the initial setup parameters; and depending on this configuration, a software file is downloaded to the device during startup.

The Bootloader CLI supports the following commands.

- **factory_reset**: Restores the factory settings
- **help**: Prints online help
- **reboot**: Reboots the device
- **set**: Sets the parameters
- **show**: Shows the parameters

The Bootloader CLI supports the following parameters (for viewing and modifying).

- **ipaddr:** IP Address
- **systemname:** System Name
- **gatewayip:** Gateway IP Address
- **serverip:** Server IP Address
- **ipaddrtype:** IP Address Type
- **netmask:** Net Mask
- **filename:** Image file name (including the file extension)

If the Bootloader fails to load the firmware from flash, it tries to get the firmware from the network. While trying to get firmware from the network, the device should be powered on using Ethernet interface of the device. The default configuration of the Bootloader parameters are as follows:

Parameter	Value
ipaddr	169.254.128.132
netmask	255.255.255.0
gatewayip	169.254.128.132
systemname	systemname
serverip	169.254.128.133
filename	imagename
ipaddrtype	dynamic

To load the Firmware from the Network

Use the **show** command to view parameters and their value, and use the set command to set the parameters value.

To load the Firmware by using Dynamic IP Parameters

1. Set the ipaddrtype to dynamic

2. Run the BOOTP and TFTP Servers followed by device reboot

When the device reboots, the device gets the IP Address and Boot filename from the BOOTP server. You need not change any of the default Bootloader parameters. After BOOTP succeeds, the device initiates a TFTP request with the filename it gets from BOOTP.

To load the Firmware by using Static IP Parameters

1. Use the **set** command to set the IP parameters like 'ipaddr', 'serverip', 'filename' and also set the parameter 'ipaddrtype' to static.
2. Run the TFTP Server followed by device reboot.

When the device reboots, the TFTP request is initiated with the value taken from the parameter "filename". This request is sent to the IP address set as "serverip". In this case, the TFTP Server should be reachable to the device.

ScanTool

If you want to access the device with ScanTool, then the host running the ScanTool should also be in the same network as the device. The ScanTool broadcast requests are discarded by the routers if the device and the host running the ScanTool are in different networks. This means that the ScanTool cannot discover the device.

: In bootloader mode, Scan Tool will support only IPv4.

A device in Bootloader can be recognized by looking at the system description. If the system description does not contain any build number in braces, conclude that the device is in Bootloader mode.

For example:

MP-10100-BSU	- Description of the device
WD	- Regulatory Domain
v6.3.0	- Firmware Version
SN-SN000000000000121212	- Serial Number
BL-V1.0.4	- Bootloader version

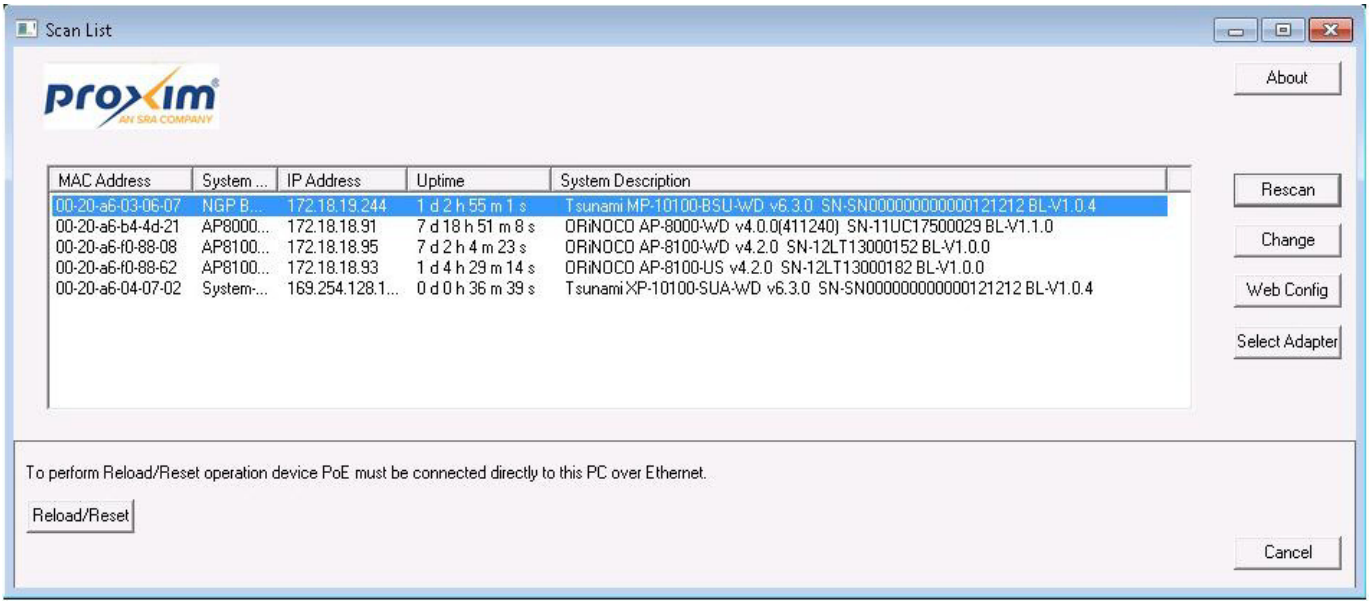


Figure 8-1 Scan Tool View of a Device in Bootloader Mode

Reset/Reload Procedure using ScanTool

For detailed Reset/Reload procedure using ScanTool refer **ScanTool Guide** available at http://support.proxim.com.

Parameters Requiring Reboot

B

Given below are the parameters that require the device to reboot.

Parameter(s)	Web Page(s)	Applicable Device Mode*
System Configuration		
Network Mode	ADVANCED CONFIGURATION -> System	All
Maximum MTU	ADVANCED CONFIGURATION -> System	All
Controller Status	ADVANCED CONFIGURATION -> System	All devices in Bridge Mode
Tunneling Status	ADVANCED CONFIGURATION -> Network -> IP Tunneling	All devices in Routing Mode
IP Configuration		
IP Configuration	BASIC CONFIGURATION	All
Ethernet	ADVANCED CONFIGURATION -> Network -> IP Configuration	All
IP Mode	ADVANCED CONFIGURATION -> Network -> IP Configuration	All
Default Gateway IP Address	BASIC CONFIGURATION ADVANCED CONFIGURATION -> Network -> IP Configuration	All
DNS	ADVANCED CONFIGURATION -> Network -> IP Configuration -> DNS	All devices in Bridge Mode
Wireless	ADVANCED CONFIGURATION -> Network -> IP Configuration	All devices in Routing Mode
Wireless (With PPPoE)	ADVANCED CONFIGURATION -> Network -> IP Configuration	SU in Routing Mode
Hotspot	ADVANCED CONFIGURATION -> Network -> Hotspot	AP
NAT		
Status	ADVANCED CONFIGURATION -> Network -> NAT	SU
Dynamic Start Port	ADVANCED CONFIGURATION -> Network -> NAT	SU
Dynamic End Port	ADVANCED CONFIGURATION -> Network -> NAT	SU
PPPoE		
Status	ADVANCED CONFIGURATION -> Network -> PPPoE Client	SU
Wireless Interface Properties		
Frequency Domain	BASIC CONFIGURATION -> Interface 1 ADVANCED CONFIGURATION -> Wireless -> Interface 1 -> Properties -> Basic	MP
Radio Mode	BASIC CONFIGURATION -> Interface 1 ADVANCED CONFIGURATION -> Wireless -> Interface 1 -> Properties -> Basic	MP
	BASIC CONFIGURATION -> Interface 2 ADVANCED CONFIGURATION -> Wireless -> Interface 2 -> Properties	AP

Parameter(s)	Web Page(s)	Applicable Device Mode*
Operation Mode	BASIC CONFIGURATION -> Interface 1 ADVANCED CONFIGURATION -> Wireless -> Interface 1 -> Properties -> Basic	MP
	BASIC CONFIGURATION -> Interface 2 ADVANCED CONFIGURATION -> Wireless -> Interface 2 -> Properties	AP
Country Code	BASIC CONFIGURATION -> Interface 2 ADVANCED CONFIGURATION -> Wireless -> Interface 2 -> Properties	AP
Channel Bandwidth		AP
Frequency Extension	ADVANCED CONFIGURATION -> Wireless -> Interface 2 -> 11n Properties	AP
RSSI Check Time	ADVANCED CONFIGURATION -> Wireless -> Interface 2 -> Properties	AP
Upgrade Firmware and Configuration		
Upgrade Firmware	MANAGEMENT -> File Management -> Upgrade Firmware	All
Upgrade Configuration	MANAGEMENT -> File Management -> Upgrade Configuration	All
Upgrade License	MANAGEMENT -> File Management -> Upgrade License	All
Upgrade Certificate	FILE MANAGEMENT -> Upgrade Certificate	All
Upgrade Certificate Authority	FILE MANAGEMENT -> Upgrade Certificate Authority	All
HTTP / HTTPS		
Admin Password	MANAGEMENT -> Services -> HTTP / HTTPS	All
Monitor Password		All
HTTP		All
HTTP Port		All
HTTPS		All
Telnet / SSH		
Admin Password	MANAGEMENT -> Services -> Telnet / SSH	All
Monitor Password		All
Telnet		All
Telnet Port		All
Telnet Sessions		All
SSH		All
SSH Port		All
SSH Sessions		All

Parameter(s)	Web Page(s)	Applicable Device Mode*
SNMP (If SNMP v1-v2c is enabled)		
SNMP	MANAGEMENT -> Services -> SNMP	All
Version		All
Read Password		All
Read / Write Password		All
SNMP Trap Host Table		All
SNMP (If SNMP v3 is enabled)		
SNMP	MANAGEMENT -> Services -> SNMP	All
Version		All
Security Level		All
Priv Protocol		All
Priv Password		All
Auth Protocol		All
Auth Password		All
SNMP Trap Host Table		All
Management Access Control		
Access Table Status	MANAGEMENT -> Access Control	All
Reset to Factory	MANAGEMENT -> Reset to Factory	All

* **BSU**: Refers to a Base Station mode.
SU: Refers to both SU and CPE mode.
AP: Refers to an Access Point devices.
QB: Refers to Point-to-Point devices.
MP: Refers to Point-to-Mulitpoint devices.
All: Refers to an Access Point, point-to-point and point-to-mulitpoint devices.

Warranty and Technical Support C

For Warranty and Technical Support Policy, please visit http://proxim.com/support.

10.1 Obtaining Technical Service and Support

If you are having trouble using the Proxim product, and require additional support to resolve your issue, please be ready to provide the following information before you contact the Proxim Technical Support team:

- Product information
  - Part number and serial number of the suspected faulty device
- Trouble/error information
  - Trouble/symptom being experienced
  - Activities completed to confirm fault
  - Network information (What kind of network are you using?)
  - Circumstances that preceded or led up to the error
  - Message or alarms viewed
  - Steps taken to reproduce the problem
- ServPak information (if a Servpak customer):
  - ServPak account number
- Registration information
  - If the product is not registered, date and location where you purchased the product

: Technical Support is free for the warranty period from the date of purchase.

10.2 Support Options

Proxim Customer Service Website Support

The Proxim Customer Service Website is available 7x24x365 at http://support.proxim.com.

On the Proxim Customer Service Website, you can access the following services:

- **Product Download Page**: Provides quick links to product firmware, software, and documentation downloads.
- **Proxim TV Links**: A link to helpful video tutorials.
- **Knowledgebase**: A solution database of all the resolved problems. You can search by product, category, keywords, or phrases.
- **Live Chat**: Chat with a support technician on-line or request to call back at a later time.
- **Create a Support Request**: Create a support request with our technical support staff who will reply to you by email.
- **Case Management**: Login to check the status of your support cases, update your personal profile, or access restricted information and features.
- **Provide Feedback**: Submit a suggestion, complaint, or other feedback about the support site and our products.

Telephone Support

Contact technical support via telephone as follows:

USA and Canada Customers

- **Phone**: +1-408-383-7700; +1-866-674-6626
- **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

International Customers

- **Phone**: +1-408-383-7700;
- **Business Hours**: 24x7 live response. Tier 3 support: 8 a.m. to 5 p.m. M-F PDT (UTC/GMT -7 hrs)

ServPak Support

To provide even greater investment protection, Proxim Wireless offers a cost-effective support program called ServPak. ServPak is a program of enhanced service support options that can be purchased as a bundle or individually, tailored to meet your specific needs. Whether your requirement is round the clock technical support or advance replacement service, we are confident that the level of support provided in every service in our portfolio will exceed your expectations.

All ServPak service bundles are sold as service contracts that provide coverage for specific products from 1 to 3 years. Servpak bundles are considered an upgrade to the standard product warranty and not an extension.

All Plans Include	ServPak Plus	ServPak Prime
24x7 Basic Technical Support	**Basic Advanced Replacement (Two business days/ International economy shipment service)**	**Priority Advanced Replacement (Next business day/ International priority shipment service)**
8x7 Advanced Technical Support		**24x7 Advanced Technical Support**
Software Maintenance		**Proxim Vision Support**

10.3 Additional Information on ServPak Options

Advanced Replacement of Hardware

In the event of a hardware failure, our guaranteed turnaround time for return to factory repair is 30 days or less. Customers who purchase this service are guaranteed replacement of refurbished or new hardware to be shipped out within one or two business days, as applicable. Options are available for shipment services depending on the customer's support needs. Hardware is shipped on business days, Monday – Friday excluding Holidays, 8:00 AM – 3:30 PM Eastern Time.

7x24x365 Availability

Unlimited, direct access to technical support engineers 24 hours a day, 7 days a week, 365 days a year including Holidays.

8x5 Availability

Unlimited, direct access to world-class technical support engineers 8 hours a day, 5 days a week, Monday through Friday from 8:00AM - 5:00PM Pacific Standard Time.

Basic Technical Support

Customers who purchase this service can be rest assured that their call will be answered by Proxim Tier 1 technical support and a case opened immediately to document the problem and provide initial troubleshooting to identify the solution and resolve the incident in a timely manner.

Advanced Technical Support

In addition to the Proxim Tier 1 technical support, customers will be able to have their more complex issues escalated to our Tier 3 technical support engineers. Our Tier 3 engineers will review specific configurations to troubleshoot intricate issues and will also provide helpful insights regarding Proxim products and various tips from decades of collective experience in the wireless industry.

Software Maintenance

It's important to maintain and enhance security and performance of wireless equipment and Proxim makes this easy by providing a Software Maintenance program that enables customers to access new feature and functionality rich software upgrades and updates. Customers will also have full access to Proxim vast Knowledgebase of technical bulletins, white papers and troubleshooting documents.

To purchase ServPak support services, please contact your authorized Proxim distributor. To receive more information or for questions on any of the available ServPak support options, please visit our website at http://www.proxim.com/support/servpak, call Proxim Support (For telephone numbers, see Telephone Support) or send an email to servpak@proxim.com.

Glossary

D

A	
Auto Channel Selection (ACS)	ACS scans all the available channels and chooses a low interference channel to establish a connection.

B	
Bridge	An interface connecting a local area network to another local area network that uses the same protocol (for example, wireless, Ethernet or token ring). Wireless bridges are commonly used to link buildings in campuses.
Broadcast	Broadcast traffic is a large series of broadcast packets (most often caused by wrong network configuration) that severely impact the network performance.
Broadband	In data communications, a "broadband connection" is a connection with a high speed of data transfer, fast enough to support a video streaming.

C	
Client IP Address Pool	This a pool of IP addresses from which the unit can assign IP addresses to clients, which perform a DHCP Request.
Cyclic Redundancy Check (CRC)	A cyclic redundancy check (CRC) is an error-detecting code commonly used in digital networks and storage devices to detect accidental changes to raw data. Blocks of data entering these systems get a short check value attached, based on the remainder of a polynomial division of their contents; on retrieval the calculation is repeated, and corrective action can be taken against presumed data corruption if the check values do not match.
CRC Errors	Cyclic redundancy check errors represents the number of packets received with invalid data. A high number of CRC errors can indicate a hidden node or co-channel interference.

D	
Domain Name Server (DNS)	A domain name server is an Internet service that translates domain names into IP addresses. For example, www.ietf.org is translated into 4.17.168.6.
Downstream / Downlink	Downstream means a data stream from the central part of the network to the end user. Also, refer **Upstream / Uplink**.
Dynamic Frequency Selection (DFS)	DFS helps you select the operating frequency that does not interfere with RADAR signals. This is accomplished by continuously detecting the range of operating frequencies with a RADAR interference.
Dynamic Host Configuration Protocol (DHCP)	Dynamic Host Configuration Protocol (DHCP) is a method to dynamically assign IP addresses. If DHCP is enabled, the device or computer broadcasts a request that is answered by a DHCP Server.
Dynamic IP address	An IP address assigned to a client, each time the client connects to the network. The dynamic IP address is configured by the DHCP server and can be different each time the client connects to the network.

D	
Decrypt Errors	Indicates the number of received packets that failed to decrypt.

E	
EIRP	Effective Isotropic Radiated Power that a radio antenna radiates.
Encryption	Encryption is a means of coding data with a key before sending it across a network. The same key must be used to decode the information at the receiver. This way, it prevents unauthorized access to the data that is sent across the network.
Encryption Key	An alphanumeric (letters and/or numbers) series that enables data to be encrypted and then decrypted, so it can be securely shared among members of the same network. WEP uses an encryption key that automatically encrypts outgoing wireless data. On the receiving side, the same encryption key enables the computer to automatically decrypt the information so it can be read.
End Point A (EPA)	The device near to ISP/deployer (local device) is EPA in a QB link.
End Point B (EPB)	The device near to the remote end is EPB in a QB link.
End Point B MAC Address	The MAC address of the device which needs to be linked.

F	
Frame Error Rate	Ratio of frame received with errors to total data received. It is used to determine the quality of a signal connection. If the Frame Error Rate is too high (too many errors), the connection may be dropped.

H	
HTTP	Hypertext Transfer Protocol (HTTP) is the protocol to transport Web pages. When you access the Internet with your browser, the HTTP protocol is used for data transport (http://www.proxim.com). When you access the unit by using the Web Interface, HTTP is used to transport the information. HTTPS is the Secure Hypertext Transfer Protocol.

I	
In Octets	In Octets specifies the total number of octets received on the wireless interface including framing characters.
Out Octets	Out Octets specifies the total number of octets transmitted out from the wireless interface including framing characters.

L	
LAN	A Local Area Network (LAN) is a network of limited size to which computers and devices can connect so that they can communicate with each other.

L	
License File	A license file is used to enable certain features of the unit. The unit already has a license file when it is shipped. When more features become available, you can purchase a license file and download it to the unit to enable these additional features.

M	
MAC Address	A MAC (Media Access Control) address is a globally unique network device address, which is hardware bound. It is used to identify a network device in a LAN. A MAC address is represented by six two-digit hexadecimal numbers (0 - 9 and A - F) separated by colons: for example 00:02:2D:47:1F:71 and 00:D0:AB:00:01:AC.
Management Information Base (MIB)	A Management Information Base (MIB) is a formal description of a set of network objects that can be managed with the Simple Network Management Protocol (SNMP). A MIB can be loaded by a management application so that it knows the unit specific objects.

N	
Network Name	Unique name to identify a wireless network. The devices in a pair should have a same network name.

P	
Pass Phrase	A text string used for WPA security on a wireless network. A passphrase may contain up to 8 to 64 alphanumeric characters, including spaces and other special characters.
Phy Errors	Physical errors represents number of frames received by the radio with data errors. High number of Phy errors indicates the interference in the wireless medium or low signal level.
Port Number	TCP and UDP provide an address mechanism, the port number, for identifying different applications communicating from the same IP address. Thus an active Web browser and an independently active mail program operating from the same IP location would typically use different port numbers so that packets are correctly delivered to specific applications.
Probe Request	A wireless client sends a probe request frame when it needs to obtain information from another wireless client or an access point. For example, a radio NIC would send a probe request to determine which access points are within range.
Probe Response	A wireless client or an access point will respond to the probe request with a probe response frame, containing capability information, supported data rates, etc.

R	
RADIUS Server	Remote Authentication Dial In User Service (RADIUS) is a client/server networking protocol that runs in the application layer, by using UDP as transport and provides centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. The RADIUS server is a background process that serves the following three functions: • To authenticate users or devices before granting them access to a network • To authorize those users or devices for certain network services • To account the users for usage of the provided services.
Router	Routers forward packets from one network to another based on routing information. A router uses a dynamic routing protocol like RIP or static routes to base its forwarding decision on.

S	
ScanTool	A Proxim tool which works from PC or laptop to discover or change the IP addresses of Proxim devices connected to the local network.
Simple Network Management Protocol (SNMP)	A protocol used for the communication between a network management application and the devices it is managing. The network management application is called the SNMP manager and the devices it manages will have SNMP agents. Not only the unit but also almost every network device contains a SNMP agent. The manageable objects of a device are arranged in a Management Information Base, also called MIB. The Simple Network Management Protocol (SNMP) allows managers and agents to communicate for accessing these objects.
Single-Band	Single-band refers to a device's ability to function only on one frequency band.
Spanning Tree Protocol (STP)	The Spanning Tree Protocol (STP) can be used to create redundant networks (“hot standby”) and to prevent loops. If enabled, spanning tree prevents loops by disabling redundant links. If a link fails, it can automatically enable a backup link.
SSH	A security protocol for logging into a remote server. SSH provides an encrypted session for transferring files and executing server programs.
SSL	Secure Socket Layer is a commonly used encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions.
SSID	A Service Set Identifier (also referred to as a network name) is a common name that identifies a wireless network. The identifier is attached to the wireless local area network (WLAN) and acts as an identifier when a device tries to connect to the system. A device will not be permitted to join the network unless it can provide the unique SSID. An SSID can be broadcast by the network router, allowing devices to detect it as an available network. An SSID does not supply security to the network
STP Frames	The data frames exchanged in an STP network topology are called as the STP Frames, BPDU frames being one of them.

S	
Subnet Mask/Network Mask	A subnet mask is a bit mask that defines which part of an IP address is used for the network part and which part for a host (computer) number. A subnet mask is like an IP address represented by four numbers in the range 0 - 255 separated by dots. When the IP address 172.17.23.14 has a subnet mask of 255.255.255.0, the network part is 172.17.23 and the host number is 14. See also IP address.
Syslog Server	Syslog Server receives, logs, displays, and forwards syslog messages from network devices like routers.

T	
Tagged Frames	When a frame enters the VLAN-aware area of the network, a tag is added to represent the VLAN membership of the frame's port or the port/protocol combination. These are called Tagged Frames.
TCP / IP	The TCP/IP internet-suite protocol describes a set of general design guidelines and implementations of specific networking protocols to enable computers to communicate over a network. TCP/IP provides end-to-end connectivity specifying how data should be formatted, addressed, transmitted, routed and received at the destination.
Telnet	Telnet is a network protocol used on the Internet or local area networks to access the command-line interface, on a remote host. Most network equipment and operating systems with a TCP/IP stack support a Telnet service for remote configuration.
Topology	Topology is the physical layout of network components (cable, wireless clients, gateways, hubs, and so on).
TPC	Transmit Power Control value applied by the device to adjust the transmit power radiated by the radio antenna.
Trap	Traps are alert messages sent by the SNMP agent, running within the device, to report significant events to the SNMP manager or TRAP receiver.
Trivial File Transfer Protocol (TFTP)	Trivial File Transfer Protocol (TFTP) is a lightweight protocol for transferring files that is like a simple form of File Transfer Protocol (FTP). A TFTP client is implemented on the unit. By using the upload and download commands, the unit can copy a file to or from a TFTP server.

U	
Unicast	Unicast transmission is the sending of messages to a single network destination identified by a unique address.
Untagged Frames	Untagged frames are frames which have no VLAN Id associated to it.
Upload	Uploading a file means copying a file from a network device to a remote server. In case of the unit, uploading means transferring a file from the unit to a TFTP server. See also download.
Upstream / uplink	Upstream means a data stream from the end users to the central part of the network. See also **Downstream / Downlink**.

V	
VLAN	The Virtual Local Area Network (VLAN) feature helps in logical grouping of network host on different physical LAN segments, which can communicate with each other as if they are all on the same physical LAN segment.

W	
WEP	The Wired Equivalent Privacy (WEP) algorithm is the standard encryption method used to protect wireless communication from eavesdropping.
Wireless Client / Station (STA)	A computer or program, connected to an access point network, that can access the wireless network, download files for manipulation, run applications, or request application-based services from a file server is called a wireless client or a wireless station (STA).
WLAN	A flexible data communication system implemented as an extension to or as an alternative for a wired LAN within a building or campus. By using electromagnetic waves, WLANs transmit and receive data over the air, minimizing the need for wired connections.
WPA	Wi-Fi Protected Access is a security standard based on IEEE 802.11i specification, that provides a high level of wireless network security. It uses data encryption through the Temporal Key Integrity Protocol (TKIP). TKIP scrambles the keys and ensures that the keys haven't been tampered with. User authentication is performed through the Extensible Authentication Protocol (EAP), to ensure that only authorized network users can access the network.