SIEMENS

RUGGEDCOM WIN v4.5

User Guide

For WIN7014, WIN7015, WIN7018, WIN7023, WIN7025, WIN7035, WIN7225, WIN7233, WIN7235, WIN7237, WIN7249, WIN7251, WIN7258

05/2016
RC1246-EN-02

Disclaimer Of Liability

Siemens has verified the contents of this document against the hardware and/or software described. However, deviations between the product and the documentation may exist.

Siemens shall not be liable for any errors or omissions contained herein or for consequential damages in connection with the furnishing, performance, or use of this material.

The information given in this document is reviewed regularly and any necessary corrections will be included in subsequent editions. We appreciate any suggested improvements. We reserve the right to make technical improvements without notice.

Registered Trademarks

RUGGEDCOM™ and ROS™ are trademarks of Siemens Canada Ltd..

Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Security Information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, machines, equipment and/or networks. They are important components in a holistic industrial security concept. With this in mind, Siemens' products and solutions undergo continuous development. Siemens recommends strongly that you regularly check for product updates.

For the secure operation of Siemens products and solutions, it is necessary to take suitable preventive action (e.g. cell protection concept) and integrate each component into a holistic, state-of-the-art industrial security concept. Third-party products that may be in use should also be considered. For more information about industrial security, visit http://www.siemens.com/industrialsecurity.

To stay informed about product updates as they occur, sign up for a product-specific newsletter. For more information, visit http://support.automation.siemens.com.

Warranty

Refer to the License Agreement for the applicable warranty terms and conditions, if any.

For warranty details, visit www.siemens.com/ruggedcom or contact a Siemens customer service representative.

Contacting Siemens

Address
Siemens Canada Ltd.
Industry Sector
300 Applewood Crescent
Concord, Ontario
Canada, L4K 5C7

Telephone
Toll-free: 1 888 264 0006
Tel: +1 905 856 5288
Fax: +1 905 856 1995

E-mail
ruggedcom.info.i-ia@siemens.com

Web
www.siemens.com/ruggedcom

Table of Contents

Preface

This guide describes v4.5 of the RUGGEDCOM WIN Web-based user interface and software application running on RUGGEDCOM WIN7000 and WIN7200 series WiMAX broadband wireless base stations. The WIN7000 and WIN7200 are members of the RUGGEDCOM family of mobile WiMAX broadband wireless access systems based on the 802.16e mobile WiMAX standard. This guide contains instructions and guidelines on how to use the base station software, as well as some general theory.

It is intended for use by network operators who are familiar with the operation of networks.

NOTE
Illustrations of the management interface screens are presented for illustrative purposes and may appear with minor differences in a working system.

Alerts

The following types of alerts are used when necessary to highlight important information.

DANGER!
DANGER alerts describe imminently hazardous situations that, if not avoided, will result in death or serious injury.

WARNING!
WARNING alerts describe hazardous situations that, if not avoided, may result in serious injury and/or equipment damage.

CAUTION!
CAUTION alerts describe hazardous situations that, if not avoided, may result in equipment damage.

IMPORTANT!
IMPORTANT alerts provide important information that should be known before performing a procedure or step, or using a feature.

NOTE
NOTE alerts provide additional information, such as facts, tips and details.

Related Documents

Other documents that may be of interest include:

- *RUGGEDCOM WIN7100 Series Installation Guides*
- *RUGGEDCOM WIN7200 Series Installation Guides*

- *RUGGEDCOM WIN v4.5 CPE User Guide*

System Requirements

Each workstation used to connect to the RUGGEDCOM WIN user interface must meet the following system requirements:

- Must have Windows XP, Windows 7 or Windows 8 installed.
- Must have the ability to configure an IP address and netmask on the computer's Ethernet interface.
- Must have a Web browser installed. Although other versions of these Web browsers may work, the following Web browsers have been tested at the time of release and verified as being compatible:
  - Microsoft Internet Explorer 11
  - Google Chrome 31 or 32
  - Mozilla Firefox 25 or 26
  - Apple Safari 5.1
  - Opera 18

Training

Siemens offers a wide range of educational services ranging from in-house training of standard courses on networking, Ethernet switches and routers, to on-site customized courses tailored to the customer's needs, experience and application.

Siemens' Educational Services team thrives on providing our customers with the essential practical skills to make sure users have the right knowledge and expertise to understand the various technologies associated with critical communications network infrastructure technologies.

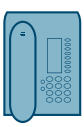
Siemens' unique mix of IT/Telecommunications expertise combined with domain knowledge in the utility, transportation and industrial markets, allows Siemens to provide training specific to the customer's application.

For more information about training services and course availability, visit www.siemens.com/ruggedcom or contact a Siemens sales representative.

Customer Support

Customer support is available 24 hours, 7 days a week for all Siemens customers. For technical support or general information, contact Siemens Customer Support through any of the following methods:

Online
Visit http://www.siemens.com/automation/support-request to submit a Support Request (SR) or check on the status of an existing SR.



Telephone
Call a local hotline center to submit a Support Request (SR). To locate a local hotline center, visit http://www.automation.siemens.com/mcms/aspa-db/en/automation-technology/Pages/default.aspx.

Mobile App
Install the Industry Online Support app by Siemens AG on any Android, Apple iOS or Windows mobile device and be able to:

- Access Siemens' extensive library of support documentation, including FAQs and manuals
- Submit SRs or check on the status of an existing SR
- Contact a local Siemens representative from Sales, Technical Support, Training, etc.
- Ask questions or share knowledge with fellow Siemens customers and the support community

1 Introduction

Welcome to the RUGGEDCOM WIN v4.5 User Guide for RUGGEDCOM WIN7000 and WIN7200 series base stations. This guide describes the wide array of features made available by the RUGGEDCOM WIN software. These features include:

- Intuitive user interface and parameter groupings
- Dashboard display for monitoring vital parameters
- Quick Start window customized for base stations in standalone or in ASN-GW topologies
- Quality of Service profile tools for standalone configuration
- Remote software upgrade and software management
- Advanced communication monitoring and troubleshooting tools

The RUGGEDCOM WIN software configures and controls RUGGEDCOM WIN7000 and WIN7200 base stations, and also configures Quality of Service (QoS) functions for individual subscriber stations. It provides browser-based Web access to a single RUGGEDCOM base station from any network connection.

Use the RUGGEDCOM WIN Web-based user interface to define initial communication parameters on the base station before you install the unit in the field. After installation, use the RUGGEDCOM WIN Web-based user interface to access the base station remotely to perform complete configuration, management, and monitoring functions.

The following sections provide more details about RUGGEDCOM WIN:

Section 1.1

Security Recommendations

To prevent unauthorized access to the device, note the following security recommendations:

Authentication

- Replace the default passwords for all user accounts and processes (where applicable) before the device is deployed.
- Use strong passwords. Avoid weak passwords such as password1, 123456789, abcdefgh, etc. An example of a strong password would be a password that contains at least eight characters, including a lowercase letter, an uppercase letter, a numeric character and a special character.
- Make sure passwords are protected and not shared with unauthorized personnel.
- Do not re-use passwords across different user names and systems, or after they expire.

- When RADIUS authentication is done remotely, make sure all communications are within the security perimeter or on a secure channel.

Physical/Remote Access

- SSL and SSH keys are accessible to users who connect to the device via the serial console. Make sure to take appropriate precautions when shipping the device beyond the boundaries of the trusted environment:
  - Replace the SSH and SSL keys with throwaway keys prior to shipping.
  - Take the existing SSH and SSL keys out of service. When the device returns, create and program new keys for the device.
- Use a AAA server whenever possible.
- Control access to the serial console.
- When using SNMP (Simple Network Management Protocol):
  - Limit the number of IP addresses that can connect to the device and change the community names.
  - Make sure the default community strings are changed to unique values.
- Limit the number of simultaneous Web Server and SSH sessions allowed.
- Configure remote system logging to forward all logs to a central location.
- Management of the configuration file, certificates and keys is the responsibility of the device owner. Before returning the device to Siemens for repair, make sure encryption is disabled (to create a cleartext version of the configuration file) and replace the current certificates and keys with temporary throwaway certificates and keys that can be destroyed upon the device's return.

Hardware/Software

- Make sure the latest firmware version is installed, including all security-related patches. For the latest information on security patches for Siemens products, visit the Industrial Security website [http://www.industry.siemens.com/topics/global/en/industrial-security/news-alerts/Pages/alerts.aspx] or the ProductCERT Security Advisories website [http://www.siemens.com/innovation/en/technology-focus/siemens-cert/cert-security-advisories.htm]. Updates to Siemens Product Security Advisories can be obtained by subscribing to the RSS feed on the Siemens ProductCERT Security Advisories website, or by following @ProductCert on Twitter.
- Use the latest Web browser version compatible with RUGGEDCOM WIN to make sure the most secure Transport Layer Security (TLS) versions and ciphers available are employed. Additionally, 1/n-1 record splitting is enabled in the latest web browser versions of Mozilla Firefox, Google Chrome and Internet Explorer, and mitigates against attacks such as SSL/TLS Protocol Initialization Vector Implementation Information Disclosure Vulnerability (e.g. BEAST).

Policy

- Periodically audit the device to make sure it complies with these recommendations and/or any internal security policies.
- Review the user documentation for other Siemens products used in coordination with the device for further security recommendations.

Section 1.2

WiMAX Overview

The following illustration details a typical WiMAX network architecture.

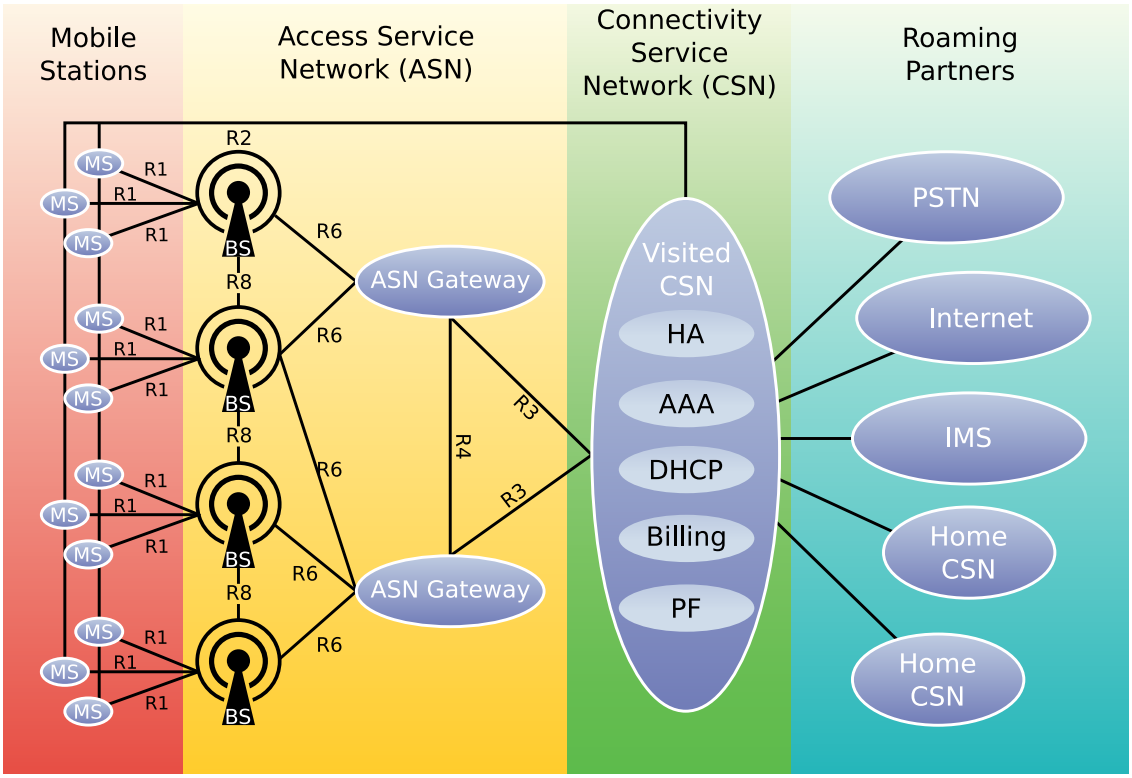


Figure 1: WiMAX Architecture

This table describes the connectivity between elements R1 through R8 shown in Figure 1:

Table: Interfaces for end-to-end WiMAX Network Architecture

Connection Type	Functions	Description
R1	Air interface	Interface between the MS and the ASN
R2	AAA, IP host configuration, mobility management	Interface between the MS and the CSN
R3	AAA, policy enforcement, mobility management	Interface between the ASN and the CSN
R4	Mobility management	Interface between ASNs
R5	Internet-working, roaming	Interfaces between CSNs
R6	IP tunnel management to establish/release MS connection, Radio Resource Management (RRM), QoS, mobility management	Interface between the base station and the ASN gateway
R8	Mobile management	Interface between base stations

The following entities and services are shown in Figure 1:

Entity/Service	Description
Home Agent (HA)	The Home Agent (HA) is a router that provides a subscriber unit's home IP address and knows how to find the subscriber in real-time. The HA provides two major functions: knowing the current location of the subscriber, and forwarding traffic to and from the subscriber's current location. The HA uses registration requests to update internal information about the subscriber's location (that is, the current IP address to be used to transmit and receive IP packets to and from that user). The HA interacts with the AAA to

Entity/Service	Description
	process authenticated Mobile IP registration requests, and to return Mobile IP registration responses. The HA also interacts with the ASN Gateway to receive subsequent Mobile IP registration requests. The HA may interact with other network elements in order to forward packets to the user's current location.
DHCP Server	The DHCP Server allocates IP addresses to the MS (mobile station). The DHCP Server may support multiple hosts behind an SS (for fixed/nomadic types of service), and also allow the operator to determine the IP address assigned to the SS and MS of its connected hosts.
Authentication, Authorization, and Accounting (AAA) Server	The AAA Server provides IP-based Authentication, Authorization, and Accounting (AAA) functions. For example, the AAA Server provides secure exchange and distribution of authentication credentials and session keys for data encryption. The WiMAX Forum specifies RADIUS (RFC 2865 and RFC 2866) as the AAA protocol used in its first standard release. Future standard releases will also include DIAMETER.
Application Servers	Application servers assist in providing multiple services to subscribers. For example, a VoIP softswitch and media gateways allow for Class 5 VoIP services, as well as for connectivity to the PSTN. In addition, video servers may be used to provide video-on-demand services.
ASN Gateway (ASN-GW)	The ASN-GW aggregates the base stations. The ASN-GW is responsible for SS and MS access control, IP connectivity, and traffic routing inside the ASN and with external networks. In addition, the ASN-GW provides security and mobility support in the ASN, and QoS support in the ASN with accordance with the core network. **NOTE** *RUGGEDCOM WIN supports an open R6 interface compatible with Cisco and Tellabs ASN gateways. The RUGGEDCOM WIN also supports a standalone mode. The standalone mode allows the creation of managed mobile networks without the need for an ASN gateway.*

Section 1.3
Standalone Mode

The RUGGEDCOM WIN system supports an operating mode called "standalone" mode. Standalone mode maintains R1interoperability with third party, but implements a layer 2 forwarding engine directly on the base station.

There is no need for an ASN gateway in standalone mode, but an AAA server is still required to enable authentication and encryption.

Section 1.4
About MIMO

Multiple Input, Multiple Output (MIMO) is a wireless technique to improve the range or throughput of the overall system. MIMO uses multiple radio transceivers transmitting and receiving at the same time and on the same frequency.

The RUGGEDCOM WIN series of base stations support both MIMO Matrix A and MIMO Matrix B. The system uses Link Adaptation to automatically select the optimal technique for a given subscriber, based on individual link conditions.

Section 1.4.1
MIMO Matrix A

MIMO Matrix A, also called STC (Space Time Coding), uses two antennas for transmitting and a single antenna for receiving.

In the first symbol time slot, the base station transmits two symbols, one from each antenna. The CPE receives the symbols as a mixture (note that each symbol has a different path to the CPE). In the second time slot, the base station transmits a variation on the same two symbols. The CPE uses both received signals from the first and second time slots to derive a processed signal with an effectively boosted SNR (signal-to-noise ratio).

This technique is combined with MRC (Maximum Ratio Combining), which is similar to STC but is applied to the receiving side. MRC uses one antenna for transmitting and two antennas for receiving.

Because the wave's path between the transmitting antenna and each receiving antennas is different (that is, multipath), the combined signal from the receiving antennas can be processed to derive a signal with a boosted SNR. Using this technique, the processed signal's SNR is boosted in comparison with a Single Input, Single Output (SISO) approach.

MIMO matrix A does not provide additional throughput over what a single antenna system would provide. Instead, MIMO is used to extend range. However, note that by extending range and providing a better link budget, it is possible to get better throughput at a given distance by being able to sustain a higher modulation rate.

Section 1.4.2
MIMO Matrix B

MIMO Matrix B uses two antennas for transmitting and for receiving. The transmitting antennas transmit independent symbols on each time slot. The received signals on each receiving antenna are a mixture of the transmitted signals. The original transmitted symbols are extracted using signal processing. This technique provides up to twice the throughput of a single antenna system.

Section 1.5
Quality-Of-Service and Service Flows

WiMAX can establish virtual over-the-air connections called "service flows". Service flows are mapped to traffic types through the use of classifiers, and are treated differently over the air by the system. Table "WiMAX Delivery Service Types" lists the different types delivery service of and the corresponding system behavior.

Table: WiMAX Delivery Service Types

Delivery Service	Meaning	Service definition	Service Flow parameters
BE	Best-Effort service	Intended for applications with no rate or delay requirements.	• Maximum Sustained Traffic Rate • Traffic Priority • Request/Transmission Policy
NRT-VR	Non real-time variable rate service	Intended for applications that require a guaranteed data rate, but that are insensitive to delays.	• Minimum Reserved Traffic Rate • Maximum Sustained Traffic Rate • Traffic Priority • Request/Transmission Policy

Delivery Service	Meaning	Service definition	Service Flow parameters
RT-VR	Real-Time Variable Rate service	Intended for real-time data applications with variable bit rates and guaranteed data rate and delay.	• Minimum Reserved Traffic Rate • Maximum Sustained Traffic Rate • Traffic Priority • Request/Transmission Policy • Maximum Latency
UGS	Unsolicited Grant Service	Intended for real-time applications generating fixed-rate data. Data can be provided as either fixed- or variable-length PDUs.	• Minimum Reserved Traffic Rate (equals Maximum Sustained Traffic Rate) • Traffic Priority • Request/Transmission Policy • Maximum Latency
ERT-VR	Extended Real-Time Variable Rate service	Intended for real-time applications with variable data rates and guaranteed data and delay. For example: VoIP with silence suppression.	• Minimum Reserved Traffic Rate • Maximum Sustained Traffic Rate • Traffic Priority • Request/Transmission Policy • Maximum Latency

2 Using WIN v4.5

This chapter describes how to use the RUGGEDCOM WIN interface. It describes the following tasks:

Section 2.1

Configuring Network Parameters in Windows

Network parameters in Microsoft Windows must be setup to allow a computer to connect to the RUGGEDCOM WIN. For instructions on how to configure the network parameters for other operating systems, refer to the user documentation for that operating system.

The device can be pre-configured in the lab, eliminating the need for configuration in the field. After installing a pre-configured device, configure additional parameters remotely through the wireless link.

NOTE
The following procedure describes how to configure the parameters using Microsoft Windows 7.

To configure the network parameters in Windows, do the following:

1. Make sure the PoE adapter is connected to the device.
2. Connect the computer’s Ethernet port to the PoE adapter's Ethernet port.
3. On the computer, click **Start** and select **Control Panel**.
4. In the **Control Panel**, select **Network and Sharing Center**.
5. Select **Local Area Connection**. The **Local Area Connections Status** dialog box appears.

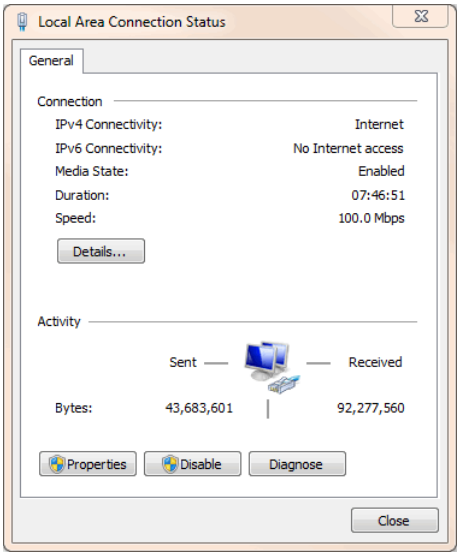


Figure 2: Microsoft Windows Local Area Connection Status Dialog Box

6. Click **Local Area Connection**. The **Local Area Connections Properties** dialog box appears with the **General** tab selected.

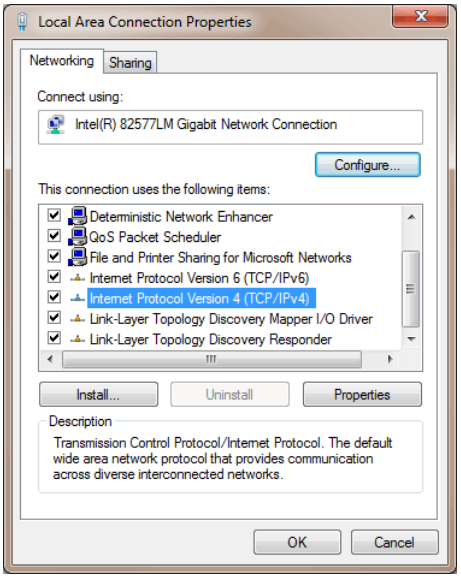


Figure 3: Windows Local Area Connection Properties Dialog Box

7. In the **Items** list, select **Internet Protocol (TCP/IP)** and then click **Properties**. The **Internet Protocol (TCP/IP) Properties** dialog box appears.

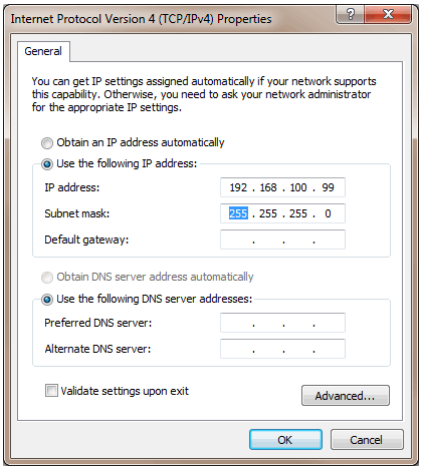


Figure 4: Windows TCP/IP Properties dialog

8. Assign the IP address `192.168.100.99` and the subnet `255.255.255.0`.
9. On the **Internet Protocol (TCP/IP) Properties** dialog box, click **OK**.
10. On the **Local Area Connection Properties** dialog box, click **OK**.
11. On the **Local Area Connection Status** dialog box, click **Close**.
12. Log in to the device to test the network settings. For more information, refer to Section 2.4, “Logging In”.

Section 2.2

Connecting to the Base Station

You can open a web session on the base station using two methods: the local method, and the remote method.

- Local web sessions are usually used during initial setup to provision the base station with an IP address and other basic parameters. Local sessions can be used whenever you have physical access to the base station. To open a local session, you need to connect the base station to a computer.
- Remote web sessions are used during normal operation after the unit is installed in a remote location. To open a remote session, you access the base station remotely through the network.

NOTE

To open a local session, your computer must be running Windows XP or higher.

Depending on your computer’s network interface, you will need an Ethernet cable or an Ethernet cross-cable. Network interfaces without automatic crossover detection need an Ethernet cross-cable to connect to the base station. Network interfaces with automatic crossover detection need a normal Ethernet cable to connect to the base station.

Section 2.3
Opening a Local Session

1. Connect an Ethernet cable to your computer and to the base station **DC/ETH** port.
2. Launch a web browser and type the base station default IP address in the address bar. The base station default IP address is **`https://192.168.100.100`**.

> **NOTE**
> *For information on browser versions and compatibility, refer to the release notes for your software version.*

3. Press **Enter**. The browser's security message appears.
4. Continue to the Web site. The **Login** window appears.

Section 2.4
Logging In

To log in to the device, do the following:

1. Launch a web browser and type **`https://192.168.100.100`** in the address parameter.

> **NOTE**
> *For information on browser versions and compatibility, refer to the section called "System Requirements".*

2. Press **Enter**. The browser's security message appears.
3. Continue to the Web site. The **Authentication Required** dialog box appears.

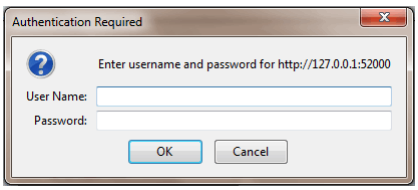


Figure 5: Authentication Required

> **NOTE**
> *The default user name is **admin**. The user name is case sensitive.*

4. In the **User Name** box, type a user name.

> **NOTE**
> *The default password is **generic**. The password is case sensitive.*

5. In the **Password** box, type a password.

NOTE
For instructions on how to navigate the management interface, refer to Section 2.9, "Using the Web-based User Interface".

6. Click **OK**. The RUGGEDCOM WIN management interface appears.

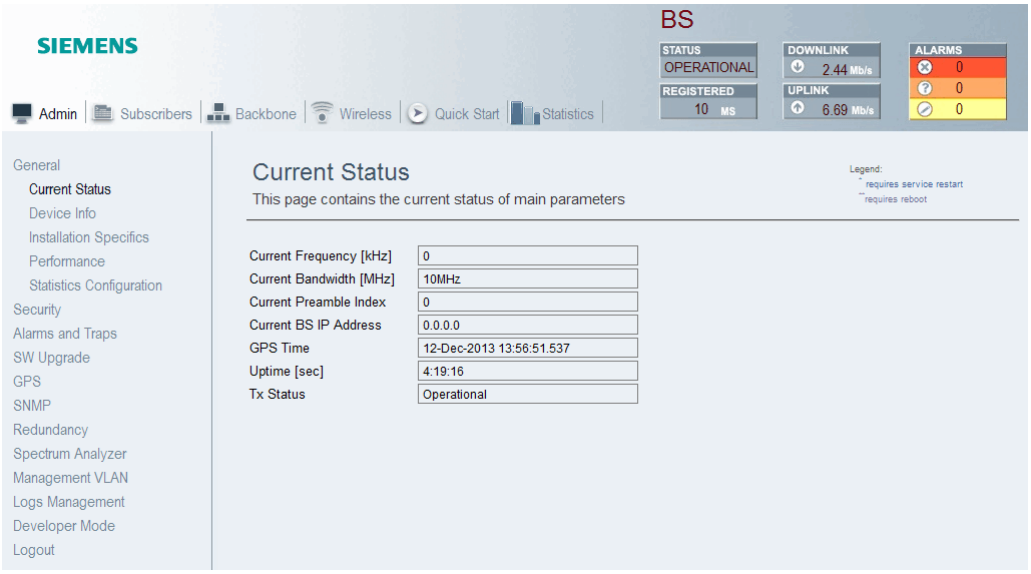


Figure 6: RUGGEDCOM WIN Management Interface

7. [Optional] If logging in for the first time, set the operating mode and initial configuration.

Section 2.5
Logging Out

To log out, do the following:

1. Navigate to ***Admin***. The **Current Status** screen appears.
2. In the options pane, click **Logout**. The **Web Logout** screen appears.

Figure 7: Logout Screen

3. Click **Logout**.

Section 2.6

Setting the Operating Mode

The base station supports two operation modes: Standalone and ASN-GW:

- In **Standalone** mode, the base station installation topology does *not* include an ASN Gateway, and Quality of Service functions are configured on the base station itself. For more information on Standalone mode, refer to the *Standalone Mode Application Note*. **Standalone** is the default operating mode.
- In **ASN-GW** mode, the base station installation topology includes an ASN gateway, and Quality of Service functions are configured through the gateway.

This section describes how to view and set the base station operating mode, and how to set the Quick Start settings for each mode.

Procedure: Viewing and setting the operating mode

1. Click **Backbone**. The **Mode Settings** pane appears.

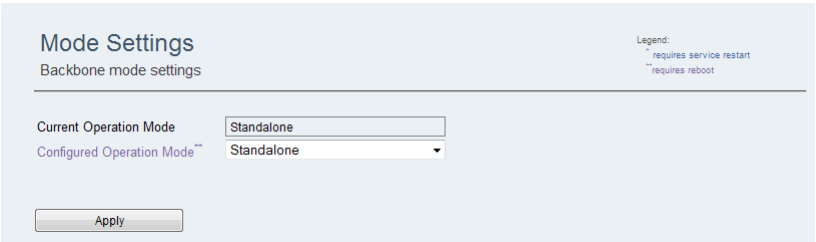


Figure 8: Mode Settings pane

2. View and set the operating mode in the following fields:

Parameter	Description
Current Operation Mode	**Synopsis:** { Standalone, ASN-GW } Displays the current base station operating mode.
Configured Operation Mode	**Synopsis:** { Standalone, ASN-GW } To change the operating mode, select a value from the list.

3. Click **Apply**.
4. If you changed the value in the **Configured Operation Mode** field, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

After setting the base station operating mode, you can configure the Quick Start settings. For more information, refer to either Section 2.8, “Standalone Mode Quick Start” or Section 2.7, “ASN-Gateway Mode Quick Start”.

Section 2.7

ASN-Gateway Mode Quick Start

Follow these instructions to configure the base station in ASN-GW mode.

The Quick Start pane provides the basic parameters required for setting up the base station in ASN-GW mode, including the base station address, ASN-GW address, frequency and bandwidth parameters, and the authentication mode.

NOTE
All parameters available in this pane are also available in other panes, corresponding to their parameter groups.

This pane also provides controls to reboot, stop, and start the base station service.

Procedure: Configuring ASN-GW Mode

1. Click **Quick Start**. The **Quick Start Settings** pane appears.

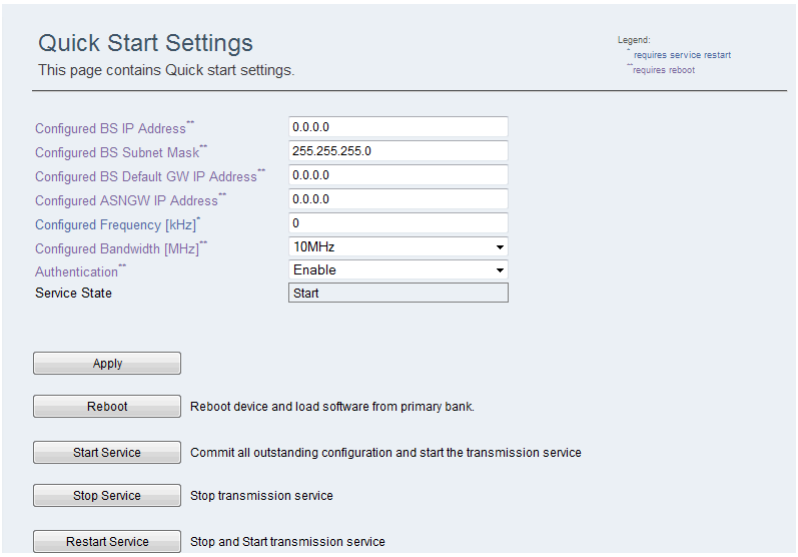


Figure 9: Quick Start pane: ASN-GW Mode

2. View and configure the base station parameters in the following fields:

Parameter	Description
Configured BS IP Address	Displays the currently configured base station IP address. To change the address, type an IPv4 address in this field.
Configured BS Subnet Mask	Displays the currently configured base station subnet mask.
Configured BS Default GW IP Address	Displays the currently configured base station default gateway IP address. To change the address, type an IPv4 address in this field.
Configured ASNGW IP Address	Displays the currently configured ASN gateway IP address. To change the address, type an IPv4 address in this field.
Configured Frequency [kHz]	Displays the currently configured base station broadcast frequency. To change the frequency, type a frequency (in kilohertz) in this field.
Configured Bandwidth [MHz]	**Synopsis:** { 3.5MHz, 5MHz, 7MHz, 10MHz } Displays the currently configured base station bandwidth. To change the bandwidth, select a value from the list.
Authentication	**Synopsis:** { Enable | Disable }

Parameter	Description
	Displays the current authentication status.
Service State	Displays the current state of the base station service.

3. Click **Apply**.
4. If you changed the value in the **Configured BS IP Address**, **Configured BS Subnet Mask**, **Configured BS Default GW IP Address**, **Configured ASNGW IP Address**, **Authentication** or **Configured Bandwidth [MHz]** fields, reboot the base station: click **Reboot**.
5. If you changed the value of the **Configured Frequency [kHz]** field, restart the base station service: click **Restart Service**.

NOTE
The parameters are not uploaded to the base station until you reboot or restart the base station service.

Section 2.8
Standalone Mode Quick Start

Follow these instructions to configure the base station in Standalone mode.

NOTE
All parameters available in this pane are also available in other panes, corresponding to their parameter groups.

The Quick Start pane provides the basic parameters required for setting up the base station in Standalone mode, including the base station address, the ASN gateway address, frequency, bandwidth, and authentication settings.

This pane also provides controls to reboot, stop, and start the base station service.

Procedure: Configuring Standalone Mode

1. Click **Quick Start**. The **Quick Start Settings** pane appears.

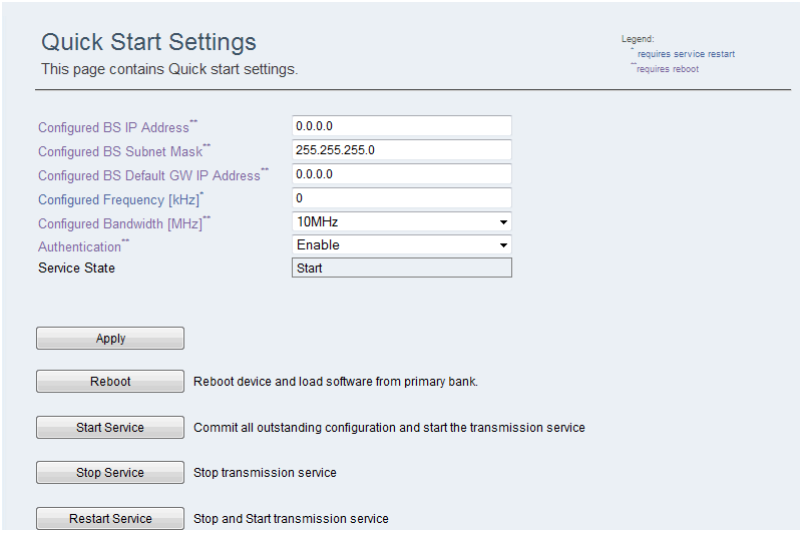


Figure 10: Quick Start pane: Standalone Mode

2. View and configure the base station parameters in the following fields:

Parameter	Description
Configured BS IP Address	Displays the currently configured base station IP address. To change the address, type an IPv4 address in this field.
Configured BS Subnet Mask	Displays the currently configured base station subnet mask.
Configured BS Default GW IP Address	Displays the currently configured base station gateway IP address. To change the gateway address, type an IPv4 address in this field.
Configured Frequency [kHz]	Displays the currently configured base station broadcast frequency. To change the frequency, type a frequency (in hertz) in this field.
Configured Bandwidth [MHz]	**Synopsis:** { 3.5MHz, 5MHz, 7MHz, 10MHz } Displays the currently configured base station bandwidth. To change the bandwidth, select a value from the list.
Authentication	**Synopsis:** { Enable | Disable } Displays the current authentication status.
Service State	Displays the current state of the base station service.

3. Click **Apply**.
4. If you changed the value in the any of the fields marked with **, reboot the base station: click **Reboot**.
5. If you changed the value of the **Configured Frequency [kHz]** field, restart the base station service: click **Restart Service**.

NOTE
The parameters are not uploaded to the base station until you reboot or restart the base station.

Section 2.9

Using the Web-based User Interface

Use the device's Web-based management interface to configure and control device settings and functions. Access the device's management interface through the device's LAN or RF IP address.

The management interface consists of three main areas:

- **Dashboard** – displays base station status information, including operational status, registered subscriber stations, downlink traffic, uplink traffic, and alarm information. To view detailed status information, click on a status indicator.
- **Configuration Buttons** – a set of buttons providing access to configuration options. To select a group of configuration options, click a button.
- **Options Pane** – a set of links providing access to individual configuration panes. To select a specific configuration pane, click a link.
- **Display Pane** – displays fields and controls for configuration options and system information displays.

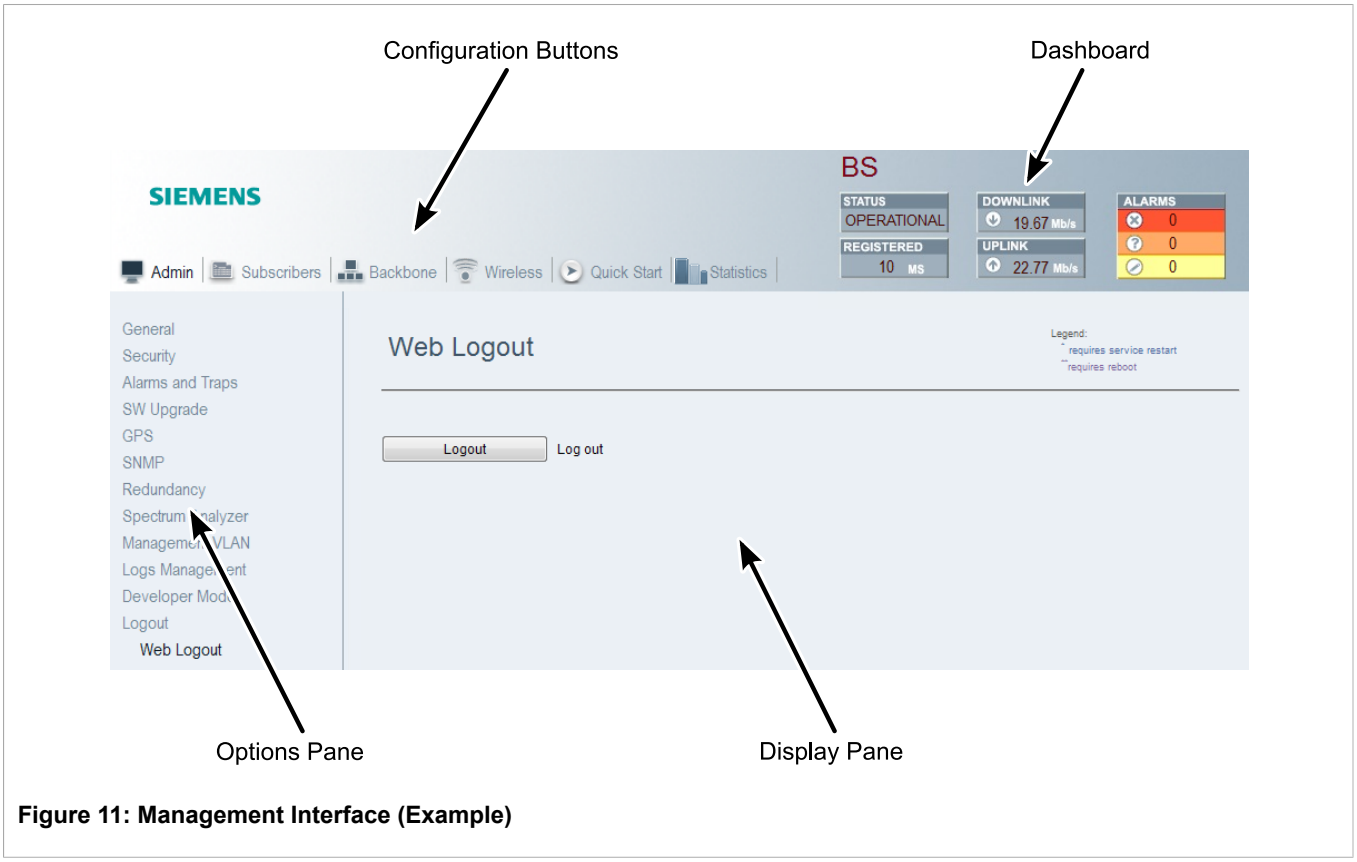


Figure 11: Management Interface (Example)

Section 2.9.1

Dashboard

The Dashboard appears at the top-right of the user interface at all times. The dashboard displays base station status information, including operational status, registered subscriber stations, downlink traffic, uplink traffic, and alarm information. To view detailed status information, click on a status indicator.

Figure 12: Dashboard

Table: Dashboard Display

Dashboard Indicator	Description
Status	Displays the current transmitter status. Click to open the base station Main Status pane
Registered	Displays the number of registered subscriber stations. Click to open the Subscriber Management pane
Downlink	Displays the average rate of downlink traffic. Click to open the Aggregate Throughput Statistics pane.
Uplink	Displays the average rate of uplink traffic. Click to open the Aggregate Throughput Statistics pane.
Alarms	Displays the number of system alarms, categorized by severity:  = critical  = major  = minor Click to display the System Alarms pane.

Section 2.9.2

Configuration Buttons

The configuration buttons provide access to the main groups of configuration options. Clicking a button displays a set of links in the **Options pane**. Clicking a link in the options pane displays a screen where you can review and configure system parameters, or review system data.

Figure 13: Configuration Buttons

Configuration Button	Description	Option Pane Links
Admin	Access to general base station information and administrative settings.	General Security Alarms and Traps SW Upgrade GPS SNMP Redundancy Spectrum Analyzer Logs Management Developer Mode

Configuration Button	Description	Option Pane Links
		Logout
Subscribers	Management of registered and provisioned subscriber stations and services (such as VLAN) in Standalone mode.	Subscriber Management Services
Backbone	Displays and sets the operation mode (Standalone or ASN-GW), and configures base station and gateway IP addresses. For *Standalone* mode, defines Switching parameters. For *ASN-GW* mode, defines ASN-GW parameters.	Backbone Admin Switching Backhaul
Wireless	Displays and sets WiMAX parameters and diagnostics options.	Wireless Admin Radio and Frame Wireless Security MAC Diagnostics
Quick Start	Displays and sets initial system setup parameters. Also provides controls to start and stop the base station service and to reboot the base station.	*Quick Start Menu*
Statistics	Displays Base Station and Customer Premises Equipment statistics, including Ethernet Counters, Traffic Statistics, and Subscriber Station statistics.	BS Statistics CPE Statistics

The configuration buttons provide access to the main groups of configuration options. Clicking a button displays a set of links in the **Options pane**. Clicking a link in the options pane displays a screen where you can review and configure system parameters, or review system data.

Figure 14: Configuration Buttons

Configuration Button	Description	Option Pane Links
Admin	Access to general base station information and administrative settings.	General Security Alarms and Traps SW Upgrade GPS SNMP Redundancy Spectrum Analyzer Logs Management Developer Mode Logout
Subscribers	Management of registered and provisioned subscriber stations and services (such as VLAN) in Standalone mode.	Subscriber Management Services
Backbone	Displays and sets the operation mode (Standalone or ASN-GW), and configures base station and gateway IP addresses.	Backbone Admin Switching Backhaul

Configuration Button	Description	Option Pane Links
	For *Standalone* mode, defines Switching parameters. For *ASN-GW* mode, defines ASN-GW parameters.	
Wireless	Displays and sets WiMAX parameters and diagnostics options.	Wireless Admin Radio and Frame Wireless Security MAC Diagnostics
Quick Start	Displays and sets initial system setup parameters. Also provides controls to start and stop the base station service and to reboot the base station.	*Quick Start Menu*
Statistics	Displays Base Station and Customer Premises Equipment statistics, including Ethernet Counters, Traffic Statistics, and Subscriber Station statistics.	BS Statistics CPE Statistics

Section 2.10

Accessing Developer Mode

To access developer mode, do the following:

NOTE

- *Developer mode is only available to developers for advanced troubleshooting purposes.*
- *Developers cannot access the device without logging into the system first.*

IMPORTANT!

The developer mode password is provided by Siemens. To obtain password, contact Siemens Custom Support.

1. Navigate to ***Admin*** » ***Developer Mode***. The **Developer Mode** screen appears.

Figure 15: Developer Mode Screen

2. In the **Password** box, type the password for developer mode.

   The status of the password appears in the **Status** box. If the password is correct, the message `Correct Password` appears.

3. Click **Apply**.

Section 2.11
Diagnostic Tools

The following sections describe how to use the diagnostic tools available within RUGGEDCOM WIN:

- Section 2.11.1, “Ping Diagnostic Tool”
- Section 2.11.2, “Trace Route Diagnostic Tool”

Section 2.11.1
Ping Diagnostic Tool

The **Ping** pane allows you to ping a specified IP address. The **Result** field indicates if the ping is successful or not.

Procedure: Using Ping

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Diagnostics** link and then click the **Ping** link. The **Ping** pane appears.

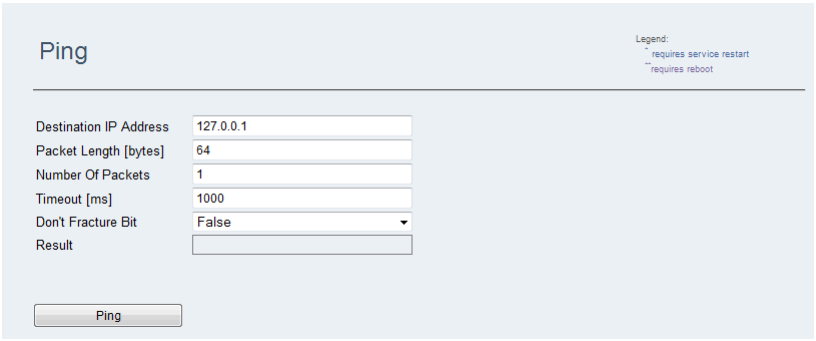


Figure 16: Ping pane

3. Set the ping parameters in the following fields:

Parameter	Description
Destination IP Address	Type the IP address to which you want to send the ping request. The default is 127.0.0.1.
Packet Length [bytes]	Type a value for ping request packet size. The default is 64.
Number Of Packets	Type a value for the number of packets in the ping request. The default is 1.
Timeout [ms]	Type a value, in milliseconds, for the ping request timeout. The default is 1000 ms (1 second).
Don't Fracture Bit	Select a value to enable or disable ping fragmentation. When set to False, ping fragmentation is disabled. When set to True, ping fragmentation is enabled. The default is False.
Result	Displays the result of the ping request.

4. To launch the ping request, click **Ping**.

Section 2.11.2

Trace Route Diagnostic Tool

The **Trace Route** pane allows you to to perform a trace route to a specified IP address. The **Diagnostic Result** field indicates if the trace route operation is successful or not.

Procedure: Using Trace Route

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Diagnostics** link and then click the **Trace Route** link. The **Trace Route** pane appears.

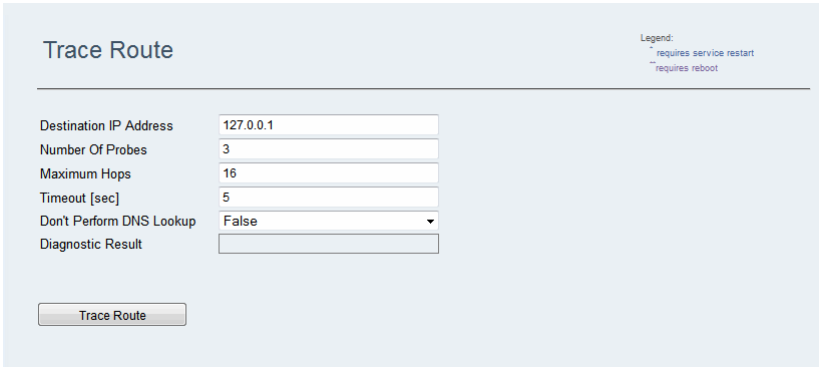


Figure 17: Trace Route pane

3. Set the trace route parameters in the following fields:

Parameter	Description
Destination IP Address	Type the IP address that you want to probe. The default is 127.0.0.1.
Number of Probes	Type a value to set the number of trace route probes. The default is 3.
Maximum Hops	Type a value to set the maximum number of hops. The default is 16.
Timeout [sec]	Type a value, in seconds, for the trace route timeout. The default is 5 seconds.
Don't Perform DNS Lookup	Select a value to enable or disable DNS lookup. When set to False, DNS lookup is performed as part of the trace route operation. When set to True, DNS lookup is not performed as part of the trace route operation. The default is False.
Diagnostic Result	Displays the result of the trace route operation.

4. To launch the trace route operation, click **Trace Route**.

3 Device Management

This chapter describes how to configure and manage the device and its components, such as device hardware, logs, files and more. It describes the following tasks:

Section 3.1

Base Station General Information

The **Current Status**, **Device Info**, and **Installation Description** panes display general base station information, including current base station status, device information, and physical installation information.

Section 3.1.1

Current Status

The **Current Status** pane displays general base station communication and configuration information. The **Current Status** pane is read-only; there are no parameters to set on this pane.

Procedure: Viewing current status information

1. Click **Admin**. The **Current Status** pane appears.

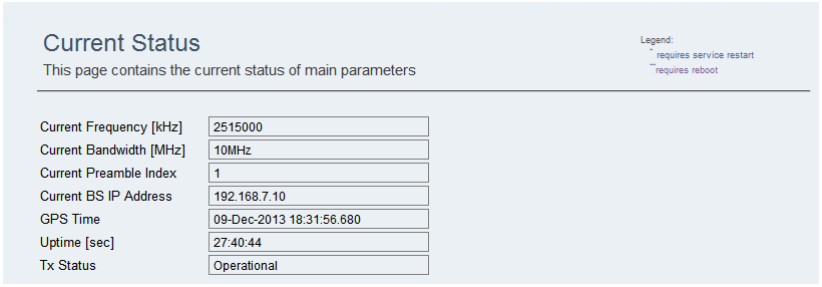


Figure 18: Current Status pane

2. The **Current Status** pane displays the following information:

Parameter	Description
Current Frequency [kHz]	Displays the base station frequency, in kHz.
Current Bandwidth [MHz]	**Synopsis:** { 3.5MHz, 5MHz, 7MHz, 10MHz } Displays the base station operating bandwidth, in Mhz.
Current Preamble Index	**Synopsis:** { 0 to 113 } **Default:** 0 Displays the base station preamble index. The preamble index is used by the subscriber station for frequency and time synchronization. Neighboring base stations must have unique preamble index values.
Current BS IP Address	Displays the base station IP address.
Current ASN-GW IP Address	Displays the ASN-GW IP address.
GPS Time	Displays the current UTC date and time from the base station's built-in GPS receiver.
Uptime [Hr:Min:Sec]	Displays the time, in hours, minutes, and seconds, since the last system restart.
Tx Status	**Synopsis:** { Radio Off, Operational } Displays the base station RF transmitter status.

Section 3.1.2
Device Information

The **Device Info** pane displays base station hardware information. The **Device Info** pane is read-only; there are no parameters to set on this pane.

Procedure: Viewing device information

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **Device Info** link. The **Device Info** pane appears.

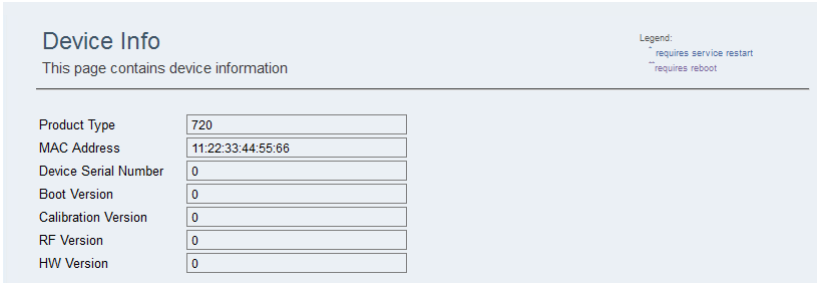


Figure 19: Device Info pane

3. The **Device Info** pane displays the following information:

Parameter	Description
Product Type	Displays the base station four-digit product type: • 7000 series are "Compact" base stations • 7200 series are "Pico" base stations The last two digits indicate the frequency band. For example, 7235 represents a 3.5GHz Pico base station.
MAC Address	Displays the base station MAC address.
Device Serial Number	Displays the base station serial number.
Boot Version	Displays the base station boot loader software version.
Calibration Version	Displays the base station calibration file version.
RF Version	Displays the base station RF hardware subsystem version.
HW Version	Displays the base station general hardware version.

Section 3.1.3
Installation Specifics

On the **Installation Specifics** pane, record the base station identification, installation, and contact information.

Procedure: Setting installation information

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **Installation Specifics** link. The **Installation Specifics** pane appears.

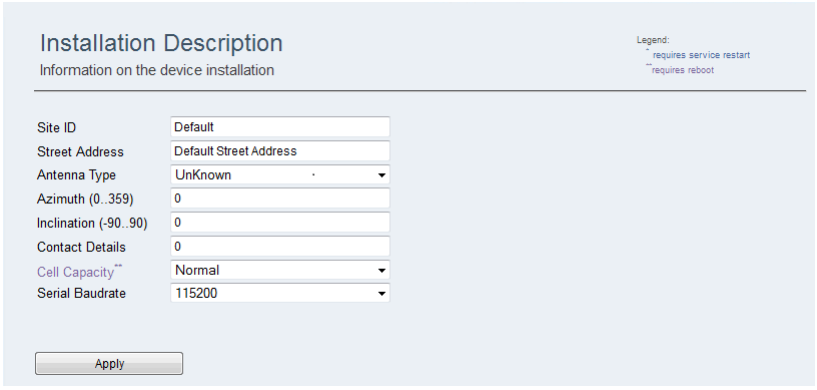


Figure 20: Installation Description pane

3. Review and set the installation information in the following fields:

Parameter	Description
Site ID [0..1000000]	**Synopsis:** { Unlimited } **Default:** Default The site identifier for the base station. Multiple base stations may share the same site identifier.

Parameter	Description
Street Address	The street address or physical location of the base station.
Antenna Type	**Synopsis:** { Omni, Directional, Unknown } **Default:** Unknown The type of antenna connected to the base station.
Azimuth [0..359]	**Synopsis:** { 0 to 359 } **Default:** 0 The antenna azimuth, in degrees.
Inclination [-90..90]	**Synopsis:** { -90 to 90 } **Default:** 0 The vertical inclination of the antenna, in degrees.
Contact Details	Installation and service personnel contact information.
Cell Capacity	**Synopsis:** { Normal, Large } The configuration parameter for networks larger than 64 CPEs.
Serial Baudrate	**Synopsis:** { 115200, 57600, 38400, 28800, 19200, 14400, 9600 } The serial baud rate of the UART port.

4. Click **Apply**.

Section 3.1.4
Enabling/Disabling Logs

On the **Performance** pane, you can enable or disable logs. Disabling logs creates more efficient CPU usage when the base station is heavily utilized with subscribers and data.

NOTE
Before disabling logs, contact Customer Support.

Procedure: Enabling/Disabling Logs

1. Click **Admin**. The **Admin** links appear in the options pane.
2. In the options pane, click the **Performance** link. The **Performance** pane appears.

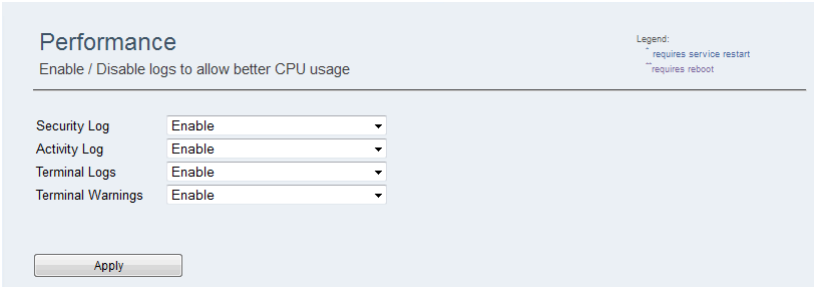


Figure 21: Performance pane

3. Under **Security Log**, select either **Enable** or **Disable**.

4. Under **Activity Log**, select either **Enable** or **Disable**.
5. Under **Terminal Logs**, select either **Enable** or **Disable**.
6. Under **Terminal Warnings**, select either **Enable** or **Disable**.
7. Click **Apply**.

Section 3.2
Viewing Statistics

The following sections describe how to view statistics collected by RUGGEDCOM WIN:

- Section 3.2.1, “Configuring Statistics”
- Section 3.2.2, “Viewing and Clearing Ethernet Statistics”
- Section 3.2.3, “Viewing and Clearing Traffic Statistics”
- Section 3.2.4, “Viewing and Clearing Subscriber Station Statistics”
- Section 3.2.5, “Viewing Aggregate Throughput Statistics”

Section 3.2.1
Configuring Statistics

The **Statistics Configuration** pane displays general uplink and downlink statistics for subscriber stations, including UL and DL signal strengths and carrier to interference plus noise ratios. The packet counters list UL and DL channels, bytes and packets transmitted and dropped, and packet rates. This pane is read-only; there are no parameters to set on this pane. You can clear all subscriber station statistics, and you can clear disconnected subscriber stations from the statistics table.

1. Click **Admin**. The Admin links appear in the options pane.
2. Click the **Statistics Configuration** link. The **Statistics Configuration** pane appears.

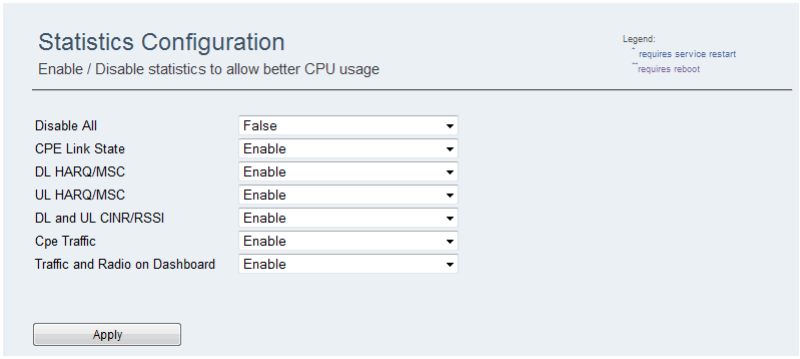


Figure 22: Statistics Configuration pane

3. Review and set the subscriber station statistics in the following fields:

Parameter	Description
Disable All	**Synopsis:** { False, True }

Parameter	Description
	To disable CPE and Dashboard statistics, select a value from this list.
CPE Link State	**Synopsis:** { Enable, Disable } To set this field, select a value from this list.
DL HARQ/MSC	**Synopsis:** { Enable, Disable } To set this field, select a value from this list.
UL HARQ/MSC	**Synopsis:** { Enable, Disable } To set this field, select a value from this list.
DL and UL CINR/RSSI	**Synopsis:** { Enable, Disable } To set this field, select a value from this list.
CPE Traffic	**Synopsis:** { Enable, Disable } To set this field, select a value from this list.
Traffic and Radio on Dashboard	**Synopsis:** { Enable, Disable } To set this field, select a value from this list.

4. Click **Apply**.

Section 3.2.2

Viewing and Clearing Ethernet Statistics

The **Ethernet Statistics** pane displays base station Ethernet traffic information, including traffic rates, packet information, drop rates, and more. This pane is read-only; there are no parameters to set on this pane. You can clear the current Ethernet statistics on this pane.

Procedure: Viewing Base Station Ethernet Statistics

1. Click **Statistics**. The Statistics links appear in the options pane.
2. Click the **Ethernet Counters** link. The **Ethernet Statistics** pane appears.

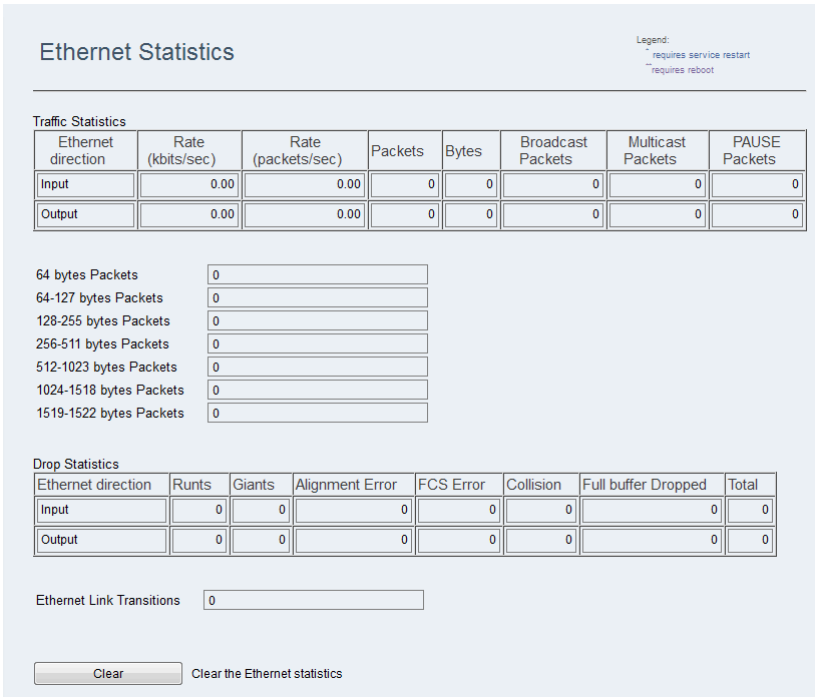


Figure 23: Ethernet Statistics pane

3. To clear the current statistics, click **Clear**.

Section 3.2.3

Viewing and Clearing Traffic Statistics

The **Traffic Statistics** pane displays base station packet counters. This pane is read-only; there are no parameters to set on this pane. You can clear the current traffic statistics on this pane.

1. Click **Statistics**. The Statistics links appear in the options pane.
2. Click the **Traffic Statistics** link. The **Traffic Statistics** pane appears.

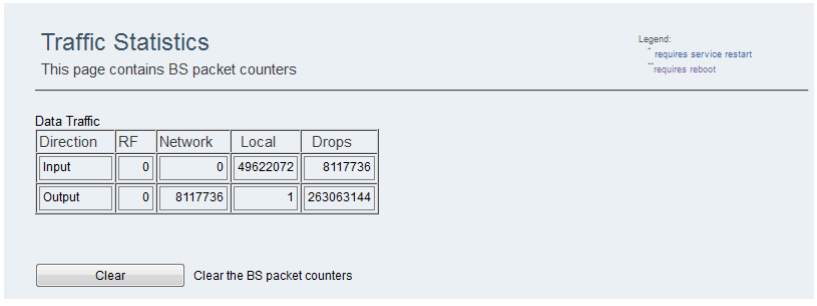


Figure 24: Traffic Statistics pane

3. To clear the current statistics, click **Clear**.

Section 3.2.4

Viewing and Clearing Subscriber Station Statistics

The **General Statistics** pane displays general uplink and downlink statistics for subscriber stations, including UL and DL signal strengths and carrier to interference plus noise ratios. The packet counters list UL and DL channels, bytes and packets transmitted and dropped, and packet rates. This pane is read-only; there are no parameters to set on this pane. You can clear clear all subscriber station statistics, and you can clear disconnected subscriber stations from the statistics table.

1. Click **Statistics**. The Statistics links appear in the options pane.
2. Click the **CPE Statistics** link and then click the **SS Statistics** link. The **General Statistics** pane appears.

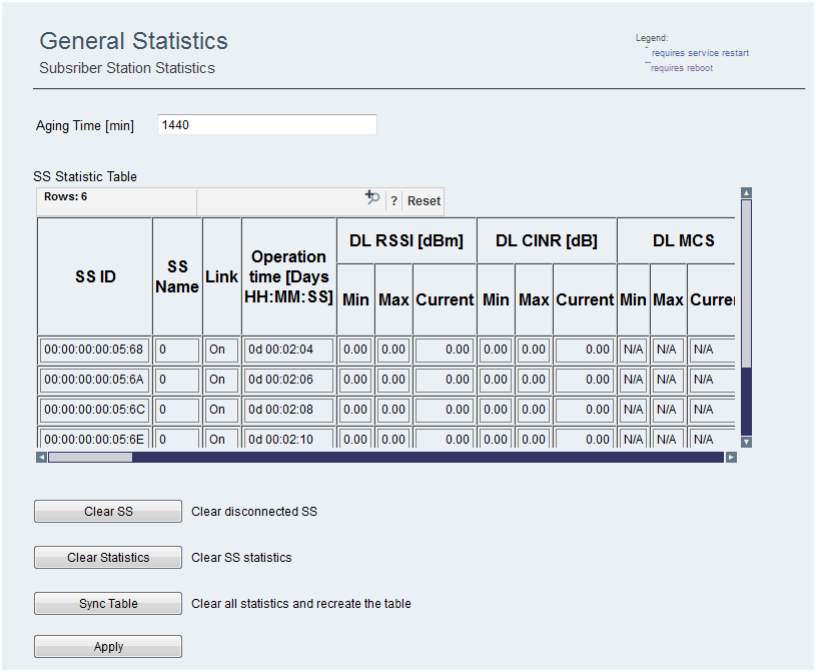


Figure 25: General Statistics pane

3. Review the subscriber station statistics in the following fields:

Parameter	Description
SS ID	Displays the subscriber station identifier.
SS Name	Displays the subscriber station name.
Link	**Synopsis:** { On, Off } Displays the status of the subscriber station link.
Operation Time	Displays the up time of the subscriber station in days, hours, minutes, and seconds.
DL RSSI [dBm]	Displays the downlink received signal strength indication for the subscriber station. Includes minimum, maximum, and current values.

Parameter	Description
DL CINR [dB]	Displays the downlink carrier to interference plus noise ratio for the subscriber station. Includes minimum, maximum, and current values.
DL MCS	Displays downlink Modulation Coding Scheme information, including the minimum, maximum, and current modulation.
DL HARQ MCS	Displays downlink Hybrid Automatic Repeat Request Modulation Coding Scheme information, including the minimum, maximum, and current modulation.
UL CINR [dB]	Displays the uplink carrier to interference plus noise ratio for the subscriber station. Includes minimum, maximum, and current values.
UL HARQ MCS	Displays uplink Hybrid Automatic Repeat Request Modulation Coding Scheme information, including the minimum, maximum, and current modulation.
UL Channels Number	Displays the number of uplink channels, including the minimum, maximum, and current number of channels.
DL Total	Displays downlink data statistics for the subscriber station, including total bytes, packets, dropped packets, and rate in kilobits per second.
DL Ucast	Displays downlink unicast statistics for the subscriber station, including total bytes, packets, dropped packets, and rate in kilobits per second.
UL Total	Displays uplink data statistics for the subscriber station, including total bytes, packets, dropped packets, and rate in kilobits per second.
MIMO Mode	Displays the current Multiple Input Multiple Output mode: MIMO A or MIMO B.

4. To remove a disconnected subscriber station from the table, select the disconnected subscriber station and click **Clear SS**.
5. To clear the statistics for a selected subscriber station, select the subscriber station and click **Clear Statistics**.
6. To synchronize the table, click **Sync Table**.
7. To save your changes, click **Apply**.

Section 3.2.5
Viewing Aggregate Throughput Statistics

The **Aggregate Throughput Statistics** displays uplink and download performance statistics.

The **Aggregate Throughput Statistics** pane is read-only; there are no parameters to set on this pane.

Procedure: Reviewing the Aggregate Throughput Statistics

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Diagnostics** link and then click the **Aggregate Throughput** link. The **Aggregate Throughput Statistics** pane appears.

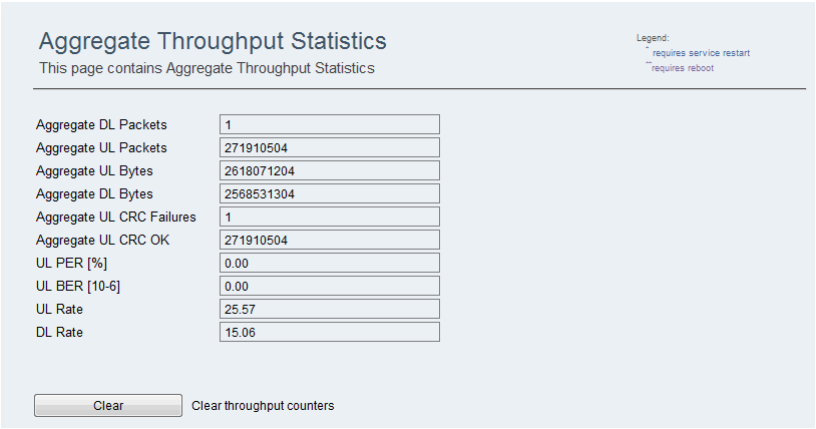


Figure 26: Aggregate Throughput Statistics pane

3. Review the uplink and downlink statistics in the following fields:

Parameter	Description
Aggregate DL Packets	Displays the total number of downlink packets since last reset.
Aggregate UL Packets	Displays the total number of uplink packets since last reset.
Aggregate UL Bytes	Displays the total number of uplink bytes since last reset.
Aggregate DL Bytes	Displays the total number of downlink bytes since last reset.
Aggregate UL CRC Failures	Displays the total number of uplink CRC (Cyclic Redundancy Check) failures since last reset.
Aggregate UL CRC OK	Displays the total number of CRC (Cyclic Redundancy Check) successes since last reset.
UL PER [%]	Displays the uplink packet error rate.
UL BER [10-6]	Displays the uplink bit error rate.
UL Rate	Displays the uplink rate.
DL Rate	Displays the downlink rate.

4. To clear the throughout statistics, click **Clear**.

Section 3.3
Software Version Management

Permanent memory storage is organized in two memory banks, "1" and "2". Two versions of the operating system software can be stored on the base station, one in each memory bank. Each memory bank is designated as either the "Primary" or "Secondary" memory bank. When you reset or reboot the base station, it always runs the software installed in the "Primary" bank. The base station web console provides controls to change the "Primary" and "Secondary" designations on the memory banks, and to reboot the base station using the "Secondary" memory bank for testing. Software saved in one bank can be copied to the other, allowing you to create backups and to restore or update versions as required.

This chapter describes how to manage base station software versions, including how to upload and download files, manage the memory banks and their "Primary" and "Secondary" designations, and how to backup and restore the operating system.

Section 3.3.1
Viewing Software Properties

The **SW Properties** pane displays information about the software loaded into each base station memory bank. On this pane, you can reboot the base station from a selected memory bank, set a selected bank as the primary bank, and restore the base station the factory default software.

Procedure: Viewing software properties

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **SW Upgrade** link. The **SW Properties** pane appears.

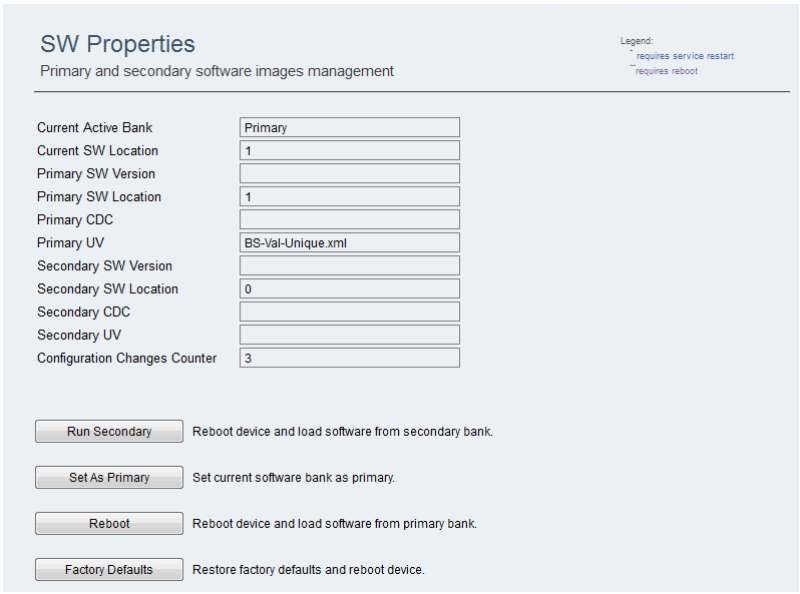


Figure 27: SW Properties pane

3. The **SW Properties** pane displays the following information:

Parameter	Description
Current Active Bank	**Synopsis:** { Primary | Secondary } Displays the name of the memory bank from which the base station software is running.
Current SW Location	**Synopsis:** { 1 | 2 } Displays the number of the memory bank from which the base station software is running.
Primary SW Version	Displays the version number of the software in the Primary memory bank.
Primary SW Location	**Synopsis:** { 1 | 2 }

Parameter	Description
	Displays the number of the current Primary memory bank.
Primary CDC	Displays the filename of the CDC (Customer Defaults Configuration) file in the Primary memory bank.
Primary UV	Displays the filename of the UV (Unique Value) file in the Primary memory bank.
Secondary SW Version	Displays the version number of the software in the Secondary memory bank.
Secondary SW Location	Displays the number of the memory bank selected as the Secondary memory bank.
Secondary CDC	Displays the filename of the CDC (Customer Defaults Configuration) file in the Secondary memory bank.
Secondary UV	Displays the filename of the UV (Unique Value) configuration file in the Primary memory bank.
Configuration Changes Counter	Displays the number of changes made to configuration values on the base station. This value only includes changes to configuration values. It does not include events, such as setting the primary software image or uploading a file.

4. The following operations can be performed from this pane:
   - **Run Secondary** — Reboot the base station and run the "Secondary" software image. Reboot a second time to run the base station using the "Primary" software image.
   - **Set as Primary** — Set the current running software as the "Primary" image. For example, if the base station is running from the "Secondary" image, the "Primary" and "Secondary" designations are exchanged.
   - **Reboot** — Reboot the base station and run the "Primary" image.
   - **Factory Defaults** — Restore the CDC and UV files in the "Primary" memory bank to the factory default settings.

Section 3.3.2
FTP Server Configuration

Use the **FTP Server Properties** pane to configure an FTP server for the base station. You need to configure the FTP settings before you can update the base station software or back up the base station configuration files.

Procedure: Setting the FTP server properties

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **SW Upgrade** link, and then click the **FTP Server** link. The **FTP Server Properties** pane appears.

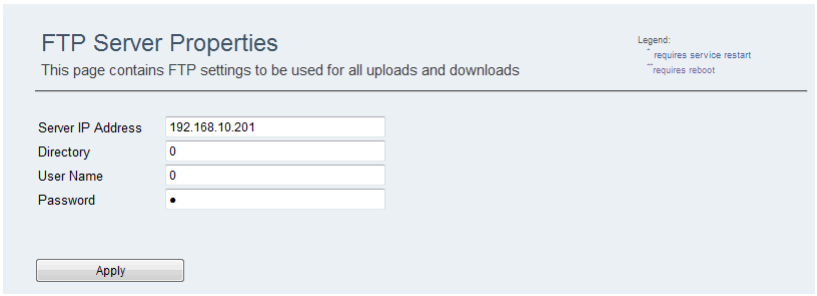


Figure 28: FTP Server Properties pane

3. Review and set the FTP server properties in the following fields:

Parameter	Description
Server IP Address	Type the IPv4 address of the FTP server.
Directory	Type the directory path on the FTP server from which you want to download base station software updates, or to which you want to upload base station configuration files.
User Name	Type the user name to use to log in to the FTP server.
Password	Type the password to use to log in to the FTP server.

4. Click **Apply**.

Section 3.3.3

Downloading Base Station Software

Use the **Downloads** pane to download base station software and configuration files from your FTP server. The base station downloads all software to the "Secondary" memory bank.

Before downloading, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, refer to Section 3.3.2, “FTP Server Configuration”.

Procedure: Downloading software

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **SW Upgrade** link, and then click the **Downloads** link. The **Downloads** pane appears.

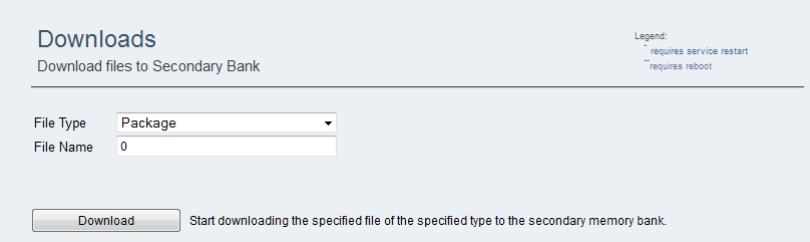


Figure 29: SW Downloads pane

3. Set the download parameters in the following fields:

Parameter	Description
File Type	Select the type of file to download: • `Package` – The software package file provided with an upgrade package. For example: `ruggedupgrade.ini` • `Web Resource` – A web console template file. For example: `web.rc` • `CDC` – A Common Default Configuration file. For example: `BS-Val-Cdc.xml` • `UV` – A Unique Value file. For example: `BS-Val-Unique.xml`
File Name	Type the name of the file you want to download.

4. Click **Download**. The base station downloads the specified file from the FTP server directory to the "Secondary" memory bank.

Section 3.3.4

Managing the Primary Memory Bank

Use the **Primary Components** pane to manage software in the "Primary" memory bank. On this pane, you can view information for the files in the memory bank, upload files from the memory bank to your FTP server, and copy files from the "Primary" memory bank to the "Secondary" memory bank.

Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, refer to Section 3.3.2, “FTP Server Configuration”.

Procedure: Viewing files in the Primary memory bank

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **SW Upgrade** link, and then click the **Primary Bank** link. The **Primary Components** pane appears.

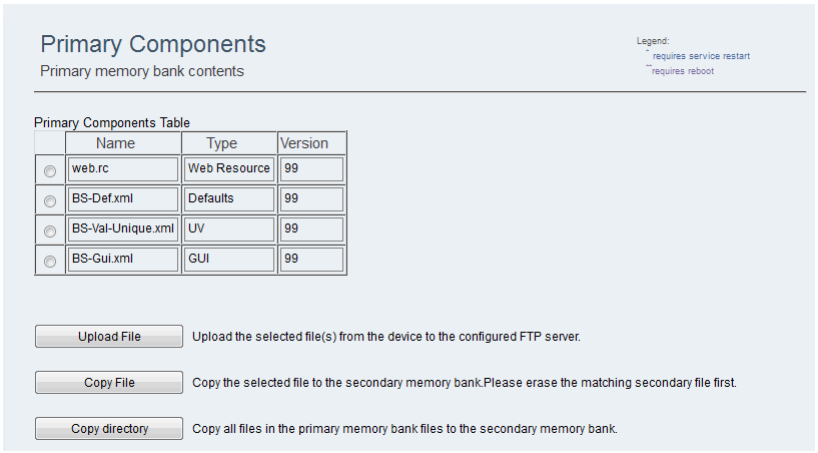


Figure 30: Primary Bank Components pane

3. The **Primary Components Table** displays the following information:

Parameter	Description
Name	Displays the software component filename.
Type	**Synopsis:** { Package, Application, VxWorks, Blob, Script, WebResource, Defaults, CDC, Regulation, UV, GUI } Displays the software component file type.
Version	Displays the software component version number.

4. To upload a file to your FTP server:

NOTE
*Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, refer to Section 3.3.2, "FTP Server Configuration".*

- Select a file from the **Primary Components Table**.
- Click **Upload File**.

5. To copy a file to the "Secondary" memory bank:

NOTE
Before copying the file, ensure that it does not already exist in the "Secondary" memory bank. If the file is present in the "Secondary" memory bank, delete the file from the "Secondary" memory bank before copying. For instructions on how to delete files from the "Secondary" memory bank, refer to Section 3.3.5, "Managing the Secondary Memory Bank".

- Select a file from the **Primary Components Table**.
- Click **Copy File**.

6. To copy all files to the "Secondary" memory bank:

- Click **Copy directory**.

Section 3.3.5

Managing the Secondary Memory Bank

Use the **Secondary Components** pane to manage software in the "Secondary" memory bank. On this pane, you can view information for the files in the memory bank, upload files from the memory bank to your FTP server, and delete files from the memory bank.

Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, refer to Section 3.3.2, “FTP Server Configuration”.

Procedure: Viewing files in the Secondary memory bank

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **SW Upgrade** link, and then click the **Secondary Bank** link. The **Secondary Components** pane appears.

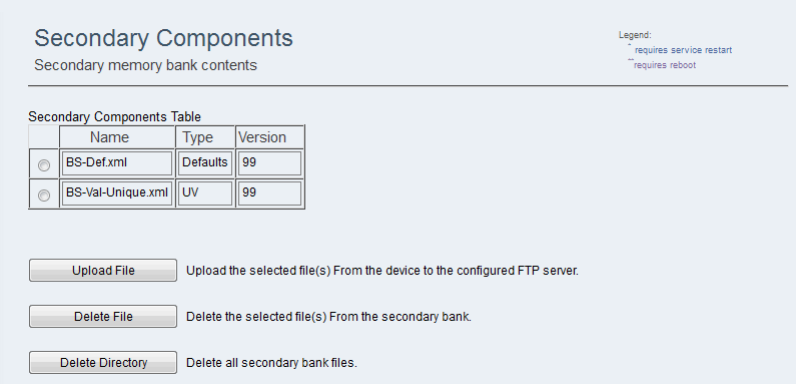


Figure 31: Secondary Bank Components pane

3. The **Secondary Components Table** displays the following information:

Parameter	Description
Name	Displays the software component filename.
Type	Displays the software component file type. **Synopsis:** { Package, Application, VxWorks, Blob, Script, WebResource, Defaults, CDC, Regulation, UV, GUI }
Version	Displays the software component version number.

4. To upload a file to your FTP server:

> **NOTE**
> *Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, refer to Section 3.3.2, “FTP Server Configuration”.*

   - Select a file from the **Secondary Components Table**.
   - Click **Upload File**.
5. To delete a file:
   - Select a file from the **Secondary Components Table**.

- Click **Delete File**.

6. To delete all files:
   - Click **Delete Directory**.

Section 3.3.6

File Status

Use the **File Transfer Status** pane to view the status of upload and download operations between the base station and your FTP server. You can also cancel current upload and download operations from this pane.

Procedure: Viewing File Transfer Status

1. Click **Admin**. The **Current Status** pane appears.
2. In the options pane, click the **SW Upgrade** link, and then click the **Files Status** link. The **File Transfer Status** pane appears.

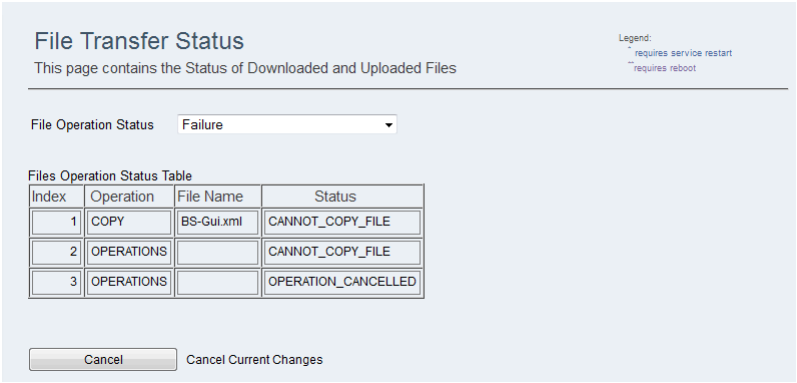


Figure 32: File Transfer Status pane

3. From the **File Operation Status** list, select an operation status:
   - OK – displays successfully completed file transfers.
   - Not Started – displays requested file transfers that have not yet started.
   - In Process – displays file transfers that are currently in progress.
   - Failure – displays failed file transfers.
4. The **File Transfer Operation Status** table displays the following information for the files in the selected operation status:

Parameter	Description
Index	Displays a unique identifier for the file.
Operation	**Synopsis:** { Download, Upload, Delete, Copy, Operations } Displays the file transfer operation performed on the file. The `Operations` option indicates the completion of a batch operation on several files.
File Name	Displays the filename for the uploaded or downloaded file.

Parameter	Description
Status	**Synopsis:** { OK, Not Started, In Process, Failure } Displays the status of the file transfer operation.

5. To cancel a download or upload operation that is currently in progress, click **Cancel**.

Section 3.3.7
Upgrading the Base Station Software

For safety and reliability, the base station software upgrade process consists of the following steps, with checks and verification at several stages:

1. Load the new software image to the secondary memory bank:
   - Configure the FTP server from which the new software files will be downloaded (see Section 3.3.2, “FTP Server Configuration”):
   - Download the software update files to the secondary memory bank (see Section 3.3.3, “Downloading Base Station Software”).
   - Verify that the downloaded software files have been correctly saved to the secondary memory bank (see Section 3.3.5, “Managing the Secondary Memory Bank”).
2. Perform a trial run of the new software image:

   On the *SW Properties* pane, click *Run Secondary*.

   The BS will reset and load the software image in the secondary memory bank. This process will take approximately two minutes.
3. Commit the new software image as the new default software:

   Again on the *SW Properties* pane, click *Set As Primary* in order to set the current memory bank (currently denoted Secondary) as Primary. Doing so will cause the software in the memory bank newly designated Primary to be run by default on bootup.

Section 3.4
Operation Mode

The base station supports two operation modes:

- Standalone mode. This is the default operation mode.
- ASN-GW mode.

The operation mode defines whether system operations, such as Quality of Service (QoS) functions, are performed by the base station or by the ASN-GW. In Standalone mode, such operations are performed on the base station itself. In ASN-GW mode, such operations are performed on the ASN-GW.

NOTE
To apply changes to the operating mode, you must restart the service.

Procedure: Setting the Operation Mode

1. Click **Backbone**. The **Backbone** links appear in the options pane.

2. In options pane, click the **Operation Modes** link. The **Mode Settings** pane appears.

Figure 33: Mode Settings pane

3. In the **Configured Operation Mode** field, select the system operation mode: **Standalone**, or **ASN-GW**.
4. Click **Apply**.
5. Click **Quick Start**. The **Quick Start Settings** pane appears.
6. Click **Stop Service**, and then click **Start Service**.

Section 3.5

Base Station Interface Configuration

Configure the base station IP address, subnet mask, and gateway address on the **IP Addresses** pane. You can also review the current configuration on this pane.

NOTE
To apply changes to this pane, you must restart the service.

Procedure: Setting the Base Station and Interface Configuration

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **IP Addresses** link. The **IP Addresses** pane appears.

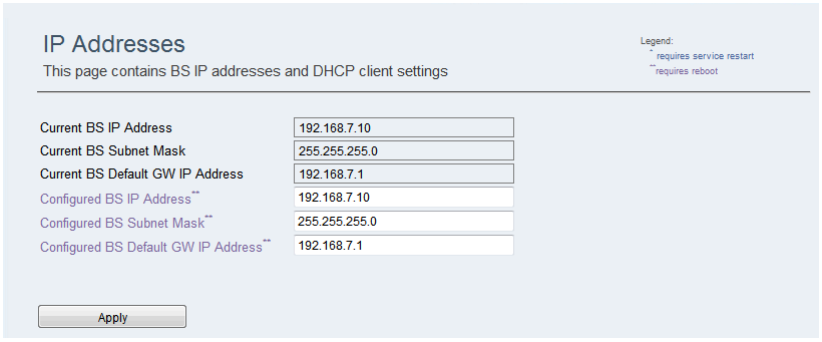


Figure 34: IP Addresses pane

3. Review and set the interface configuration in the following fields:

Parameter	Description
Current BS IP Address	Displays the current base station IP address.
Current BS Subnet Mask	Displays the current base station subnet mask.
Current BS Default GW IP Address	Displays the current base station default gateway IP address.
Configured BS IP Address	To change the base station IP address, type a new address is this field.
Configured BS Subnet Mask	To change the base station subnet mask, type a new subnet mask in this field.
Configured BS Default GW IP Address	To change the base station default gateway IP address, type a new IP address in this field.

NOTE
*If the base station is directly connected to the ASN gateway, specify the ASN gateway's IP address in the **Configured BS Default GW IP Address** field. If the base station reaches the ASN gateway through a router, specify the router's IP address in the **Configured BS Default GW IP Address** field.*

4. Click **Apply**.
5. Click **Quick Start**. The **Quick Start Settings** pane appears.
6. Click **Stop Service**, and then click **Start Service**.

Section 3.6
MTU Configuration

On the **MTU** pane, you can enable or disable the maximum transmission unit. The MTU specifies the size of the largest data unit, in bytes, that the Base Station will transmit. The MTU value includes the L2 header and cyclic redundancy check (CRC).

Procedure: Enabling/Disabling MTU

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **MTU** link. The **MTU Configuration** pane appears.

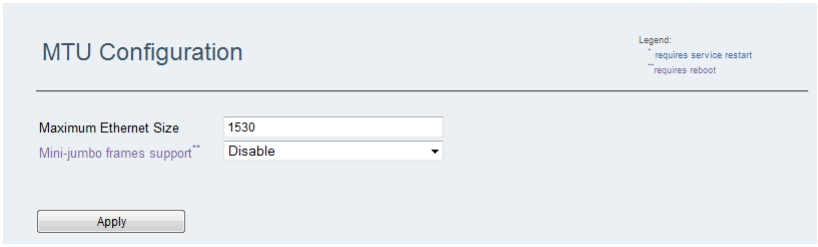


Figure 35: MTU Configuration pane

3. Under **Mini-jumbo frames support**, select either **Enable** or **Disable**.
4. Click **Apply**.

5. Reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 3.7
Standalone Mode Configuration

The following configuration settings and tables are available in Standalone mode:

- Switching Settings: see Section 3.7.1, “Switching Settings”.
- MAC Address Table: see Section 3.7.2, “MAC Address Table”.
- ARP Table: see Section 3.7.3, “ARP Table”.

Section 3.7.1
Switching Settings

The switching settings determine the layer 2 switching method and the MAC Address Table aging time. The MAC address aging period determines the time after which an inactive MAC address is dropped from the MAC Address Table.

NOTE
Layer 2 switching is not supported in ASN-GW mode.

Procedure: Configuring the Switching Settings

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **Switching** link, and then click the **Switching Settings** link. The **Switching Settings** pane appears.

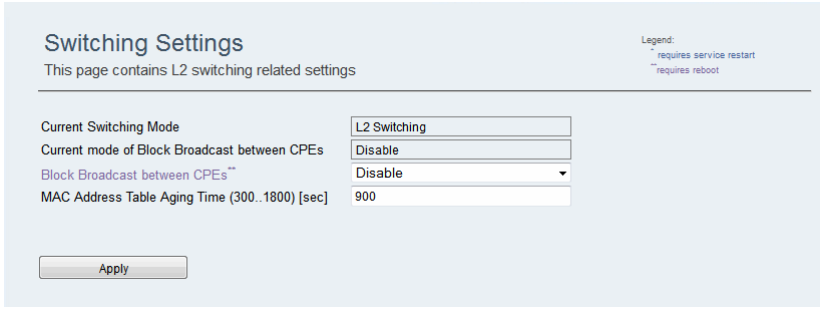


Figure 36: Switching Settings pane

3. Review and set the switching parameters in the following fields:

Parameter	Description
Current Switching Mode	Displays the current layer 2 switching mode: L2 Switching.

Parameter	Description
	With L2 Switching, traffic flooding is enabled. To dynamically learn station locations, the base station listens to incoming frames and inspects the source MAC address. If the source MAC address is not already in the MAC Address Table, the address is added to the table. If the source MAC address is already in the table, its aging time is refreshed. As part of the forwarding decision, if a MAC address destination is found, the frame is forwarded to the address. If the MAC address is not found in the table, the frame is flooded to all CPEs (if it is a downlink packet) and to the CPEs and network interface (if it is an uplink packet).
Current mode of Block Broadcast between CPEs	Displays the current setting for the **Block Broadcast Between CPEs** parameter.
Block Broadcast Between CPEs	**Synopsis:** { Enable, Disable } **Default:** Disable When enabled, non-VLAN tagged broadcast/multicast frames are not forwarded between CPEs over RF. Broadcast or multicast frames received from a CPE are forwarded only to the Ethernet side of the base station. This feature prevents the creation of phantom links between CPEs, which can be created by an L3 network that uses L3 protocols (e.g. ISIS or OSPF) over WiMAX. Phantom links (or adjacencies) can quickly fill an adjacency database, increasing convergence times and creating multiple alarms when a site goes down.
MAC address Table Aging Time (300…1800) [sec]	Determines the MAC address aging period, in seconds. Type a value in the range of 300 to 1800. After a MAC address is inactive for this period of time, the base station drops the address from the MAC Address Table.

4. Click **Apply**.

Section 3.7.2
MAC Address Table

The MAC Address Table displays the MAC addresses learned by the base station using the Layer 2 switching mode. On the **MAC Address Table** pane, you can clear the MAC Address Table, show MAC addresses per subscriber station, and show MAC addresses per VLAN.

Procedure: Viewing the MAC Address Table

1. Click **Backbone**. The **Backbone Admin** links appear in the options pane.
2. In the options pane, click **Switching**, and then click **MAC Address Table**. The **MAC Address Table** pane appears.

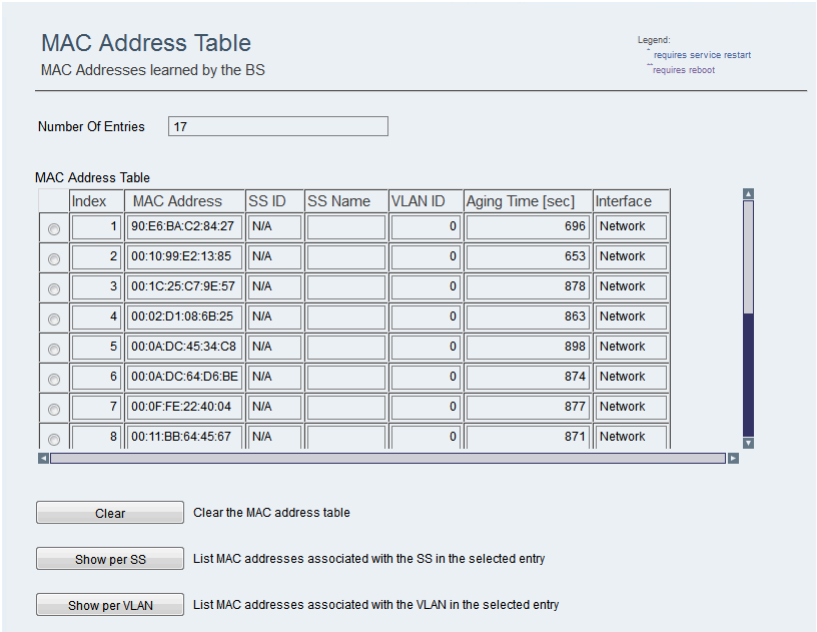


Figure 37: MAC Address Table

3. The MAC Address Table displays the following information:

Parameter	Description
Number Of Entries	Displays the number of entries in the MAC Address Table.
Index	Displays a unique identifier for the table entry.
MAC Address	Displays the MAC address of a local or remote node.
SS ID	Displays the Subscriber Station ID, if applicable, from which the MAC address was learned.
VLAN ID	Displays the identifier for the Virtual LAN on which the node is active.
Aging Time [sec]	Displays the time, in seconds, until the entry will be removed from the table.
Interface	Displays the interface from which the base station learned the MAC address. Options include: • `Network` – The base station acquired the address from the Ethernet network interface • `RF` – The base station acquired the address from the RF interface • `Local` – Indicates the MAC address of the base station itself

4. To clear the MAC Address Table, click **Clear**. The system clears all entries from the table.
5. To display table entries sorted by SS ID, select a row from the table and click **Show per SS**. The table displays all entries with the SS ID of the selected row.
6. To display table entries sorted by VLAN ID, select a row from the table and click **Show per VLAN**. The table displays all entries with the VLAN ID of the selected row.

Section 3.7.3
ARP Table

The **ARP Table** pane displays IP addresses associated with MAC addresses, as discovered by the base station using the Address Resolution Protocol (ARP).

Procedure: Viewing the ARP Table

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **Switching** link, and then click the **ARP Table** link. The **ARP Table** pane appears.

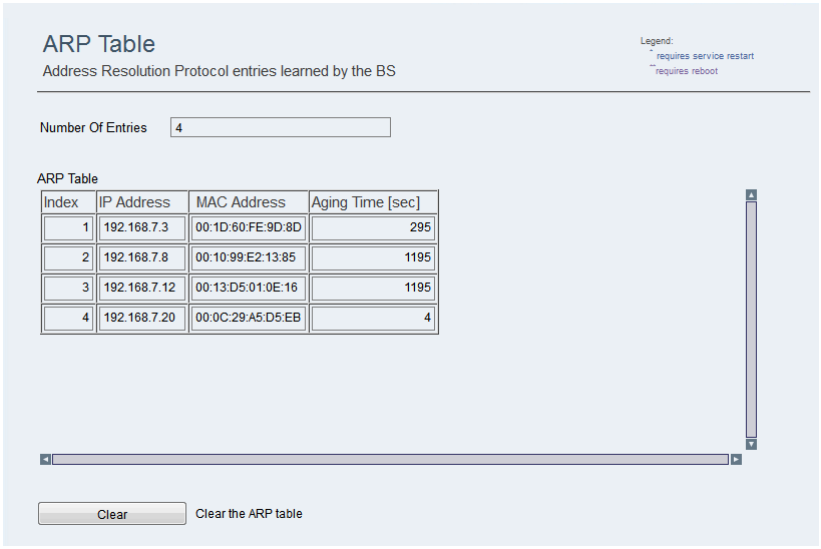


Figure 38: ARP Table

3. The ARP Table displays the following information:

Parameter	Description
Number Of Entries	Displays the number of entries in the ARP Table.
Index	Displays a unique identifier for the table entry.
IP Address	Displays the IP address of the node as discovered through ARP.
MAC Address	Displays the MAC address of the node.
Aging Time [sec]	Displays the time, in seconds, until the entry will be removed from the table.

Section 3.7.4
Configuring Priority Tagging

On the **Priority Tagging** pane, you can enable or disable priority tagging. Enabling priority tagging pass-through support Ethernet frames means that protocol 802.1Q, tagged as VLAN ID = 0 (PROFINET traffic) will not be dropped.

PROFINET is an open standard for industrial Ethernet. The network was developed by Siemens and the PROFIBUS User Organization (PI). PROFINET is used for factory and process automation, for safety applications, and for the entire range of drive technology right up to clock-synchronized motion control. PROFINET traffic consists of Ethernet frames with protocol 802.1Q, tagged with VLAN ID = 0. By default this traffic is dropped by the base station.

Procedure: Configuring Priority Tagging

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **Switching** link and then click **Priority Tagging**. The **Priority Tagging** pane appears.

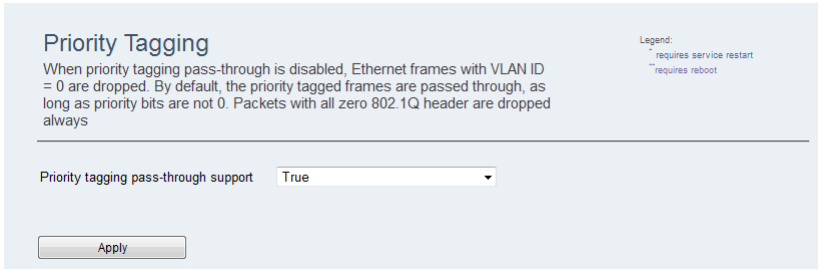


Figure 39: Priority Tagging pane

3. Under **Priority tagging pass-through support**, select either **True** or **False**. The default setting for priority tagging is **False**.
4. Click **Apply**.

Section 3.8

ASN-GW Mode Configuration

In ASN-GW mode, configure the following:

- ASN-GW Link settings: see Section 3.8.1, “ASN-GW Link Settings”.
- Keep Alive settings: see Section 3.8.2, “Keep Alive Settings”.

Section 3.8.1

ASN-GW Link Settings

On the **ASN-GW Settings** pane, you configure the ASN-GW IP address. On this pane, you can also view the R6 signaling protocol in use between the base station and the ASN-GW.

NOTE
The ASN-GW IP address must be configured correctly. In ASN-GW mode, the base station relies on the ASN-GW for Quality of Service (QoS) signaling and other functions.

You must reboot the system after changing the ASN-GW IP address.

Procedure: Configuring the ASN-GW IP Address

1. Click **Backbone**. The **Backbone** links appear in the options pane.

2. In the options pane, click the **ASN Settings** link, and then click the **ASN-GW Settings** link. The **ASN-GW Settings** pane appears.

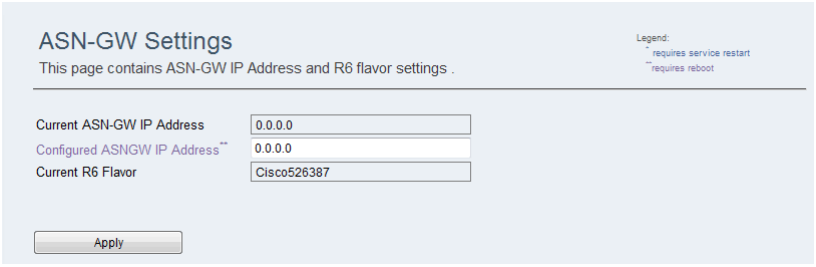


Figure 40: ASN-GW Settings pane

3. Review and set the ASN-GW settings in the following fields:

Parameter	Description
Current ASN-GW IP Address	Displays the current ASN-GW IP address set in the base station.
Configured ASN-GW IP Address	To set a new ASN-GW IP addresses, type the IP address in this field.
Current R6 Flavor	Displays the R6 signaling protocol currently in use between the base station and the ASN-GW.

4. Click **Apply**.
5. If you changed the value in the **Configured ASN-GW IP Address** field, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 3.8.2
Keep Alive Settings

On the **Keep Alive Settings** pane, you configure the keep-alive message interval, the number of message retries, and whether the Keep Alive Activation Mode is enabled or disabled.

NOTE
You must reboot the system after enabling or disabling the Keep Alive Activation Mode.

Procedure: Configuring the Keep Alive Settings

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **ASN Settings** link, and then click the **Keep Alive** link. The **Keep Alive Settings** pane appears.

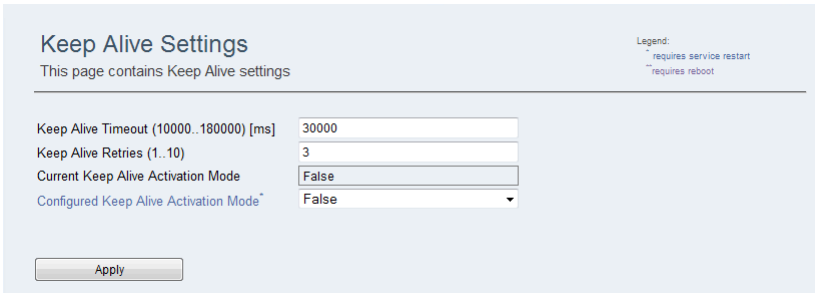


Figure 41: Keep Alive Settings pane

3. Review and set the Keep Alive settings in the following fields:

Parameter	Description
Keep Alive Timeout (10000..180000) [ms]	The time, in milliseconds, that the base station waits for the keep-alive response before it performs a keep-alive retransmission. Valid values are in the range of 1000 to 180000. The default value is 30000.
Keep Alive Retries (1..10)	The maximum number of keep-alive retransmissions to perform before the base station de-registers all of the currently registered CPEs. Valid values are in the range of 1 to 10. The default value is 3.
Current Keep Alive Activation Mode	Displays the current state of the Keep Alive Activation Mode. Valid values are True (Keep Alive Activation Mode is enabled), or False (Keep Alive Activation Mode is disabled). The default value is False.
Configured Keep Alive Activation Mode	To enable or disable the Keep Alive Activation Mode, select a value in this field. Valid values are True (Keep Alive Activation Mode is enabled), or False (Keep Alive Activation Mode is disabled). The default value is False.

4. Click **Apply**.
5. If you changed the value in the **Configured Keep Alive Activation Mode** field, restart the base station service:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Stop Service**, and then click **Start Service**.

Section 3.9
Backhaul CPE

On the **Managing CPE** pane, you can configure a CPE device connected to the base station to manage the base station. A backup CPE can also be configured.

Configuring a device to be a backhaul CPE (or managing CPE) allows the base station to be accessed from a host behind the CPE (using the LAN side of the CPE), and also allows backbone infrastructure including AAA, DHCP and RUGGEDCOM NMS servers to be located behind the CPE. When all traffic is routed to the CPE, the CPE is acting as a backhaul device. For more information, refer to the application note on Network Management via CPE.

Procedure: Configuring a CPE to Manage the Base Station

1. Click **Backbone**. The **Backbone** links appear in the options pane.
2. In the options pane, click the **Backhaul** link. The **Managing CPE** pane appears.

Figure 42: Managing CPE pane

3. Under **Manage By CPE**, type the MAC Address of the CPE.
4. Under **Backup CPE**, type the MAC Address of the backup CPE.
5. Click **Apply**.

4 System Administration

This chapter describes how to perform various administrative tasks related to device identification, user permissions, alarm configuration, certificates and keys, and more. It describes the following tasks:

Section 4.1

Managing Users

Access to the CPE web management application is secured through user accounts and access levels. Two access levels are available:

- Admin – users can access all read and write options, including user definitions.
- Guest – users can access all read options only.

The following sections describe how to add and delete users:

Section 4.1.1

Adding Users

To add a user profile, do the following:

NOTE
Only users with Admin access rights can manage user profiles.

1. Navigate to ***Admin*** » ***Security***. The **Device Access Permissions** screen appears.

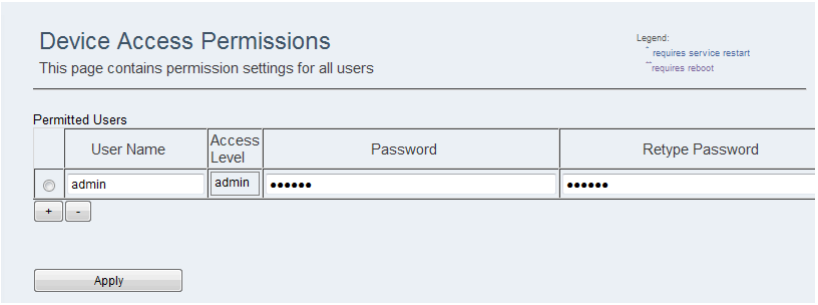


Figure 43: Device Access Permissions Screen

2. Click the + button. A new row appears in the **Permitted Users** table.
3. In the **User Name** box, type the user name.
4. In the **Access Level** column, select an access level for the user.
5. In the **Password** column, type the password for the user.
6. In the **Retype Password** column, retype the password for the user.
7. Click **Apply**.

Section 4.1.2
Deleting Users

To delete a user profile, do the following:

NOTE
Only users with Admin access rights can manage user profiles.

1. Navigate to ***Admin*** » ***Security***. The **Device Access Permissions** screen appears.

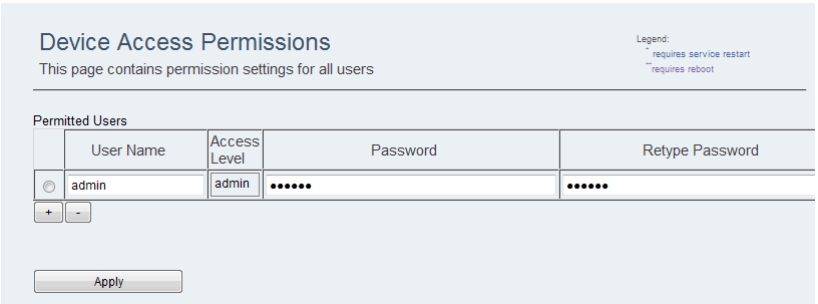


Figure 44: Device Access Permissions Screen

2. Select a user from the **Permitted Users** list.
3. Click the - button.
4. Click **Apply**.

Section 4.2

RADIUS Login

Use the **Radius Login** pane to set RADIUS login authentication settings for remote login, including enabling or disabling local login.

Local login can be disabled in the **Allow Local Login** field by choosing a value of **No**. If local login is disabled, users cannot log in with the user name, admin@local. Only users with user names configured **Permitted Users** list can log in. For more information about the **Permitted Users** list, refer to Section 4.1.1, “Adding Users”.

NOTE

After local login has been disabled, users cannot access the Security menu to enable local login while there is an active connection to an AAA server. If the connection to the configured AAA servers is lost, local login will be enabled.

Procedure: Setting the RADIUS Login parameters

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Radius Login** link. The **Radius Login Settings** pane appears.

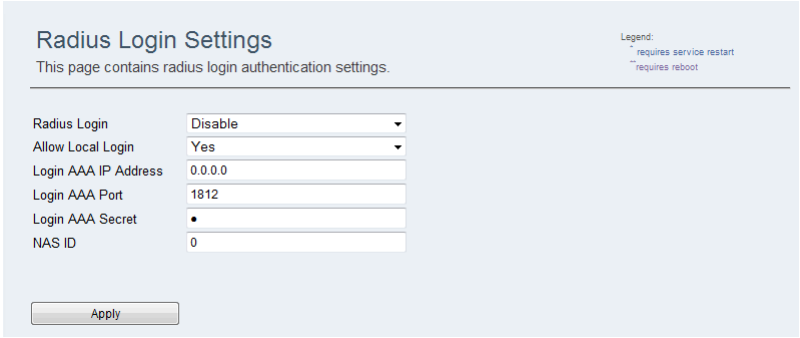


Figure 45: Radius Login Settings pane

3. Review and set the parameters in the following fields:

Parameter	Description
Radius Login	**Synopsis:** { Enable, Disable } To set the RADIUS Login authentication mode, select a value from this list.
Allow Local Login	**Synopsis:** { Yes, No } Enables or disables local login.
Login AAA IP Address	The configured Web Login AAA Server IP Address. Type an IP address in this field.
Login AAA Port	The configured Web Login AAA Server Port. Type a value in this field.
Login AAA Secret	The configured Web Login AAA Server Secret. Type a value in this field.
NAS ID	The RADIUS NAS Identifier. Type a value in this field.

4. Click **Apply**.

Section 4.3
Enabling/Disabling SSH Shell Access

To enable/disable access to the SSH shell, do the following:

1. Navigate to ***Admin » Security » Remote Shell***. The **SSH Shell Access** screen appears.

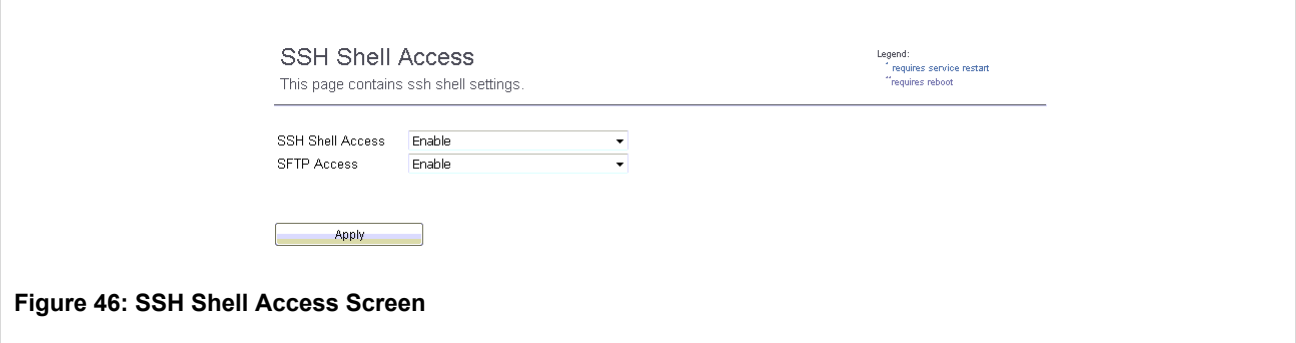


Figure 46: SSH Shell Access Screen

2. In the **SSH Shell Access** list, select **Enable** or **Disable**.
3. In the **SFTP Access** list, select **Enable** or **Disable**.
4. Click **Apply**.

Section 4.4
Managing Keys and Certificates

The following sections describe how to manage keys and certificates on the device.

- Section 4.4.1, “Loading HTTPS Certificates and Private Keys”
- Section 4.4.2, “Generating SSH Keys”

Section 4.4.1
Loading HTTPS Certificates and Private Keys

NOTE
Resetting the device to its factory defaults will erase the loaded certificate, key and delete the password from the UV file (as the whole UV is erased). The device will revert its default certificate and key.

NOTE

- *All certificates and keys must be saved in .pem format*
- *The filename for the certificate must be* `httpscert.pem`
- *The filename for the private key must be* `httpskey.pem`

- *The maximum certificate file size is 20 kb*
- *The maximum private key file size is 4 kb*
- *The private key password can be up to 16 characters long*

To load HTTPS certificates and private keys, do the following:

1. Navigate to ***Admin*** » ***HTTPS Certificate***. The **Load HTTPS Certificates** screen appears.

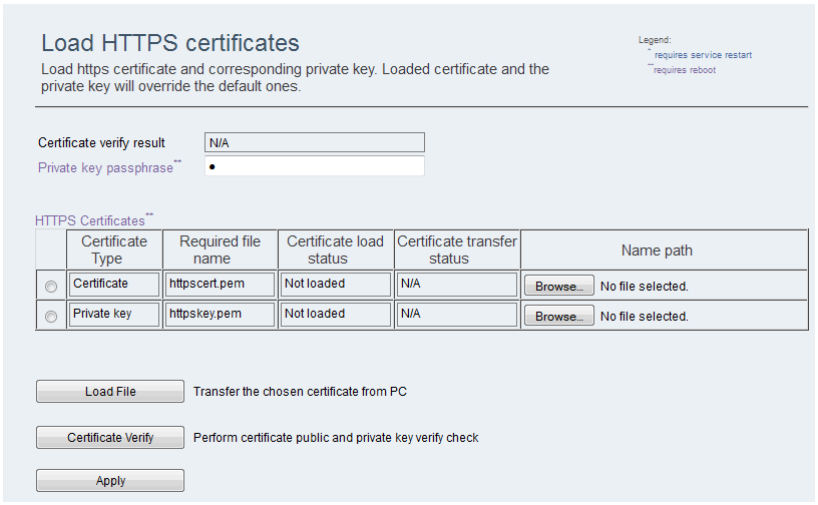


Figure 47: Load HTTPS Certificates Screen

2. Type a passphrase in the **Private Key Passphrase** box.
3. Under **HTTPS Certificates**, select the certificate type and then click **Browse**.
4. Select the file to upload.
5. Click **Load** to load the certificate or key.
6. Click **Certificate Verify** to verify the passphrase, certificate and key.
7. Click **Apply**.
8. Reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 4.4.2
Generating SSH Keys

To reboot the device and generate new SSH keys, do the following:

1. Navigate to ***Management*** » ***SSH Keys***. The **SSH Keys** screen appears.

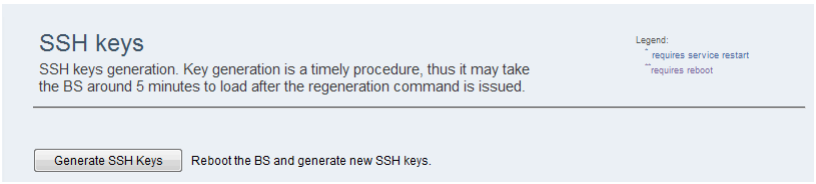


Figure 48: SSH Keys Screen

NOTE
Key generation can take up to 5 minutes to complete.

2. Click **Generate SSH Keys**. The device reboots and generates new SSH keys.

Section 4.5
Alarms and Traps

Use the **System Alarms** and **SNMP Trap Settings** panes to view system alarms and to configure SNMP traps.

Section 4.5.1
System Alarms

The **System Alarms** pane displays current system alarms. This pane is read-only; there are no parameters to set on this pane.

Procedure: Viewing System Alarms

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Alarms and Traps** link. The **System Alarms** pane appears.

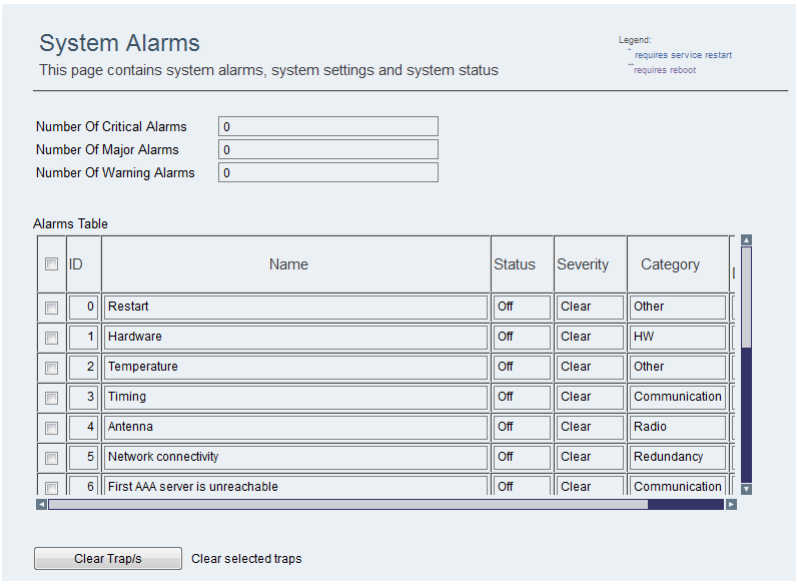


Figure 49: System Alarms pane

3. Review the current number of alarms in the following fields:

Parameter	Description
Number of Critical Alarms	Displays the number of critical alarms.
Number of Major Alarms	Displays the number of major alarms.
Number of Warning Alarms	Displays the number of warning or advisory alarms.

4. Review the current alarm settings in the Alarms Table:

Parameter	Description
ID	Displays the alarm type identification number.
Name	Displays the alarm type. For a list of alarm and trap conditions, refer to Section 4.5.3, “SNMP Traps List”.
Status	**Synopsis:** { Off, On } Indicates if the alarm type is enabled or disabled.
Severity	**Synopsis:** { Clear, Critical, Major, Warning } Displays the severity of the alarm.
Category	**Synopsis:** { Restart, Communication, RF, Hardware, Security, Environmental, Redundancy, Services, Link Status } Displays the category for the alarm type.
Last Description	Displays a message describing the alarm.
Last Update Time	Displays the date and time of the most recent alarm.

NOTE
If there is an active Antenna Disconnect alarm, you must reboot the base station:

1. Click **Quick Start**. The **Quick Start Settings** pane appears.
2. Click **Reboot**.

Section 4.5.2
SNMP Trap Settings

On the **SNMP Trap Settings** panel, configure the base station SNMP traps. From this pane, you can also select traps and send them on demand.

NOTE
To send traps, you must have SNMP Trap Destinations configured. For instructions on configuring SNMP Trap Destinations, refer to Section 5.5.1, "SNMP General Settings".

Procedure: Setting SNMP traps

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Alarms and Traps** link, and then click the **Traps** link. The **SNMP Trap Settings** pane appears.

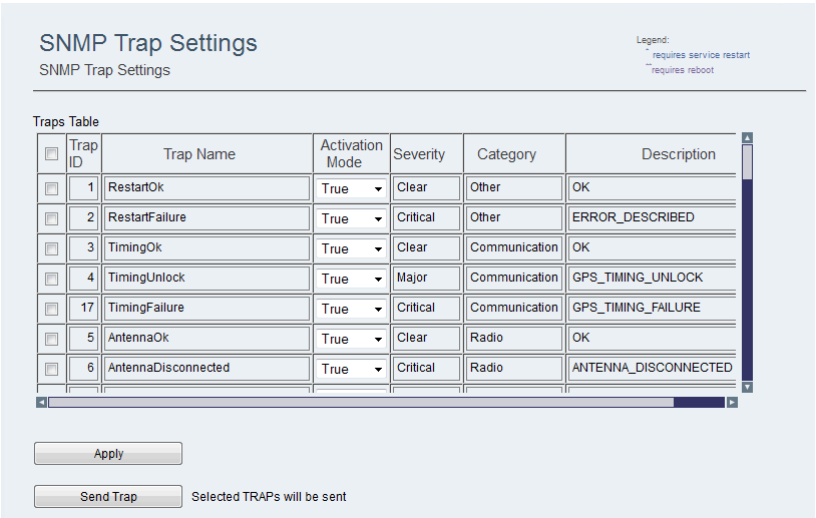


Figure 50: SNMP Trap Settings pane

3. In the **Traps Table**, review and configure the SNMP traps:

Table: Traps Table

Column	Description
Trap ID	Displays the trap identification number.
Trap Name	Displays the trap name.

Column	Description
Activation Mode	Indicates if the trap is enabled or disabled. To enable a trap, select True. To disable a trap, select False. Values: True | False
Severity	Displays the severity of the trap condition. Values: Clear | Critical | Major | Warning
Category	Displays the category of the trap condition. Values: Restart | Communication | RF | Hardware | Security | Environmental | Redundancy | Services | Link Status
Description	Displays a description of the trap condition
Value	Displays the value reported by the SNMP trap.

4. Click **Apply**.

For testing purposes, you can send selected traps on demand. To send traps, you must have SNMP Trap Destinations configured. For instructions on configuring SNMP Trap Destinations, refer to Section 5.5.1, “SNMP General Settings”.

Procedure: Sending SNMP traps on demand

1. In the **Traps Table**, select one or more SNMP traps
2. Click **Send Trap**.

Section 4.5.3
SNMP Traps List

NOTE
The WIMAX-BS-TRAPS.mib file in the software release folder contains a full list of traps.

Table: Restart Trap

Event Name	Description	
RestartOK	Base station software is restarting. Value represents the initiator for the action and transmission status.	
	Condition	SW init completed successfully.
	Value Range	Power up TX ON | Power up TX OFF | Watchdog TX OFF | Watchdog TX ON | Software TX OFF | SW TX ON
	Severity	Warning
	Default	Enabled
	Alarm ID[a]	0
	Action	None
	Text	BS has restarted successfully. Parameter specify TX off/on and restart cause.
RestartFailure	BS init failure. This event shall report all causes of initialization errors.	
	Condition	Init completed with failure.

Event Name	Description	
	Value Range	Configuration | SW | HW
	Severity	Major
	Default	Enabled
	Alarm ID[a]	0
	Action	Configuration: Load Backup Configuration withTX off. SW: Load other Secondary/Main SW with TX off. HW: TX off.
	Text	Init Failure, service is not provided.

[a] *A Device Alarm ID of 0 means that no alarm is generated.*

Table: Communication Traps

Event Name	Description	
TimingUnLock	Lost synchronization with GPS time. Value indicates time source.	
	Condition	GPS lost synchronization, HoldOverAlarmTimeout elapses
	Value Range	GPS | 1588
	Severity	Major
	Default	Enabled
	Alarm ID[b]	4
	Action	None
	Text	Timing is unlocked, Transmission stopped.
TimingOK	This event is clearing the TimingUnLock event.	
	Condition	Successful time acquisition after GPS failure.
	Value Range	GPS | 1588
	Severity	Clear
	Default	Enabled
	Alarm ID[b]	4
	Action	If startTx after sync parameter is enabled, then start transmission; else none.
	Text	Timing is now locked
FirstAAAUnreachable	First AAA is Unreachable.	
	Condition	Primary AAA does not reply to Access-Request (KA) messages and retransmission is exhausted.
	Value Range	Primary AAA IP address
	Severity	Critical
	Default	Enabled
	Alarm ID[b]	7
	Action	None
	Text	Primary AAA is unreachable.

Event Name	Description	
SecondAAAUnreachable	Second AAA is unreachable.	
	Condition	Secondary AAA does not reply to Access-Request (KA) messages and retransmission is exhausted.
	Value Range	Secondary AAA IP address
	Severity	Critical
	Default	Enabled
	Alarm ID[b]	8
	Action	None
	Text	Secondary AAA is unreachable.
FirstAAAReachable	First AAA is alive. The trap is sent when the AAA server is back after being unreachable.	
	Condition	Primary AAA starts replying to Access-Request (KA) messages.
	Value Range	Primary AAA IP address
	Severity	Clear
	Default	Enabled
	Alarm ID[b]	None
	Action	None
	Text	Primary AAA is reachable.
SecondAAAReachable	Second AAA is alive. The trap is sent when the AAA server is back after being unreachable.	
	Condition	Secondary AAA starts replying to Access-Request (KA) messages.
	Value Range	Secondary IP address
	Severity	Clear
	Default	Enabled
	Alarm ID[b]	23
	Action	None
	Text	Secondary AAA is reachable.
EthernetUp	Ethernet link is up.	
	Condition	Base station Ethernet link is up
	Value Range	—
	Severity	Info
	Default	—
	Alarm ID[b]	12
	Action	None
	Text	—

[b] *A Device Alarm ID of 0 means that no alarm is generated.*

Table: RF Traps

Event Name	Description	
AntennaHighReturnLoss	Antenna Disconnected, parameter is radio identifier.	
	Condition	When the average return loss is lower than 6db for 5 seconds. This means that channel i antenna is disconnected and radio powered is on.
	Value Range	Radio 1 | Radio 2
	Severity	Critical
	Default	Enabled
	Alarm ID[c]	5
	Action	Tx off
	Text	Antenna Disconnected, TX turned off.
AntennaNormalReturnLoss	Parameter is radio identifier.	
	Condition	After TX on when the average return loss is in the normal range.
	Value Range	—
	Severity	Clear
	Default	Enabled
	Alarm ID[c]	0
	Action	None
	Text	All Antennas are now connected.
TransmissionStop	BS SW is performing radio off value represent the initiator for the action.	
	Condition	Tx has turned off.
	Value Range	SW API | Other
	Severity	Info
	Default	Disabled
	Alarm ID[c]	0
	Action	None
	Text	Radio is off
TransmissionStart	BS SW is turning on radio value represent the initiator for the action.	
	Condition	Tx has turned on.
	Value Range	SW API | Power Up | Other
	Severity	Info
	Default	Disabled
	Alarm ID[c]	0
	Action	None
	Text	Radio is on

[c] *A Device Alarm ID of 0 means that no alarm is generated.*

Table: Hardware Trap

Event Name	Description	
HWFailure	Such as current cannot converge, power cannot converge, HW not responding, GPS fatal and others. Parameter represent module name i.e. radio 1, Radio 2, GPS.	
	Condition	Any HW Failure Detected that prevents the service.
	Value Range	—
	Severity	Critical
	Default	Enabled
	Alarm ID[d]	6
	Action	TX off
	Text	HW Failure

[d] *A Device Alarm ID of 0 means that no alarm is generated.*

Table: Security Traps

Event Name	Description	
Login	Every login to one of the BS local management interfaces; this allows WiNMS user to be updated.	
	Condition	Successful user login.
	Value Range	User's credentials
	Severity	Warning
	Default	Enabled
	Alarm ID[e]	0
	Action	None
	Text	Login via local CLI/Web has occurred
Login	Every login to one of the BS local management interfaces; this allows WiNMS user to be updated.	
	Condition	Successful user log out.
	Value Range	User's credentials
	Severity	Warning
	Default	Enabled
	Alarm ID[e]	0
	Action	None
	Text	Login via local CLI/Web has occurred
Login	This event should assist operator to recognize hackers trying to enter the network.	
	Condition	Ten (10) consecutive login retries have failed.
	Value Range	—
	Severity	Major
	Default	Enabled

Event Name	Description	
	Alarm ID[e]	0
	Action	None
	Text	Suspicious login failures

[e] *A Device Alarm ID of 0 means that no alarm is generated.*

Table: Environmental Traps

Event Name	Description	
TemperatureFaultLow	Temperature reached first upper threshold, parameter is module name and temperature value.	
	Condition	RF temp exceeds MedRFTemp per sensor limit (developer level)
	Value Range	—
	Severity	Major
	Default	Enabled
	Alarm ID	—
	Action	Decrease TX power by 3 db.
	Text	RF temperature in is above normal
TemperatureFaultHigh	Temperature indicates failure, the transmitter must be off to protect the hardware.	
	Condition	Temp exceeds MaxRFTemp per sensor limit in RF (developer level)
	Value Range	—
	Severity	Critical
	Default	Enabled
	Alarm ID	—
	Action	Stop Tx
	Text	RF temperature failure in channel "I"
TemperatureOk	Temperature returned to normal, I represent channel	
	Condition	RF temp below MedRFTemp[i]*0.8 limit (developer level)
	Value Range	—
	Severity	Clear
	Default	Enabled
	Alarm ID	—
	Action	Reduce attenuator db from TX power
	Text	RF temperature is above normal

Table: Redundancy Traps

Event Name	Description	
BSStatusChangeToMasterOK	Describes BS mastership status change to MasterOK	
	Condition	BS has become a master due to current master failure or election

Event Name	Description	
	Value Range	—
	Severity	Info | Clear (for Duplicate Master Detected trap)
	Default	Enabled
	Alarm ID	—
	Action	None
	Text	—
BSStatusChangeToMasterNotOK	Describes BS mastership status change to MasterNotOK	
	Condition	BS has become a masterNotOK due to failure
	Value Range	—
	Severity	Info
	Default	Enabled
	Alarm ID	—
	Action	None
	Text	—
BSStatusChangeToSlaveReady	Describes BS mastership status change to SlaveReady	
	Condition	BS has become slave ready due to slave not ready that became capable of doing redundancy or election
	Value Range	—
	Severity	Info | Clear (for SlaveNotReady DuplicateMasterDetected traps)
	Default	Enabled
	Alarm ID	—
	Action	None
	Text	—
BSStatusChangeToSlaveNotReady	Describes BS mastership status change to SlaveNotReady	
	Condition	BS has become slave not ready due to failure
	Value Range	—
	Severity	Critical
	Default	Enabled
	Alarm ID	8
	Action	None
	Text	—
NeighborBSUnreachable	Describes the status of the neighbor BS.	
	Condition	No redundancy protocol message received from the neighbor after one of the following timeouts: • MastershipQuery timeout • Wait_For_Master timeout

Event Name	Description	
		• Wait_For_Slave reply timeout
	Value Range	Neighbor BS is unreachable
	Severity	Critical
	Default	Enabled
	Alarm ID	9
	Action	• In case the BS is slave ready -> become master. • In case the BS is master -> declare the neighbor as unreachable.
	Text	—
NeighborBSOK	Indicates that the neighbor BS is reachable.	
	Condition	Redundancy protocol message received
	Value Range	Neighbor BS is reachable
	Severity	Clear
	Default	Enabled
	Alarm ID	—
	Action	None
	Text	—
DuplicateMasterDetected	Indicates that there are 2 master BSs on the network.	
	Condition	Master BS receives MasterStatus message from the neighbor (indicating there is a master)
	Value Range	Duplicate master BS detected, master re-election procedure is in process.
	Severity	Critical
	Default	Enabled
	Alarm ID	10
	Action	Go to Master Election
	Text	—
NetworkTestFail	Networking test fails.	
	Condition	No ping to AAA or ASN-GW.
	Value Range	—
	Severity	Critical
	Default	Enabled
	Alarm ID	13
	Action	The BS becomes “slave not ready”.
	Text	—
NetworkTestOK	Networking test successful.	
	Condition	Successful ping to AAA or ASN-GW.

Event Name	Description	
	Value Range	—
	Severity	Info | Clear
	Default	Enabled
	Alarm ID	14
	Action	The BS becomes “slave ready”.
	Text	—

Table: Services Traps

Event Name	Description	
SF not established for CPE	SF establishment failure. CPE de-registration will occur.	
	Condition	After network entry, the CPE is Operational and ISF fails to establish.
	Value Range	CPE MSID = “fill in the MSID”
	Severity	Major
	Default	Enabled
	Alarm ID	—
	Action	De-register the CPE
	Text	—
Secondary SF not established for CPE	Secondary SF establishment failure.	
	Condition	After network entry, the CPE is Operational, ISF is established, but one of the secondary SFs fails to establish
	Value Range	CPE MSID = “fill in the MSID” + “fill in the SF name” service cannot be provided to the CPE.
	Severity	Major
	Default	Enabled
	Alarm ID	—
	Action	None
	Text	—

Table: Link Status Traps

Event Name	Description	
LinkUp	CPE is operational. Clears the LinkDown and LinkFlap traps.	
	Condition	CPE has performed successful INE(=OPERATIONAL)
	Value Range	—
	Severity	Info
	Default	Enabled
	Alarm ID[f]	—

Event Name	Description	
	Action	—
	Text	—
LinkDown	CPE link is down.	
	Condition	CPE is de-registered from the network.
	Value Range	Unknown reason | Manual Dereg | DL Sync failure | UL Acquisition failure | Ranging failure | Capabilities Negotiation failure | Authorization failure | Registration failure
	Severity	Major
	Default	Enabled
	Alarm ID[f]	—
	Action	—
	Text	—
LinkFlap	CPE link is flapping	
	Condition	CPE is de-registered from the network and cannot complete INE
	Value Range	DL Sync failure | UL Acquisition failure | Ranging failure | Capabilities Negotiation failure | Authorization failure | Registration failure
	Severity	—
	Default	—
	Alarm ID[f]	—
	Action	—
	Text	—
LinkUpButCPENotInService	Link is functioning but CPE is not in service.	
	Condition	—
	Value Range	—
	Severity	—
	Default	—
	Alarm ID[f]	—
	Action	—
	Text	—

[f] *A Device Alarm ID of 0 means that no alarm is generated.*

Section 4.6

Log Management

On the **Syslog Configuration** and **Log Files** panes, you configure the log management options. The options include setting the server to which log files are sent, and the maximum size of each log file. On the **Log Files**

pane, you can upload the log files to the specified server. For instructions on setting the maximum log file size and for uploading the log files to the specified server, refer to Section 4.6.1, “Log Files”.

Procedure: Setting Syslog Configuration Options

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Logs Management** link. The **Syslog Configuration** pane appears.

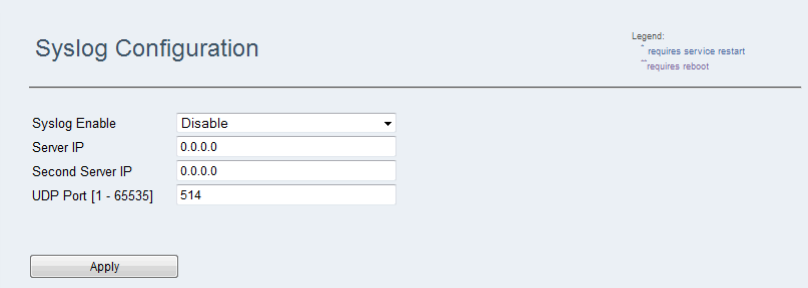


Figure 51: Syslog Configuration pane

3. Review and set the syslog configuration parameters in the following fields:

Parameter	Description
Syslog Enable	**Synopsis:** { Enable | Disable } **Default:** Disable Enables or disables logging.
Server IP	**Synopsis:** { IPv4 address } **Default:** 0.0.0.0 Sets the IP address of the server to which log files are uploaded. Type an IPv4 address.
Second Server IP	**Synopsis:** { IPv4 address } **Default:** 0.0.0.0 Sets the IP address of the server to which log files are uploaded. Type an IPv4 address.
UDP Port (1-65535)	**Synopsis:** { Number in the range of 1 to 65535 } **Default:** 514 Sets the UDP port on the server to use when uploading the log files to the server. Type a value in the range of 1 to 65535.

4. Click **Apply**.

For instructions on setting the maximum log file size and for uploading the log files to the specified server, refer to Section 4.6.1, “Log Files”.

Section 4.6.1

Log Files

On the **Log Files** pane, you configure the maximum size of the log files and upload the files to the server specified on the **Syslog Configuration** pane. For instructions on setting the upload destination server, refer to Section 4.6, “Log Management”. For a description of the types of events that are logged, refer to Section 4.6.2, “Logged Events”.

Procedure: Displaying the Log Files Pane

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Logs Management** link and then click the **Log Files** link. The **Log Files** pane appears.

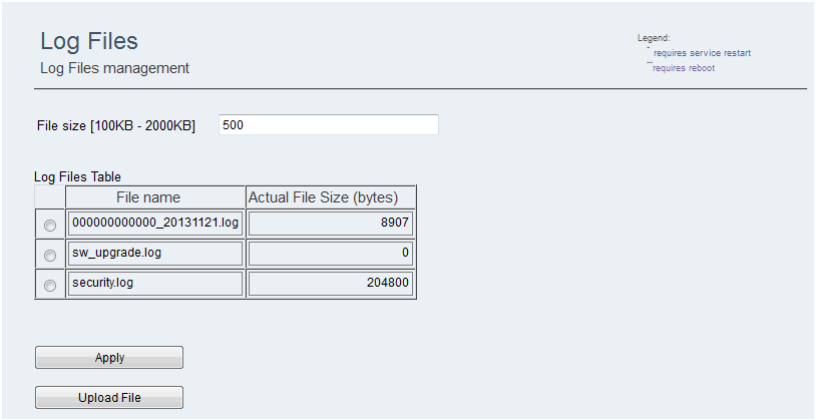


Figure 52: Log Files pane

Procedure: Setting Log File Sizes

1. On the **Log File** pane, in the **Log Files Table**, select one or more log files.
2. In the **File Size [100KB - 2000KB]** field, type a value in the range of 100 to 2000.
3. Click **Apply**.

   The selected files are now limited to the size you specified in the **File Size [100KB - 2000KB]** field.

Procedure: Uploading Log Files

1. On the **Log File** pane, in the **Log Files Table**, select one or more log files.
2. Click **Upload File**.

   The selected files are uploaded to the server specified on the **Syslog Configuration** pane.

Section 4.6.2
Logged Events

The following types of log files exist and log events in the system.

- Time stamped file - logs Sequans events
- sw_upgrade.log - logs upgrade information
- security.log - logs security events that occur in the base station and the CPE, including those related to login, logout, configuration changes, SNMP and other events.

5 Setup and Configuration

This chapter describes how to set up and configure the device for use on a network using the various features available in the RUGGEDCOM WIN. It describes the following tasks:

Section 5.1

Managing Quality of Service

NOTE
Quality of Service (QoS) capabilities only apply to base stations in Standalone mode. In ASN-GW mode, QoS management is performed through the ASN-GW.

By default, subscriber stations (CPE devices) are assigned a Best Effort (BE) service profile for the uplink and downlink channels. Only the maximum bandwidth can be configured for the default service profile.

Subscriber stations can be assigned a number of user-defined uplink and downlink Service Flows (SF). A service flow is a unidirectional flow of medium access control (MAC) service data units (SDUs) on a connection.

A connection is a unidirectional mapping between base station and subscriber station medium access control (MAC) peers for the purpose of transporting a service flow’s traffic. Connections are identified by a connection identifier (CID). A service flow is characterized by a set of QoS parameters, such as latency, jitter, and throughput assurances. Any number of service flows can be defined for the uplink and for the downlink.

A service profile is a set of service flows assigned to a subscriber station. The service profiles correspond to the QoS requirements of the subscriber station.

For example, a service profile can consist of the following service flows: one flow matching VoIP needs, a second flow matching video conferencing needs, and a third flow matching web browsing needs.

Service profiles and their service flows are defined and allocated through the Subscribers panes.

The following sections describe how to manage QoS capabilities:

Section 5.1.1

QoS Definition Workflow

Follow these general steps to define service flows and assign them to subscriber stations:

1. Define a service profile.
2. Define a set of uplink and downlink service flows within the service profile.
3. For each service flow, define the relevant attributes, such as Classification-Rule-Priority, Scheduling, Minimum and Maximum Rates, Latency, and other parameters.
4. If required for each service flow, define relevant classifiers. Classifiers determine the traffic to which the service flow is applied. Traffic can be defined according to the traffic source, traffic type, or combination of traffic source and type. For example, traffic can be defined by DSCP range, port range, IP address source or destination, and other parameters. The base station performs a logical OR when considering traffic types.
5. Define the MAC address of the subscriber station to which the service flows are to be assigned.
6. Define the QoS profile for the subscriber station by assigning it the relevant Service Flows.

NOTE
When changing service profiles, you must perform a CPE de-registration to restart the service on the CPE to which the service flow is applied.

Section 5.1.2

Defining Service Profiles

Create and manage service profiles on the **Service Profiles** pane.

On the **Service Profiles** pane, you create and manage service profiles. You then assign service flows to the service profiles. On this pane, you can view the list of subscribers to each profile, activate and deactivate profiles, and apply updated profiles to their subscribers.

Procedure: Defining Service Profiles

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Services** link and then click the **Service Profiles** link. The **Service Profiles** pane appears.

Figure 53: Service Profiles pane

3. To add a new service flow, click the + button. A new row appears in the **Configured Service Profiles Table**. In the **Service Profile Name** field, type a name for the new profile. The table can contain up to 32 rows.
4. To show a list of subscribers for a service profile, select a service profile from the table and click **Subscribers**.
5. To add or edit service flows, select a service profile from the table and click **Add/Edit Service Flows**. The **Unicast Service Flows** pane appears. For instructions on how to add service flows, refer to Section 5.1.3, “Unicast Service Flows”.
6. To activate or deactivate a one or more service profile, select one or more rows from the table and click **Set Activation On/Off**. The selected profiles are activated if they were inactive, or are deactivated if they were active.
7. To apply an updated profile to its subscribed members, select one or more rows from the table and click **Update profile**.

> **NOTE**
> *Updating the profile de-registers all CPEs associated with the profile.*

8. To save your changes, click **Apply**.

Section 5.1.3

Unicast Service Flows

The **Unicast Service Flow** pane appears when you click **Add/Edit Service Flows** on the **Service Profiles** pane.

On this pane, you define a pool of service flows, where each flow is assigned a range of attributes. You then assign selected service flows to subscriber stations.

Procedure: Defining Unicast Service Flows

1. On the **Service Profiles** pane, select a service profile from the **Configured Service Profiles Table** and click **Add/Edit Service Flows**. The **Unicast Service Flows** pane appears.

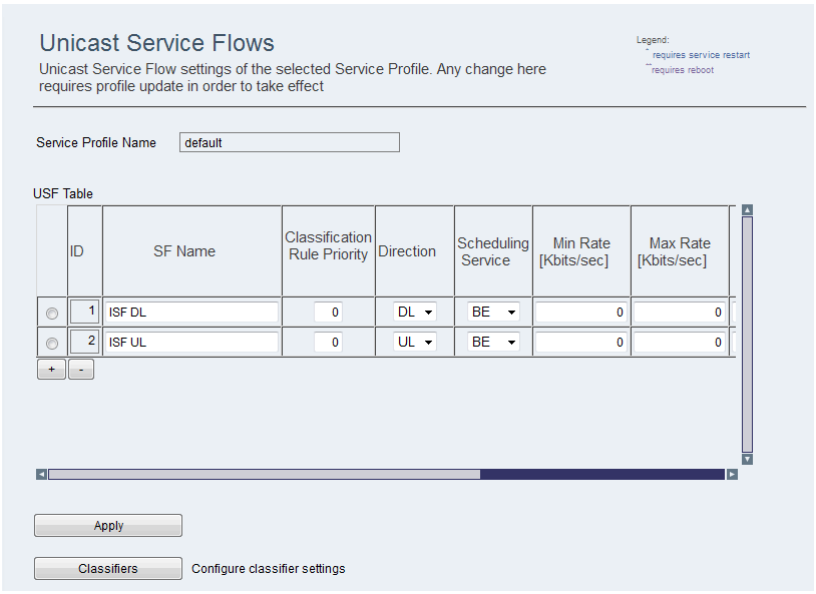


Figure 54: Unicast Service Flows pane

2. Review and set the unicast service flows in the **USF Table**.

   The top two rows in the table display the default Best Effort (BE) uplink and downlink service flows. In these service flows, only the maximum bandwidth value can be modified.

   The default service flows do not provide QoS to the subscriber station. QoS is only provided by assigning the subscriber station a profile based on user-defined service flows.

   You can add up to 30 rows to the table. Each subscriber station can be assigned up to 4 service flows.

   After changing any service flow definition, the CPE must re-register with the network.

Table: The USF Table

Column	Description
SF Num	Displays the service flow identifier. This field is read-only. The number is assigned automatically when you create a new service flow.
SF Name	Sets the service flow now. When setting a name, include the service flow direction (UL or DL).
Classification Rule Priority	Sets the classification rule priority Values: A number in the range of 0 to 255. The Priority Level determines how the service flow data is classified. The same priority can be assigned to an uplink and to a downlink service flow, but the Classification Rule Priority must be unique for each uplink service flow and downlink service flow. That is, there cannot be two service flows in the same direction with the same rule priority. This parameter is related to the classifier lookup mechanism, but is not related to traffic scheduling itself.
Direction	Sets the direction to which the SF is assigned: Downlink (DL) or Uplink (UL).
Scheduling Service	Sets the Service Scheduling Flows supported by WiMAX. For more information, refer to Table "Scheduling Service".
Min Rate [Kbits/sec]	Sets the minimum bandwidth (BW) rate for this service flow.

Column	Description
Max Rate [Kbits/sec]	Sets the maximum bandwidth (BW) rate for this service flow. A value of 0 (zero) provides an unlimited rate.
Traffic Priority	Sets the priority among service flows.
Unsolicited Grant Interval (UL only) [ms]	For RT (Real Time) and nRT (Non-Real Time) polling, sets the interval (in milliseconds) between successive grant opportunities for the traffic flow. This setting applies to the uplink only.
Unsolicited Polling Interval (UL only) [ms]	For UGS (Unsolicited Grant Service) and eRT (Extended Real Time) polling, sets the maximum interval (in milliseconds) between successive polling grant opportunities for the traffic flow. This setting applies to the uplink only.
HARQ Max Retries	Sets the maximum number of Hybrid Automatic Repeat Request (HARQ) attempts.
Latency [msec]	Sets the maximum permitted latency (in milliseconds), starting at the arrival of a packet until its successful transmission to its destination.

This table shows the values supported in the **Scheduling Service** column of the **USF Table**.

Table: Scheduling Service

Service Flow Designation	Defining QoS Parameters	Application Examples
UGS — Unsolicited Grant Services	Maximum sustained rate Maximum latency tolerance Jitter tolerance	Voice over IP (VoIP) without silence suppression
RT — Real-Time Polling service	Minimum reserved rate Maximum sustained rate Maximum latency tolerance Traffic priority	Streaming audio and video, MPEG encoded
nRT — Non-Real-Time Polling service	Minimum reserved rate Maximum sustained rate Traffic priority	File Transfer Protocol (FTP)
BE — Best-effort service	Maximum sustained rate Traffic priority	Web browsing, data transfer
eRT - Extended-Real-Time Polling service	Minimum reserved rate Maximum sustained rate Maximum latency tolerance Jitter tolerance Traffic priority	VoIP with silence suppression

3. To add a new service flow, click the + button.

   The table can contain up to 30 rows.
4. To remove a row from the table, select one or more rows from the table and click the - button.
5. After making changes to the table, click **Apply**.
6. To add classifiers to the service flow, click **Classifiers**. For more information on adding classifiers, refer to Section 5.1.4, “Unicast Service Flow Traffic Classifiers”.
7. To view subscribers to the service flow, click **Subscribers**. For more information on working with subscribers, refer to Section 5.1.5, “Assigning Service Profiles to Subscriber Stations”.
8. After changing any service flow definition, the CPE must re-register with the network. Follow these steps to reset subscriber station-base station connectivity.

To reset the connection of a single subscriber station (where the service flow is applied on a *Registration Base*):

a. Click **Subscribers**. The **Subscribers** links appear in the options pane.

b. In the options pane, click the **Subscriber Management** link. The **Registered SS** pane appears.

c. In the **SS Table**, select a subscriber station.

d. Click **Deregister**.

To reset the connection of all subscriber stations (where the service flow is applied to *All Users*):

a. Click **Quick Start**. The **Quick Start Settings** pane appears.

b. Click **Stop Service**, and then click **Start Service**.

Section 5.1.4

Unicast Service Flow Traffic Classifiers

The **Unicast SF classifiers** pane appears when you click **Classifiers** on the **Unicast Service Flows** pane.

On this pane, you select traffic rules according to which traffic is mapped to the service flow. The traffic can be selected according to traffic source and destination, DSCP, and IP protocol.

Up to *four classifiers* can be defined for each service flow. Data is analyzed according to each of the classifiers assigned to the service flow until a match is found (the system performs a logical OR). The order of classifier lookup is determined by the classification rule priority. Each classifier consists of either one or two filtering rules (for example: traffic source from a specific IP address and a specific Port, or DSCP range of traffic type). In case two filtering values are taken into consideration for one classifier, the system performs a logical AND between them.

Procedure: Setting Unicast Traffic Classifiers

1. On the **Unicast Service Flows** pane, select a service flow.
2. Click **Classifiers**. The **Unicast SF classifiers** pane appears.

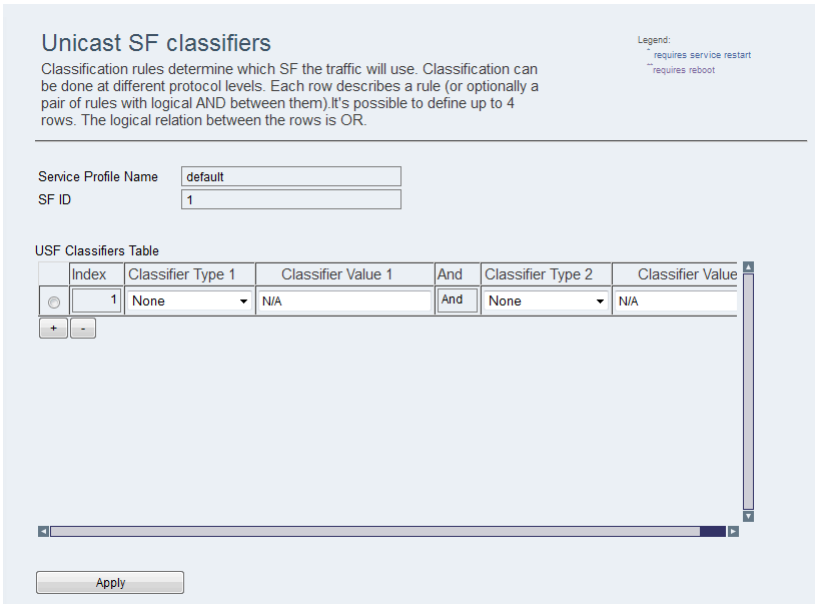


Figure 55: Unicast SF classifiers pane

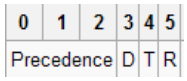
3. Review and set the classifiers in the **USF Classifiers Table**.

Table: Classifier Types and Values

Column	Description
Index	Displays the classifier identifier. This field is read-only. The index number is assigned automatically when you create a new classifier.
Classifier Type 1 Classifier Type 2	Sets the type of traffic for the classifier. • MAC src — source MAC address. • MAC dest — destination MAC address. • IP src — source IP address. • IP dest — destination IP address. • Port src — source port. • Port dest — destination port. • DSCP — DSCP Range Mask (**DSCP** field, providing differentiated services codepoint). The DSCP is the first six bits of the TOS (Type of Service) byte of the IP packet header. • IP protocol — value of the IP header field determining the upper layer protocol (such as TCP, UDP, and others).
Classifier Value 1 Classifier Value 2	The traffic-classification value for the type selected in the **Classifier Type 1** or **Classifier Type 2** field. For more information, refer toTable "Classifier Values".

Table: Classifier Values

Classifier Type	Classifier Value Description	Classifier Value Example	Comment
MAC src MAC dest	MAC address with optional mask	11:22:33:44:55:66/48	Mask is optional. Default is /48.
IP src IP dest	IP address with optional mask	192.168.1.1/32	Mask is optional. Default is /32.

Classifier Type	Classifier Value Description	Classifier Value Example	Comment
Port src Port dest	Port range	1230-1250	
DSCP Range Mask	toslow:toshigh:tosmask Range of TOS values followed by the TOS mask. • To specify a simple range, such as X through Y, enter the range as X:Y. The tosmask is not required. • To specify a complex range, such as X through Y and Z through A (where there is a gap between Y and Z), enter the range as X:A:mask. • To specify a single DSCP value, such as the single value X, enter the value as X. The toshigh and tosmask values are not required.	13:57:63	 **Bits 0, 1, 2:** IP precedence bits value: 0-7 indicate datagram importance. Default = 0; higher is better. **Bits 3,4,5:** Values: D,T,R requesting: low delay, high throughput, high reliability
IP Protocol	IP Protocol	6	6 represents TCP. Valid values are in the range of 0 to 255

4. To add a new classifier, click +.

   The table can contain up to 4 rows.

5. To remove a row from the table, select one or more rows from the table and click -.
6. After making changes to the table, click **Apply**.
7. To return to the **Unicast Service Flows** pane, click **Back**.
8. After changing any service flow definition, the CPE must re-register with the network. Follow these steps to reset subscriber station-base station connectivity.

   To reset the connection of a single subscriber station (where the service flow is applied on a *Registration Base*):

   a. Click **Subscribers**. The **Subscribers** links appear in the options pane.

   b. In the options pane, click the **Subscriber Management** link. The **Registered SS** pane appears.

   c. In the **SS Table**, select a subscriber station.

   d. Click **Deregister**.

   To reset the connection of all subscriber stations (where the service flow is applied to *All Users*):

   a. Click **Quick Start**. The **Quick Start Settings** pane appears.

   b. Click **Stop Service**, and then click **Start Service**.

Section 5.1.5

Assigning Service Profiles to Subscriber Stations

After defining the pool of service flows, the service flows can be can be assigned to subscriber stations according to QoS requirements.

To assign a service flow, define the MAC address of the subscriber stations in the **Pre-provisioned SS** pane, and then assign the MAC address to the relevant service flows.

After assigning service flows to a subscriber station, reset the connection between the subscriber station and the base station.

NOTE
Resetting the connection between the subscriber station and the base station is required when applying any change to a service flow that is allocated to the subscriber station.

Procedure: Setting Subscriber Station Service Profiles

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Pre-provisioned SS** link. The **Pre-provisioned SS** pane appears.

Figure 56: Pre-provisioned SS pane

3. **To add a new subscriber station, do the following:**
   a. Click the + button. A new row appears in the table.
   b. In the **SS ID** field, type the MAC address of the subscriber station.
   c. Click **Apply**.
4. **To set the service flows for a subscriber station, do the following:**
   a. Select a subscriber station from the list.
   b. Click **Service Profile**. The **Service Profile Subscription** pane appears.

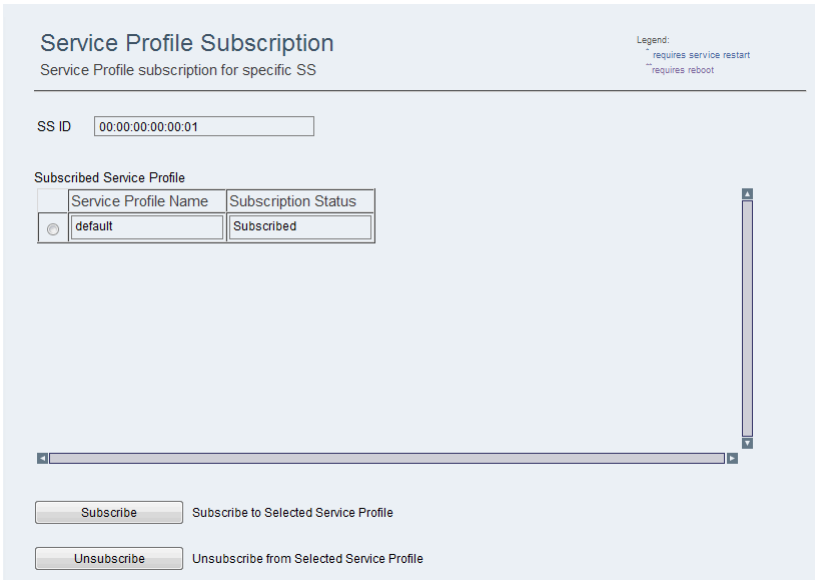


Figure 57: Service Profile Subscription pane

c. To add a service flow to the subscriber station, select one or more service flows from the list and click **Subscribe**.

d. To remove a service flow from the subscriber station, select one or more service flows from the list and click **Unsubscribe**.

5. After changing any service flow definition, the CPE must re-register with the network. Follow these steps to reset subscriber station-base station connectivity.

   To reset the connection of a single subscriber station (where the service flow is applied on a *Registration Base*):

   a. Click **Subscribers**. The **Subscribers** links appear in the options pane.

   b. In the options pane, click the **Subscriber Management** link. The **Registered SS** pane appears.

   c. In the **SS Table**, select a subscriber station.

   d. Click **Deregister**.

   To reset the connection of all subscriber stations (where the service flow is applied to *All Users*):

   a. Click **Quick Start**. The **Quick Start Settings** pane appears.

   b. Click **Stop Service**, and then click **Start Service**.

Section 5.1.6

Configuring VLAN Subscriptions

The **VLAN Subscription** pane displays the VLAN subscriptions for specific subscriber stations.

Procedure: Configuring VLAN Subscriptions

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Pre-provisioned SS** link. The **Pre-provisioned SS** pane appears.

Figure 58: Pre-provisioned SS pane

3. Select a subscriber station from the list.
4. Click **VLAN**. The **VLAN Subscription** pane appears.

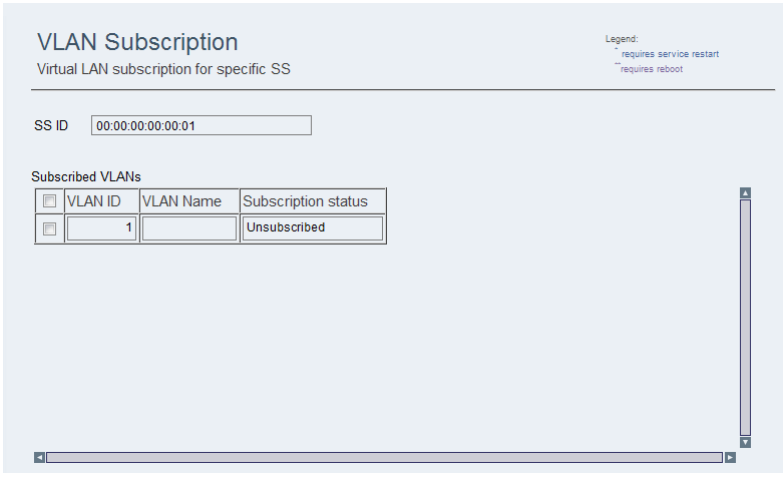


Figure 59: VLAN Subscription pane

5. To subscribe, select one or more VLANs from the list and click **Subscribe**.
6. To unsubscribe, select one or more VLANs from the list and click **Unsubscribe**.

Section 5.1.7

SS Configuration

The **SS Configuration** pane displays the SS configuration parameters.

Procedure: Setting the SS Configuration Parameters

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Pre-provisioned SS** link. The **Pre-provisioned SS** pane appears.

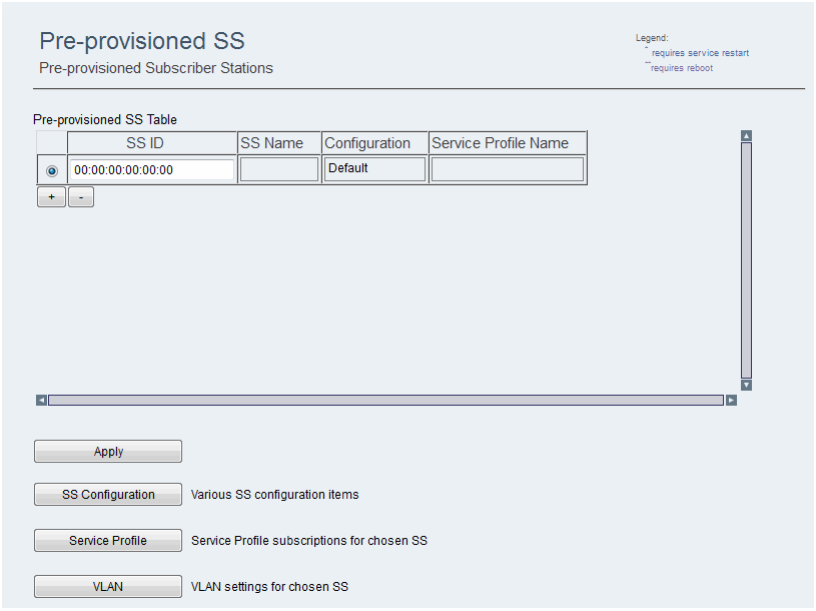


Figure 60: Pre-provisioned SS pane

3. Select a subscriber station from the list.
4. Click **SS Configuration**. The **SS Configuration** pane appears.

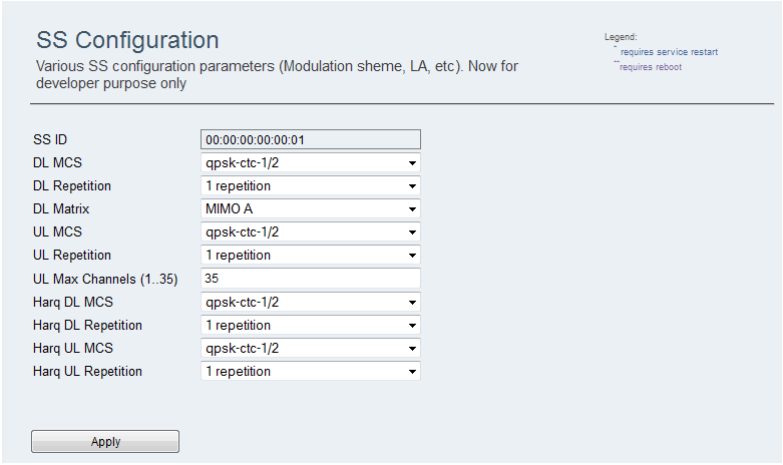


Figure 61: SS Configuration pane

5. Review and set the parameters in the following fields.

Parameter	Description
SS ID	Displays the subscriber station identifier.
DL MCS	**Synopsis:** { qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6 } The DL MCS for the SS device.
DL Repetition	**Synopsis:** { 1 repetition, 2 repetitions, 4 repetitions, 6 repetitions } The DL repetition for the SS device (valid only for QPSK-1/2).
DL Matrix	**Synopsis:** { SISO, MIMO A, MIMO B } The MIMO configuration of the SS device.
UL MCS	**Synopsis:** { qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6 } The UL MCS for the SS device.
UL Repetition	**Synopsis:** { 1 repetition, 2 repetitions, 4 repetitions, 6 repetitions } The UL repetion for the SS device (valid only for QPSK-1/2).
UL Max Channels (1..35)	The UL MAX allocated subchannels for the SS device.
Harq DL MCS	**Synopsis:** { qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6 } The DL Static Harq MCS for the SS device.
Harq DL Repetition	**Synopsis:** { 1 repetition, 2 repetitions, 4 repetitions, 6 repetitions } The static symbol repetitions for the SS device.
Harq UL MCS	**Synopsis:** { qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6 } The UL Static Harq MCS for the SS device.
Harq UL Repetition	**Synopsis:** { 1 repetition, 2 repetitions, 4 repetitions, 6 repetitions } The static symbol repetitions for the SS device.

6. Click **Apply**.

Section 5.1.8

Monitoring and Maintaining Registered Subscriber Station Connections

The **Registered SS** pane displays a summary of the registered subscriber station's basic operating information. This panel also provides basic maintenance controls.

Procedure: Viewing Registered Subscriber Station Information

1. Click **Subscribers**. The **Registered SS** pane appears.

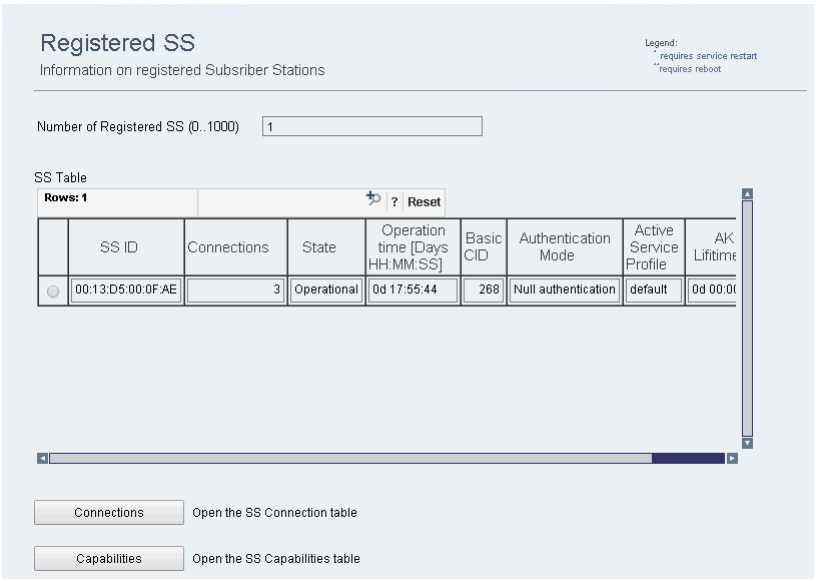


Figure 62: Registered SS pane

2. The **SS Table** displays all of the registered subscriber stations. Information about each subscriber station is displayed in the following columns:

Table: SS Table

Column	Description
SS ID	Displays the subscriber station identifier.
SS Name	Displays the subscriber station name.
Connections	The number of downlink and uplink connections to and from the subscriber station.
State	The operating state of the subscriber station. For more information, refer to Table "Subscriber Station Operating States".
Operation time [Days HH:MM:SS]	Displays the elapsed time since the CPE registered with the base station.
Basic CID	Displays the connection identifier.
Authentication Mode	Indicates if the CPE has entered the base station as unauthenticated or if it passed authentication. Values: Null authentication | PKMv2.0
Active Service Profile	Displays the current service profile name.
AK Lifetime	Displays the subscriber station authorization key lifetime.
Next Re-Authentication	Displays the next subscriber station re-authentication.

Table: Subscriber Station Operating States

Subscriber Station Operating state	Description
Init	Initial state.
DL Synchronization	MS seeks a valid preamble and DL MAPS.

Subscriber Station Operating state	Description
Ranging	Subscriber station is in ranging state. Power, frequency and timing correction are sent to MS by the base station.
Handover ranging	Subscriber station has started the handover process.
Capabilities negotiation	Subscriber station and base station are exchanging capability parameters (authentication support, number of service flows supported, different modulations supported, and other parameters).
Authorization	Subscriber station is being authorized.
Registration	Service Flows are being created.
Operational	Subscriber station has completed its entry to the network.
Sleep	MS is in sleep mode.
IDLE	MS is in idle mode.

3. To view information for a subscriber station, select a subscriber station in the table and click one of the following buttons:
   - **Connections** — displays the **SS Connections** pane. For more information, refer to Section 5.1.8.3, “Subscriber Station Connections pane”.
   - **Capabilities** — displays **SS Capabilities** pane. For more information, refer to Section 5.1.8.5, “Subscriber Station Capabilities pane”.

Section 5.1.8.1
SS Remote Recovery Functions pane

The **SS Remote Recovery Functions** pane provides recovery functions for the subscriber stations that you can use remotely from the base station. You can reset the password, deregister the subscriber station from the base station and reboot the subscriber station.

Procedure: Using Remote Recovery Functions

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Recovery Options** link. The **SS Remote Recovery Functions** pane appears.

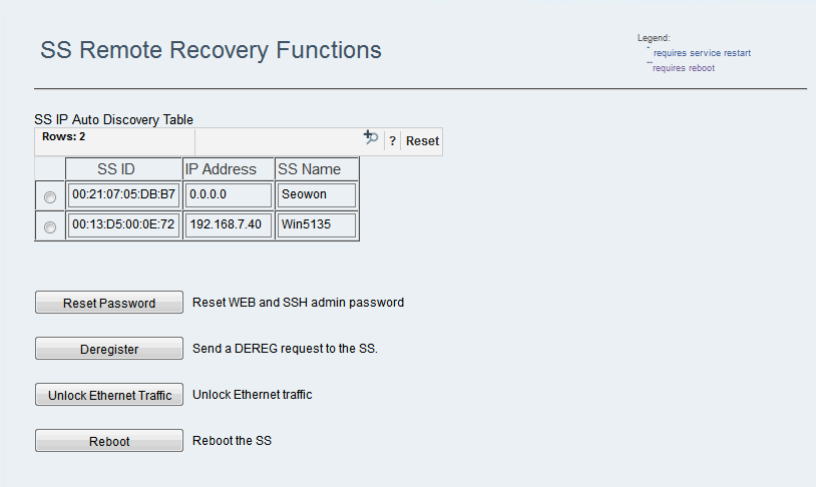


Figure 63: SS Remote Recovery Functions pane

3. To use one of the remote recovery functions, select a subscriber station in the table and click one of the following buttons:
   - **Reset Password** — resets the admin access level password to the default password. For more information about the admin default password, refer to Section 2.4, “Logging In”. For more information about how to change passwords, refer to Section 4.1.1, “Adding Users”.
   - **Deregister** — resets the connection between the base station and the selected subscriber station. The base station sends a DEREG request to the subscriber station and deletes the subscriber station from the lists.
   - **Reboot** — reboots the subscriber station.

Section 5.1.8.2
Unlocking Devices

When the Ethernet Lock feature is enabled in a CPE, and the Ethernet is disconnected for any reason, the device will automatically lock and no data will be forwarded. The feature can be reset from the base station GUI without the need for remote log in.

To unlock the device, do the following:

1. Navigate to ***Subscribers » Recovery Options***. The **SS Remote Recovery Functions** screen appears.

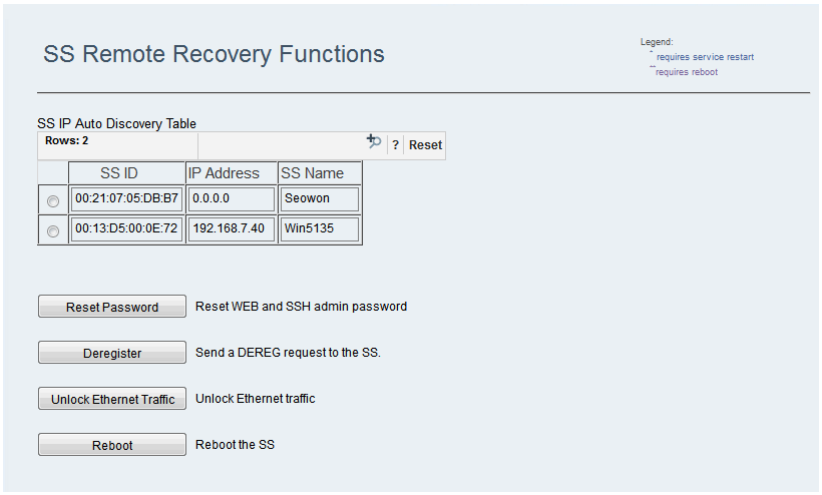


Figure 64: SS Remote Recovery Functions

2. From the **SS IP Auto Discovery Table**, select the locked CPE.
3. Click **Unlock Ethernet Traffic**.
4. When prompted, answer **OK**.

Section 5.1.8.3

Subscriber Station Connections pane

The **SS Connections** pane appears when you select a subscriber station on the **Registered SS** pane and click **Connections**. This pane displays information about connections to the selected subscriber station.

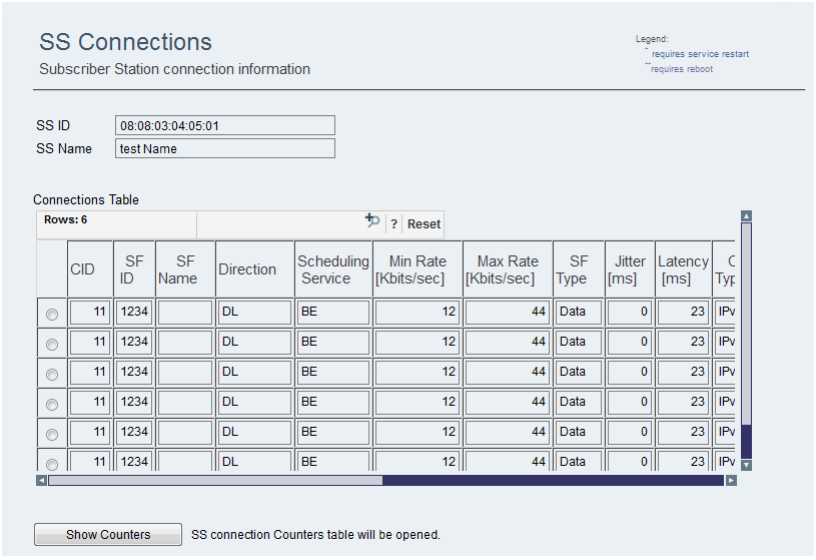


Figure 65: SS Connections pane

- To return to the **Registered SS** pane, click **Back**. For more information, refer toSection 5.1.8, “Monitoring and Maintaining Registered Subscriber Station Connections”.
- To view subscriber station connection counters, click **Show Counters**. For more information, refer toSection 5.1.8.4, “Subscriber Station Connection Counters pane”.

Section 5.1.8.4
Subscriber Station Connection Counters pane

The **SS Connection Counters** pane appears when you click **Show Counters** on the **SS Connections** pane. This pane displays connection information, including the packets dropped, the packets sent, and the bytes sent.

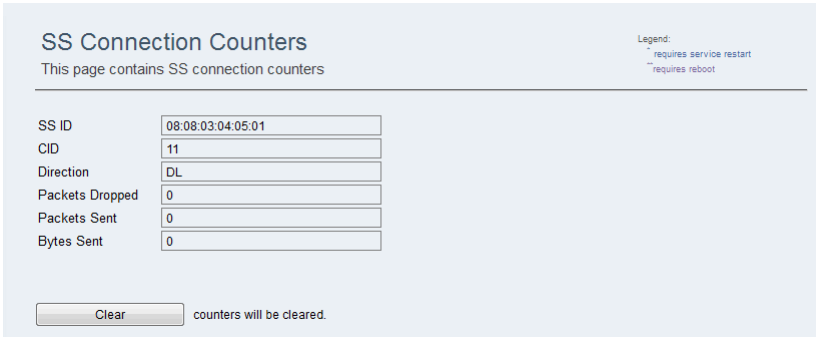


Figure 66: SS Connection Counters pane

- To return to the **SS Connections** pane, click **Back**. For more information, refer toSection 5.1.8.3, “Subscriber Station Connections pane”.
- To clear the counters, click **Clear**.

Section 5.1.8.5
Subscriber Station Capabilities pane

The **SS Capabilities** pane appears when you select a subscriber station on **Registered SS** pane and click **Capabilities**. This pane displays the capabilities that the subscriber station has negotiated with the base station.

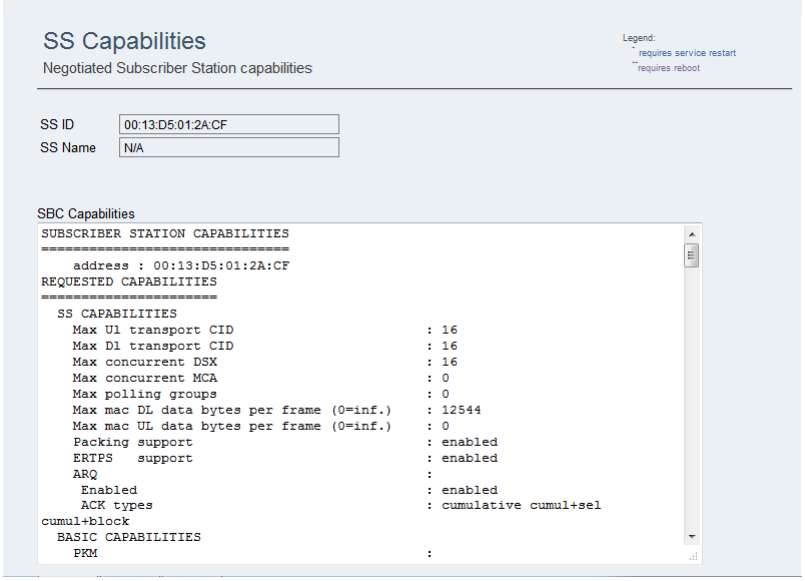


Figure 67: SS Capabilities pane

- To return to the **SS Connections** pane, click **Back**. For more information, refer toSection 5.1.8.3, “Subscriber Station Connections pane”.

Section 5.1.8.6

Registered SS IP Addresses

Use the **Registered SS IP Addresses** pane to discover IP addresses of devices and open the interfaces of Subscriber Stations.

Procedure: Displaying the Registered SS IP Addresses Pane

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options panel, click the **SS IP Addresses** link. The **Registered SS IP Addresses** pane appears.

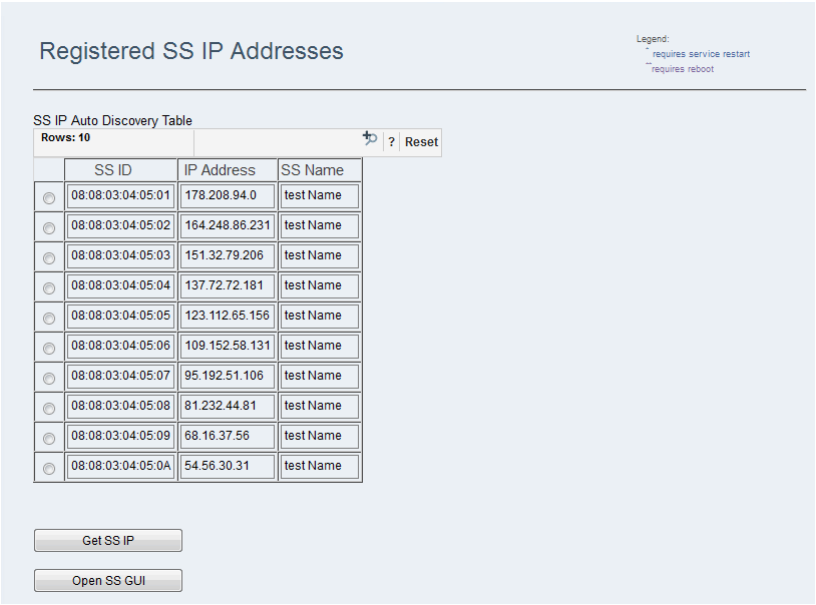


Figure 68: Registered SS IP Addresses pane

3. Review the parameters in the following fields:

Parameter	Description
SS ID	Displays the SS ID information.
IP Address	Displays the IP Address of the subscriber station.

Procedure: Discovering SS IP Addresses

1. On the **Registered SS IP Addresses** pane, in the SS IP Auto Discovery Table, select an entry in the **SS IP Auto Discovery Table**.
2. Click **Get SS IP**.

Procedure: Opening an Interface for a Subscriber Station

1. On the **Registered SS IP Addresses** pane, in the SS IP Auto Discovery Table, select an entry in the **SS IP Auto Discovery Table**.
2. Click **Open SS GUI**.

Section 5.1.9

Configured VLANs

The **Configured VLAN Services** pane provides information for configuring the VLAN service flow for the base station. The configuration parameters include the VLAN ID number, VLAN name, subscriber base (the option to select either a registered subscriber or all subscribers), broadcast maximum rate, and broadcast traffic priority. **Subscribers** at the bottom of the pane displays a list of subscriber stations subscribed to the selected VLAN.

Procedure: Displaying VLAN Services

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Services** link and then click the **Configured VLANs** link. The **Configured VLAN Services** pane appears.

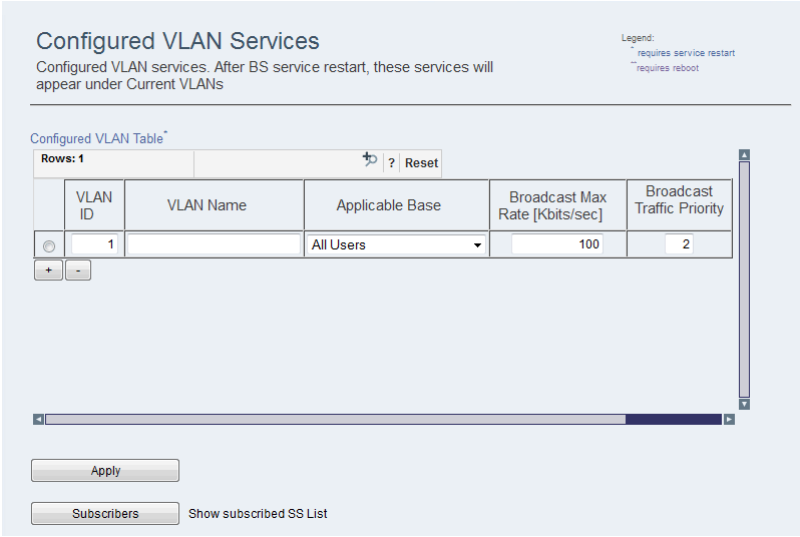


Figure 69: Configured VLAN Services pane

3. Review the VLAN services in the **Configured VLAN Table**:

Table: Configured VLAN Table

Column	Description
VLAN ID	Displays the VLAN identifier.
VLAN Name	Displays the name of the VLAN multicast connection.
Applicable Base	Indicates a CPE association with the VLAN multicast connection. Similar to the unicast service flows, the subscription to the VLAN multicast connection can be All Users or Registration Base.
Broadcast Max Rate	Displays the VLAN-tagged broadcast traffic rate limitation. Default: 100 kbits/s
Broadcast Traffic Priority	Displays the VLAN-tagged broadcast traffic priority (for Quality of Service). Default: 0

4. To add a new VLAN service, click +. Define the VLAN service with the fields in the new row.
5. To remove a row from the table, select one or more rows from the table and click -.
6. After making changes to the table, click **Apply**.
7. To view a list of subscribers for a VLAN service, select a service from the table and click **Subscribers**.
8. If you edited or added rows to the **Configured VLAN Table**, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 5.1.10

Configuring VLAN-Based Service Flows

Follow these steps to configure a VLAN-based service flow.

1. Configure a VLAN multicast service flow from the **Services** menu.
2. Activate the VLAN multicast service flow by rebooting the base station from the **Quick Start Settings** page.
3. Verify the VLAN Multicast service flow created in **Current VLAN** under the **Services** menu.
4. Create a unicast service flow for VLAN by selecting **Service Profiles** and then **Unicast Service Flows** in the **Services** menu.
5. Add a VLAN ID classifier to the unicast service flow in the **Services** menu.
6. Add a subscriber station MAC to the pre-provisioned subscriber station table in the **Pre-provisioned Subscriber Station** menu.
7. Select the subscriber and select **Service Profile** at bottom of the pane.
8. Select the service flow (with the VLAN classifier) and select **Subscribe** at the bottom of the pane.
9. Repeat Step 7 and Step 8 for subscribing the multicast service flow to the subscriber station by selecting **VLAN** at the bottom of the **Pre-provisioned** pane.
10. Verify that the subscriber station is subscribed with the required unicast and multicast service flows for the VLAN.
11. To apply the new VLAN service flows to the subscriber station, de-register the subscriber station from the **Subscriber** menu.

Section 5.1.11

Current VLANs

The **Current VLAN Services** pane provides information about configured VLANS. It includes the values for the VLAN ID number, the VLAN name, the VLAN applicable base (either a registered subscriber or all subscribers), broadcast maximum rate, and broadcast traffic priority.

Procedure: Viewing Current VLANs

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Services** link and then click the **Current VLANs** link. The **Current VLAN Services** pane appears.

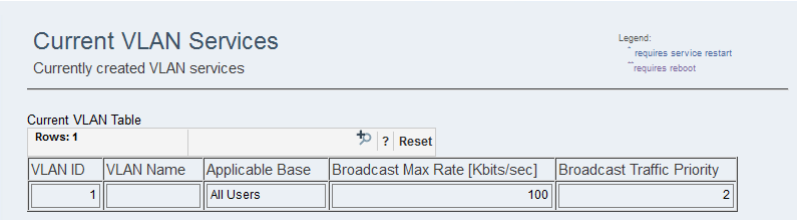


Figure 70: Current VLAN Services pane

3. Review the VLAN services in the **Current VLAN Table**:

Table: Current VLAN Table

Column	Description
VLAN ID	Displays the VLAN identifier.
VLAN Name	Displays the name of the VLAN multicast connection.
Applicable Base	Indicates a CPE association with the VLAN multicast connection. Similar to the unicast service flows, the subscription to the VLAN multicast connection can be All Users or Registration Base.
Broadcast Max Rate	Displays the VLAN-tagged broadcast traffic rate limitation. Default: 100 kbits/s
Broadcast Traffic Priority	Displays the VLAN-tagged broadcast traffic priority (for Quality of Service). Default: 0

Section 5.1.12
Transparent VLAN

Use the **Transparent VLAN** pane for Transparent VLAN configuration. When Transparent VLAN status is enabled, the base station treats TVLANs as untagged, allowing an unlimited number of VLANs. TVLANs are transparent to both the base station and the CPE.

Procedure: Setting the Transparent VLAN parameters

1. Click **Subscribers**. The **Subscribers** links appear in the options pane.
2. In the options pane, click the **Services** link and then click the **Transparent VLAN** link. The **Transparent VLAN** pane appears.

Figure 71: Transparent VLAN pane

3. Review and set the parameters in the following fields:

Parameter	Description
TVLAN Status	**Synopsis:** { Enable, Disable } To set the TVLAN Status, select a value from this list.

4. Click **Apply**.

Section 5.2
GPS Settings

The base station is configured to use GPS by default. This section describes how to view GPS settings and information, and how to disable and enable the GPS received for testing and troubleshooting.

NOTE
To enable or disable the GPS receiver, you must reboot the system. To reset the GPS-to-base station link state, you must restart the base station service.

Procedure: Setting the GPS parameters

1. Navigate to ***Admin*** » ***Synchronization*** » ***GPS***. The **GPS Info and Settings** screen appears.

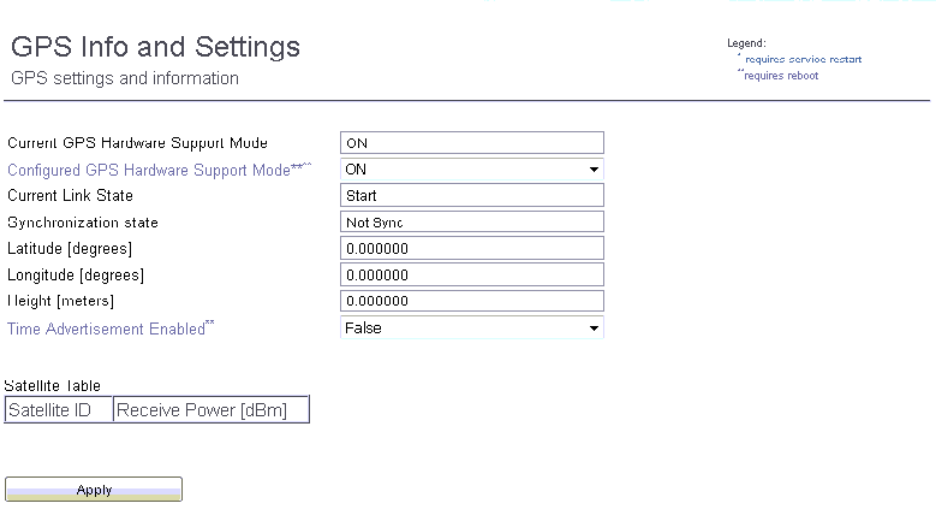


Figure 72: GPS Info and Settings pane

2. Review and set the GPS settings in the following fields:

Parameter	Description
Current GPS Hardware Support Mode	**Synopsis:** { OFF, ON } **Default:** ON Displays the current state of the GPS subsystem.
Configured GPS Hardware Support Mode	**Synopsis:** { OFF, ON } **Default:** ON Enables or disables the GPS receiver. Options include: • `ON` – Normal operation. The base station maintains synchronization with the GPS. • `OFF` – For testing and other special cases. The base station does not attempt to synchronize with the GPS. Use this option for testing, for installations with a single base station, or for other instances where GPS is not used. **IMPORTANT!** *The base station must be rebooted after changing this value.*

Parameter	Description
Current Link State	**Synopsis:** { Stop, Start, Auto } **Default:** Auto Displays the state of the GPS-to-base station data link. Set to `Start` if **Configured GPS Hardware Support Mode** is set to `OFF`. Set to `Auto` if **Configured GPS Hardware Support Mode** is set to `ON`.
Synchronization State	**Synopsis:** { Not Sync, Sync OK } **Default:** Not Sync Displays the synchronization state of the GPS subsystem.
Latitude [degrees]	Displays the terrestrial latitude, in degrees, as received from the GPS receiver.
Longitude [degrees]	Displays the terrestrial longitude, in degrees, as received from the GPS receiver.
Height [meters]	Displays the height above sea level, in meters, as received from the GPS receiver.
Time Advertisement Enabled	**Synopsis:** { True, False } Advertises the GPS time to the CPE. Enables the NTP feature in the CPE to work correctly.

3. The Satellite Table displays the following information for each GPS satellite seen by the GPS receiver:

Table: Satellite Table

Column	Description
SatelliteID	Displays the GPS satellite identifier.
ReceivePower	Displays the received signal strength, in dBm.

4. Click **Apply**.
5. If you changed the value in the **Configured GPS Hardware Support Mode** field, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.
6. If you changed the value in the **Configured Link State** field, restart the base station service:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Stop Service**, and then click **Start Service**.

Section 5.3
Synchronization Settings

The base station can be configured to report time and date from either a GPS or IEEE 1588 receiver. The user may also choose to have no synchronization setting.

NOTE
Selecting IEEE1588 or NONE from the Configured Time Synchronization Mode will override the settings for GPS Info and Settings.

NOTE
Base station synchronization can take up to 1 minute, depending on the accuracy of the Master Clock source.

1. Navigate to ***Admin*** » ***Synchronization*** » ***Synchronization Settings***. The **Synchronization Settings** screen appears.

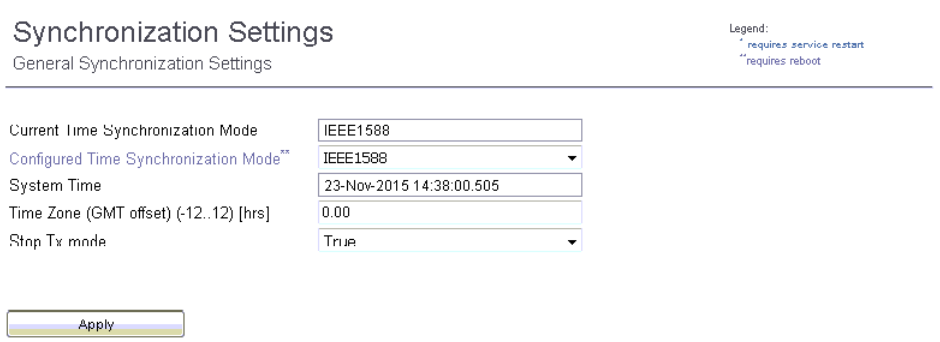


Figure 73: Synchronization Settings

2. Review and set the synchronization settings in the following fields:

Parameter	Description
Current Time Synchronization Mode	**Synopsis:** { GPS, IEEE1588, NONE } Displays the current time synchronization mode.
Configured Time Synchronization Mode	**Synopsis:** { GPS, IEEE1588, NONE } Configured time synchronization mode of the base station.
System Time	Reported time from the GPS receiver or the IEEE1588 receiver.
Time Zone (GMT offset) (-12..12) [hrs]	Time Zone - GMT offset. Range (-12 to +12)
Stop Tx Mode	**Synopsis:** { True, False } Determine if the BS will continue transmitting after hold over stop TX timeout.

3. Click **Apply**.

NOTE
The base station will need to be rebooted for the changes to take effect.

4. Click **Quick Start**. The **Quick Start Settings** pane appears.
5. Click **Reboot**.

Section 5.4
IEEE1588 Settings

To view IEEE1588 settings and information, do the following:

1. Navigate to ***Admin » Synchronization » IEEE1588***. The **IEEE1588** screen appears.

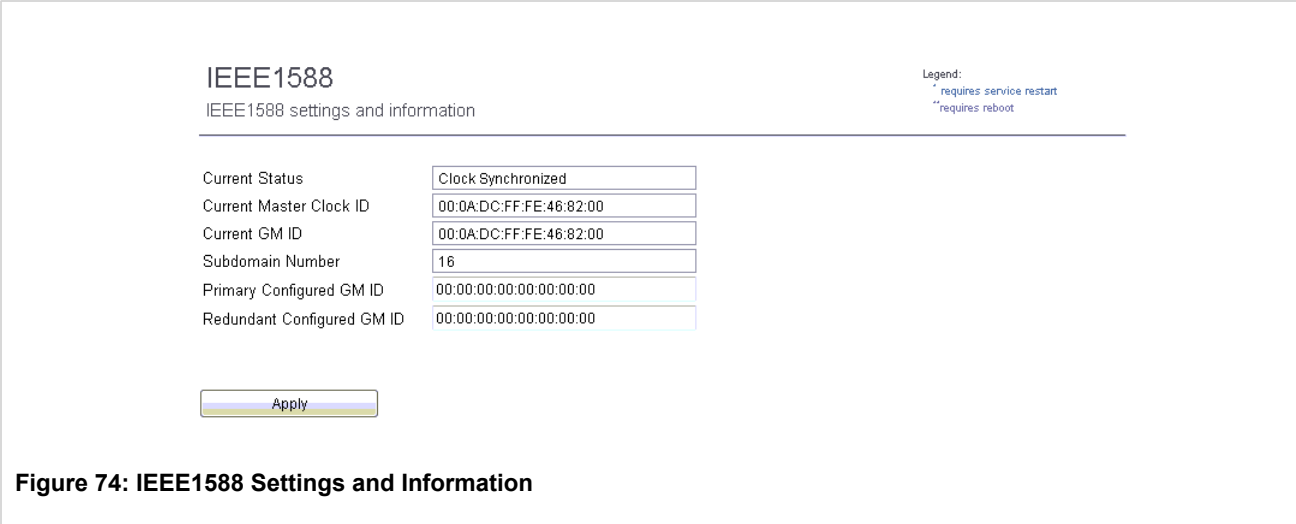


Figure 74: IEEE1588 Settings and Information

2. The following information is displayed:

Parameter	Description
Current Status	IEEE1588 slave current state.
Current Master Clock ID	IEEE1588 clock source ID BS is currently listening to.
Current GM ID	IEEE1588 Grandmaster clock source ID BS is currently listening to.
Subdomain Number	IEEE1588 subdomain BS is currently listening to.
Primary Configured GM ID	If configured to a value other than all zeroes, the BS will not synchronize on the IEEE1588 clock source unless the GM ID published is equal to the configured value.
Redundant Configured GM ID	If configured to a value other than all zeroes, the BS will not synchronize on the IEEE1588 clock source unless the GM ID published is equal to the configured value.

Section 5.5

SNMP Administration

In SNMP administration, you enable and disable SNMPv2 and SNMPv3, configure trap destinations, SNMP communities, and MIB2 system identification parameters.

For instructions on enabling and disabling SNMPv2 and SNMPv3, and on setting SNMP trap destinations, refer to Section 5.5.1, “SNMP General Settings”.

For instructions on configuring SNMPv2, refer to Section 5.5.1.1, “SNMPv2 Configuration”.

For instructions on configuring SNMPv3, refer to Section 5.5.1.2, “SNMPv3 Configuration”.

For instructions on setting the MIB2 system identification information, refer to Section 5.5.2, “SNMP MIB2 System Identification”.

Section 5.5.1
SNMP General Settings

On the **SNMP General Settings** pane, you can enable or disable SNMPv2 and SNMPv3, set the SNMP trap destinations, and access the SNMPv2 and SNMPv3 configuration settings. You can specify up to five trap destination addresses.

Procedure: Setting the SNMP general settings

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options pane, click the **SNMP** link, and then click the **SNMP General Settings** link. The **SNMP General Settings** pane appears.

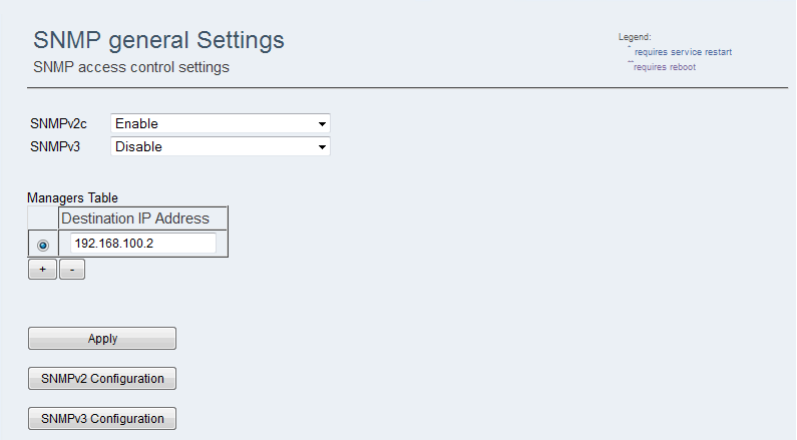


Figure 75: SNMP General Settings

3. In the **SNMPv2c** and **SNMPv3** fields, enable or disable SNMPv2c and SNMPv3.
4. In the **Managers Table**, add up to five trap destination addresses:
   a. Click the + button. A new row appears in the **Managers Table**.
   b. Type an IP address in the new row.
5. To remove an SNMP trap destination, select a row and click the - button. If no rows are selected, clicking the - button removes the last entry in the table.
6. Click **Apply**.
7. To configure SNMPv2 parameters, click **SNMPv2 Configuration**. For more information, refer toSection 5.5.1.1, “SNMPv2 Configuration”.
8. To configure SNMPv3 parameters, click **SMPv3 Configuration**. For more information, refer toSection 5.5.1.2, “SNMPv3 Configuration”.

Section 5.5.1.1
SNMPv2 Configuration

The **SNMPv2c Configuration** pane appears when you click **SNMPv2 Configuration** on the **SNMP General Settings** pane. On this pane, you set the SNMPv2c read, write, and trap community settings.

Procedure: Setting the SNMPv2c parameters

1. On the **SNMP General Settings** pane, click **SNMPv2 Configuration**. The **SNMPv2c Configuration** pane appears.

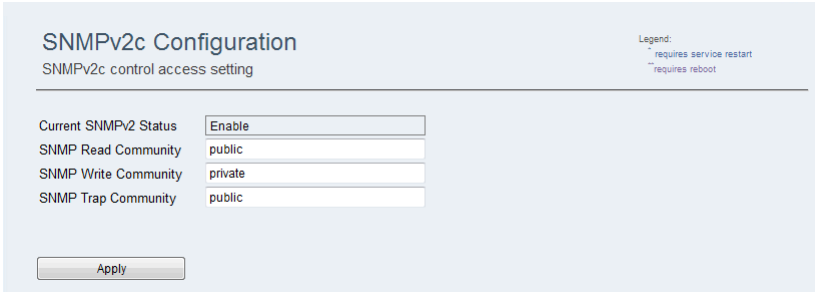


Figure 76: SNMPv2c Configuration pane

2. The **Current SNMPv2 Status** field displays the current status for the SNMPv2 system: Enabled or Disabled.
3. Review and set the SNMPv2c settings in the following fields:

Parameter	Description
SNMP Read Community	**Default:** public The SNMP community name for read access. This name can be used as a password for secure information retrieval. Type a name in the field. The SNMP Read Community name must be different from the SNMP Write Community name.
SNMP Write Community	**Default:** private The SNMP community name for write access. This name can be used as a password for secure set commands. Type a name in the field. The SNMP Write Community name must be different from the SNMP Read Community name.
SNMP Trap Community	**Default:** public The SNMP community name to use when the SNMP service receives a request that does not contain the correct community name and does not match an accepted host name.

4. Click **Apply**.

Section 5.5.1.2
SNMPv3 Configuration

The **SNMPv3 Configuration** pane appears when you click **SMPv3 Configuration** on the **SNMP General Settings** pane. On this pane, you configure SNMPv3 users, authentication parameters, and access groups.

Procedure: Setting the SNMPv3 parameters

1. On the **SNMP General Settings** pane, click **SNMPv3 Configuration**. The **SNMPv3 Configuration** pane appears.

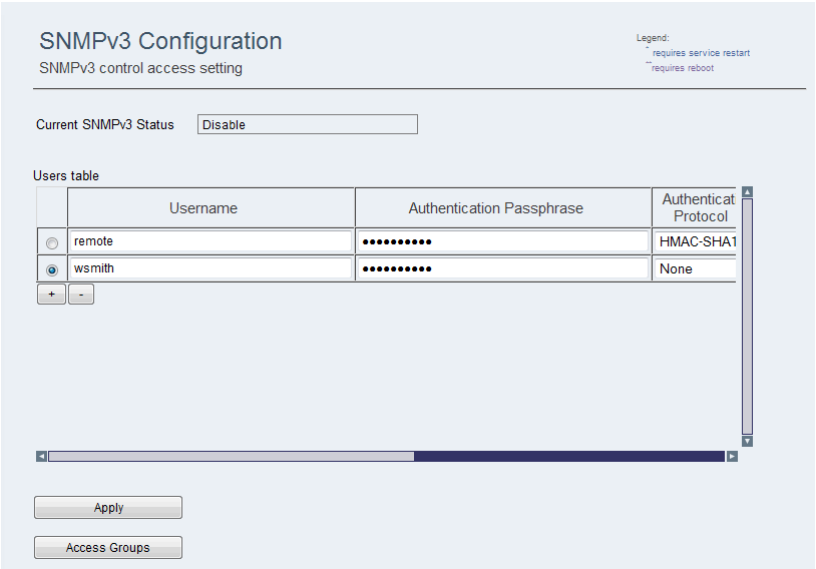


Figure 77: SNMPv3 Configuration pane

2. The **Current SNMPv3 Status** field displays the current status for the SNMPv3 system: Enabled or Disabled.
3. Review and set the SNMPv3 users in the **Users table**.

   To add an SNMPv3 user, click the + button. A new row appears in the **Users Table**. Enter the following parameters:

Parameter	Description
Username	The user name.
Authentication Passphrase	The passphrase used for authentication.
Authentication Protocol	**Synopsis:** HMAC-SHA1 Select the authentication protocol for the user.
Privacy Passphrase	The passphrase used for privacy.
Privacy Protocol	**Synopsis:** CBC-DES Select the privacy protocol.
Access Group	Associated the user with an SNMPv3 Access Group.

4. To remove an SNMPv3 user, select a row in the **Users Table** and click the - button. If no rows are selected, clicking the - button removes the last entry in the table.
5. Click **Apply**.
6. To view the SNMPv3 access groups, click **Access Groups**. For more information, refer toSection 5.5.1.3, “Viewing SNMPv3 Access Groups”.

Section 5.5.1.3
Viewing SNMPv3 Access Groups

The **SNMPv3 Access Groups Configuration** pane appears when you click **Access Groups** on the **SNMPv3 Configuration** pane. On this pane, you can review the default SNMP v3 access groups.

Procedure: Viewing the SNMPv3 Access Groups

1. On the **SNMPv3 Configuration** pane, click **Access Groups**. The **SNMPv3 Access Groups Configuration** pane appears.

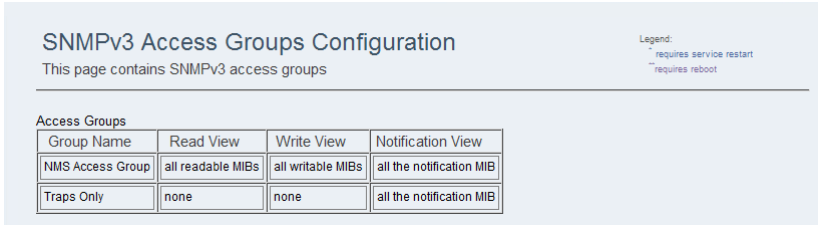


Figure 78: SNMPv3 Access Groups Configuration

2. Review the SNMPv3 access groups in the **Access Groups** table:

Parameter	Description
Group Name	The access group name.
Read View	The read view for the access group.
Write View	The write view for the access group.
Notification View	The notification view for the access group.

Section 5.5.2
SNMP MIB2 System Identification

The SNMP MIB2 settings provide base station system identification information.

On the **SNMP - MIB2 Settings** pane, you set the base station contact details, name, and street address. This pane also displays the read-only SNMP system description, object identifier, system up time, and system services values.

Procedure: Setting SNMP MIB2 system identification information

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **SNMP** link, and then click the **MIB2 System** link. The **SNMP - MIB2 Settings** pane appears.

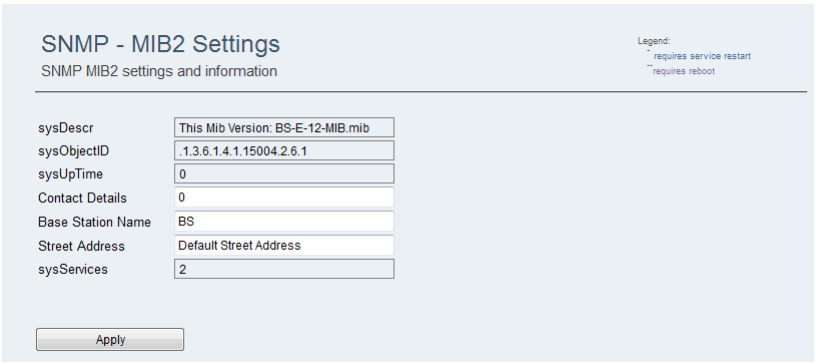


Figure 79: SNMP MIB2 Settings pane

3. Review and set the SNMP system identification information in the following fields:

Parameter	Description
sysDescr	**Default:** This MIB version: BS-E-12-MIB.mib Displays the SNMP MIB version.
sysObjectID	**Default:** .1.3.6.1.4.1.15004.2.6.2 Displays the Siemens private enterprise number and object identifier for the base station SNMP subsystem.
sysUpTime	Displays the length of time, in hundredths of a second, since the SNMP subsystem was last initialized.
Contact Details	Contains base station contact information. Type a name and contact details, such as an e-mail address, in this field.
Base Station Name	Contains the base station name. Type a descriptive name in this field.
Street Address	Contains the base station street address or location. Type and address or location in this field.
sysServices	Displays a value indicating the set of services provided by the system. The value 2 indicates the datalink/subnetwork layer.

4. Click **Apply**.

Section 5.6

Redundancy

Base station redundancy helps ensure service continuity in the event of a base station failure. Two base stations are required for redundancy. On each base station, redundancy must be enabled and must be configured with the other's IP address.

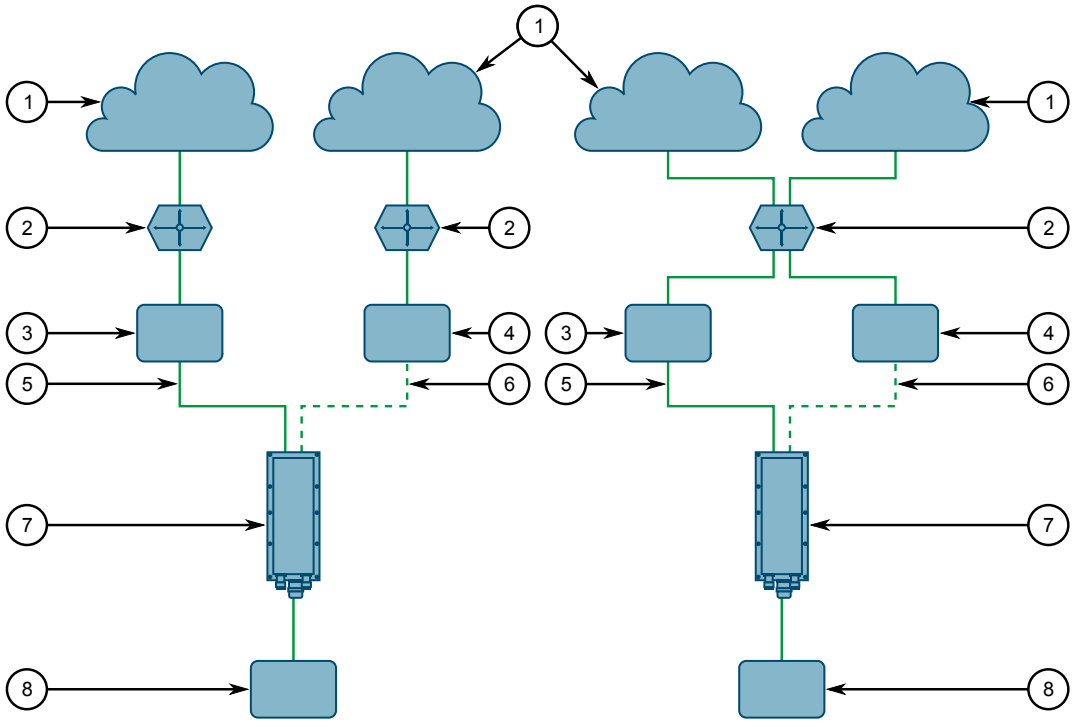


Figure 80: Typical Redundancy Topologies

1. Network **2.** L2 Switch/Router **3.** Base Station Master **4.** Base Station Slave **5.** Activity Link (Frequency = F1) **6.** Backup Link (Frequency = F1) **7.** CPE **8.** Field Device

On the **Redundancy Settings** pane, you enable and disable the redundancy function, and set the IP address for for the other base station in the redundant pair. This pane also displays the current status of the two base stations, and whether the current base station can reach the AAA server and ASN-GW.

NOTE
Base station redundancy is disabled by default.

To enable or disable base station redundancy, you must reboot the base station.

Procedure: Setting base station redundancy

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Redundancy** link. The **Redundancy Settings** pane appears.

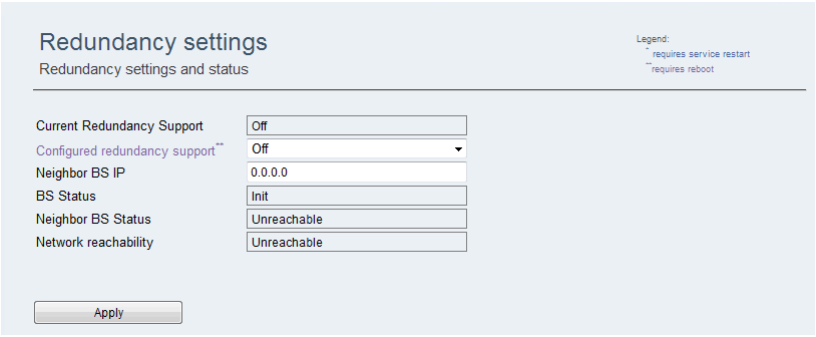


Figure 81: Redundancy Settings pane

3. Review and set the redundancy parameters in the following fields:

Parameter	Description
Current Redundancy Support	**Synopsis:** { Off, On } **Default:** Off Displays the current state of the redundancy function.
Configured Redundancy Support	**Synopsis:** { Off, On } **Default:** Off Enables and disables base station redundancy. Select Off or On.
Neighbor BS IP	The IP address of the neighboring base station used for redundancy. Type an IPv4 address in this field.
BS Status	**Synopsis:** { Init, ElectionBackoff, ElectionQuerySent, MasterOk, MasterNotOk, SlaveReady, SlaveNotReady } **Default:** MasterOK Displays the status of the current base station.
Neighbor BS Status	**Synopsis:** { MasterOk, MasterNotOk, SlaveReady, SlaveNotReady, SlaveGoingToMaster, Unreachable } **Default:** MasterOK Displays the status of the redundant base station.
Network Reachability	**Synopsis:** { Reachable, Unreachable } **Default:** Unreachable Indicates if the base station can reach the AAA and ASN-GW over the network.

4. Click **Apply**.
5. If you changed the value in the **Configured Redundancy Support** field, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 5.7

Spectrum Analyzer Tool

NOTE
Activating the Spectrum Analyzer resets the Base Station, interrupting service until you reboot the base station to exit from spectrum mode.

Use the Spectrum Analyzer tool for preliminary review of the base station spectrum. The Spectrum Analyzer is useful if you suspect that base station operation is affected by interference, such as from other base stations operating in the same bandwidth.

The tool provides only a preliminary indication of the presence of interference. If interference is detected, it is recommended to perform detailed, in-depth analysis using a spectrum analyzer and other relevant analysis tools.

The Spectrum Analyzer tool provides the following analysis capabilities:

- Viewing the spectrum of all frequencies in which the base station is designed to operate
- Setting the Spectrum Analyzer to operate and accumulate data within a specified span
- Viewing a frozen or held signal for comparison with continuing incoming signals
- Other basic measurement tools and functions

Procedure: Activating the Spectrum Analyzer

1. Click **Admin**. The **Current Status** pane appears.
2. Click the **Spectrum Analyzer** link. A prompt appears to confirm that you want to reboot the base station. Click **OK**. The base station reboots.
3. After the base station reboots, log in to the web management interface again and refresh the web page. The **Spectrum Configuration** page appears.

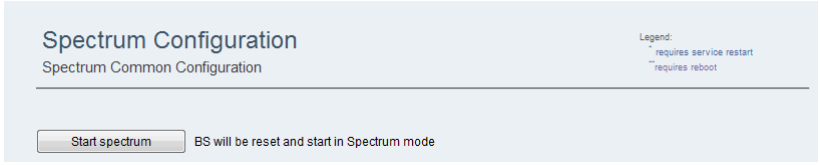


Figure 82: Spectrum Configuration pane

4. Click **Start Spectrum**. The base station reboots and enters the Spectrum Mode. The **Spectrum Configuration** pane appears and displays the spectrum analyzer configuration parameters.

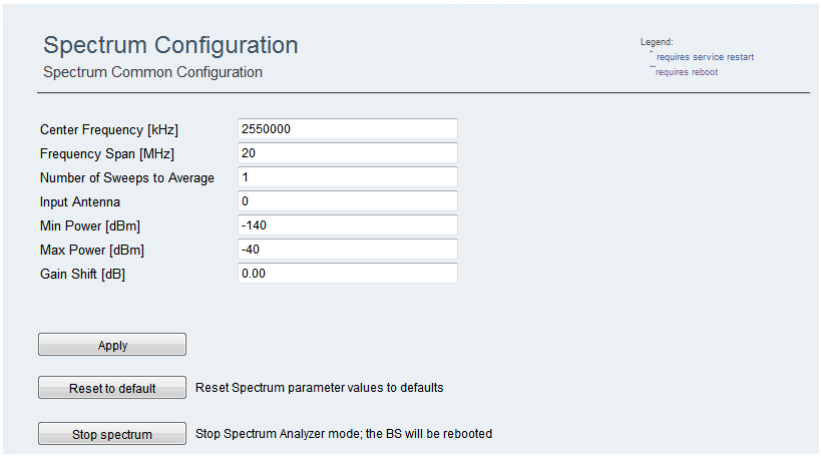


Figure 83: Spectrum Configuration pane in Spectrum Mode

5. Review and set the spectrum analyzer parameters in the following fields:

Parameter	Description
Central Frequency [kHz]	Center of the displayed range of frequencies.
Frequency Span [MHz]	The width of the displayed range of frequencies.
Number of Sweeps to Average	The depth in time of the averaging used in the spectrum calculation.
Input Antenna	The antenna on whose received signals the spectrum calculation is based.
Min Power [dBm]	Lower power limit of the displayed spectrum.
Max Power [dBm]	Upper power limit of the displayed spectrum.
Gain Shift [dB]	Rx Gain correction used to avoid compression of the input signals.

6. After making changes to the parameters, click **Apply**.
7. To restore the default values, click **Reset to default**.
8. To exit spectrum mode and return the base station to normal operation, click **Stop spectrum**. The base station reboots.
9. To activate the spectrum plot, click the **Spectrum Plot** link in the options pane. The **Spectrum Plot** pane appears. For more information, refer to Section 5.7.1, “Using the Spectrum Plot”.

Section 5.7.1
Using the Spectrum Plot

The **Spectrum Plot** pane appears when you click the **Spectrum Plot** link in the options pane. The pane displays the spectrum analysis plot and its controls.

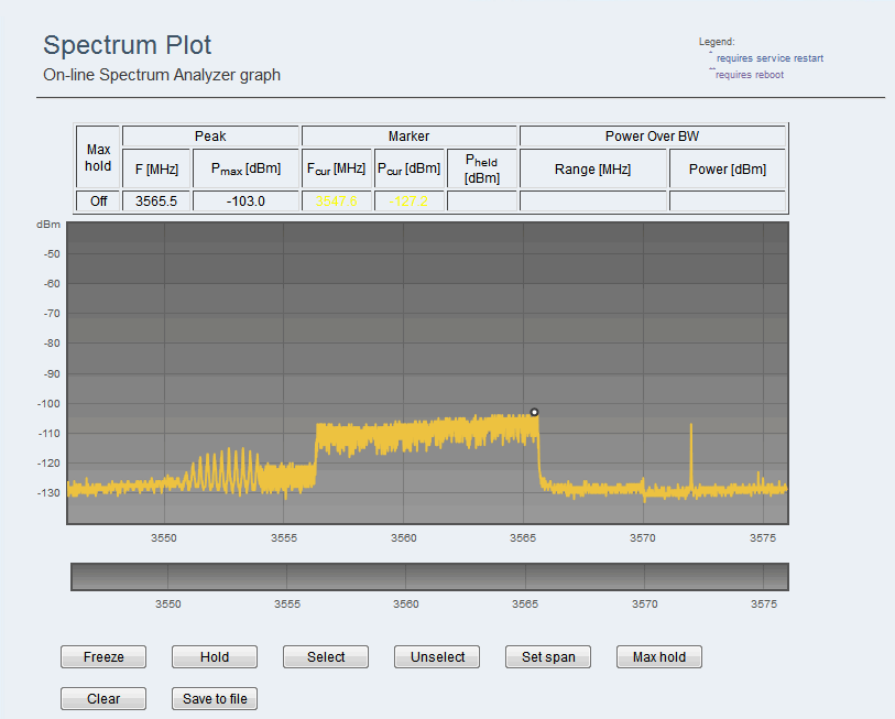


Figure 84: Spectrum Plot pane

The following status information appears above the spectrum graph:

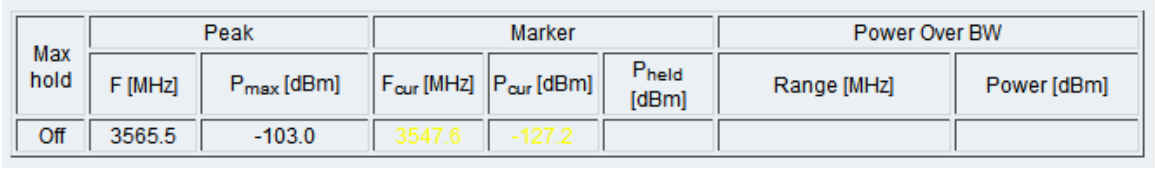


Figure 85: Spectrum Plot Status Information

Table: Spectrum Plot Status Information

Parameter	Description
Max Hold	Status of Max Hold function: ON | OFF
Peak	Frequency and power of maximum signal level within spectrum.
Marker	Frequency and power at the marker location. To activate the marker, click **Freeze** or **Hold** and then left-click on the graph. If you clicked **Hold**, the power of the held signal at the marker point is also displayed.
Power Over BW	Overall power over the range selected using **Freeze** and **Select**.

Buttons below the plot provide the following functions:

Table: Spectrum Plot Functions

Function	Description
Freeze	Freezes the current signal.
Hold	Freezes the signal and displays it in blue and continues to display real-time signals in yellow. Use this to compare signal changes over time.
Select	Zooms in on the selected Freeze mode signal. To select a signal, click and drag on the graph.
Unselect	Clears the selection made with **Select**.
Set Span	Sets the span of the spectrum analyzer to the frequency band of the selected part of the Freeze mode signal.
Max Hold	Displays only the highest point detected for each frequency range during the test. This is analogous to the Max Hold function on a standard spectrum analyzer.
Clear	Clears the display.
Move to File	Saves plotted data to a comma-separated value file.
Left click on the graph	Places a vertical marker on the graph. The frequency and power information for the selected point appears in the **Marker** columns in the status information above the graph.

Section 5.7.1.1
Max Hold

To display the highest point detected for each frequency range during the test, click **Max Hold**. The Max Hold status, ON or OFF, appears in the **Max hold** column in the status information above the graph.

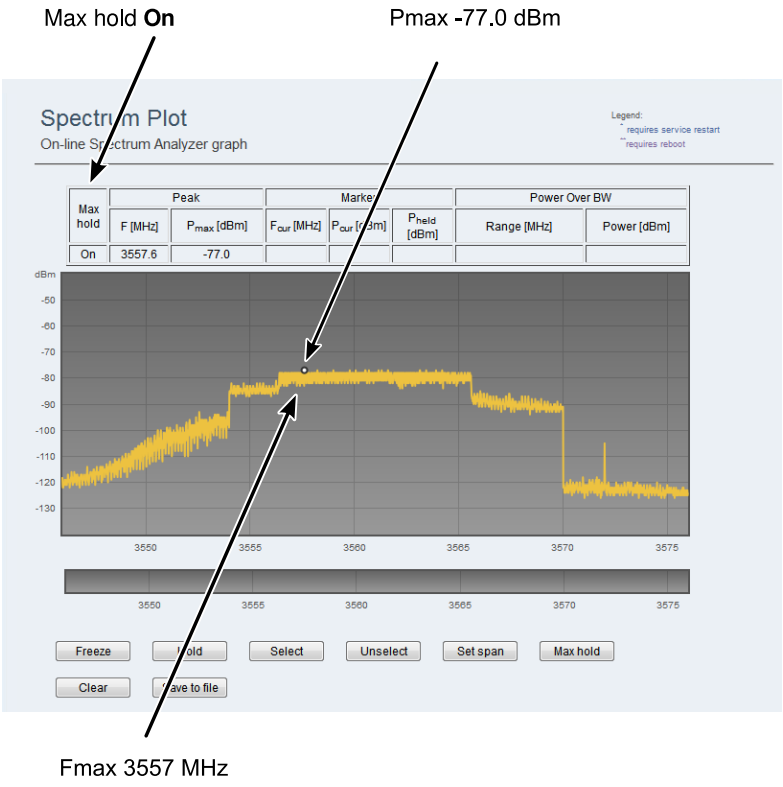


Figure 86: Spectrum Max Hold Example

Section 5.7.1.2

Marker Information

To place a marker, left-click on the graph. Use the marker to analyze a specific area in the display. Frequency and power information for the marker location appears in the **Marker** columns in the status information above the graph.

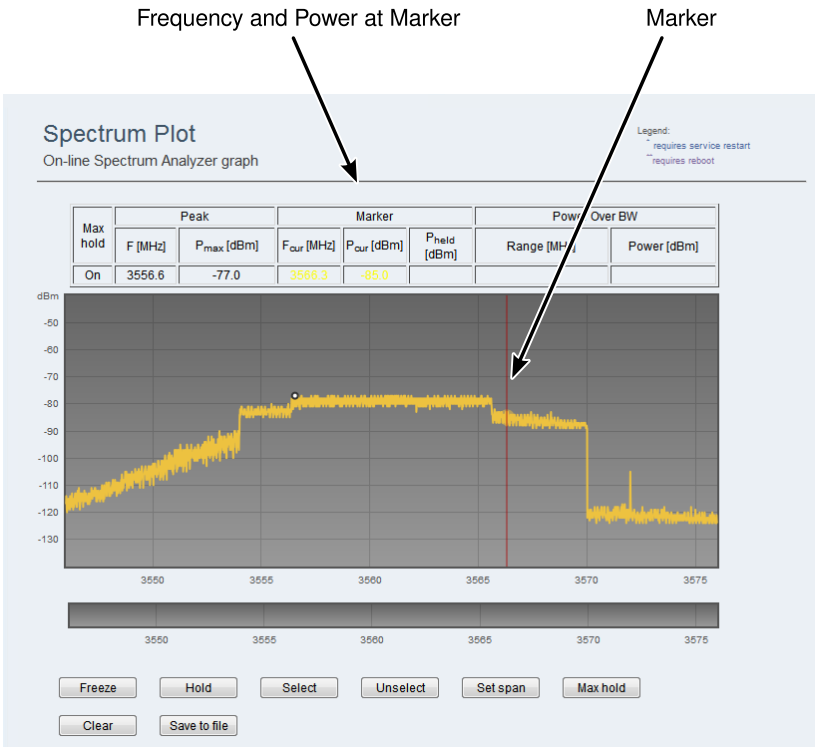


Figure 87: Spectrum Marker Example

Section 5.7.1.3

Zooming In

To zoom-in, click-and-drag on the spectrum plot to highlight a specific area and click **Select**. You can repeat the zoom operation by clicking **Select** a second time. To zoom out, click **Unselect**.

The power over the selected band and the frequency range of the zoomed area appear in the **Power Over BW** columns in the status information above the graph.

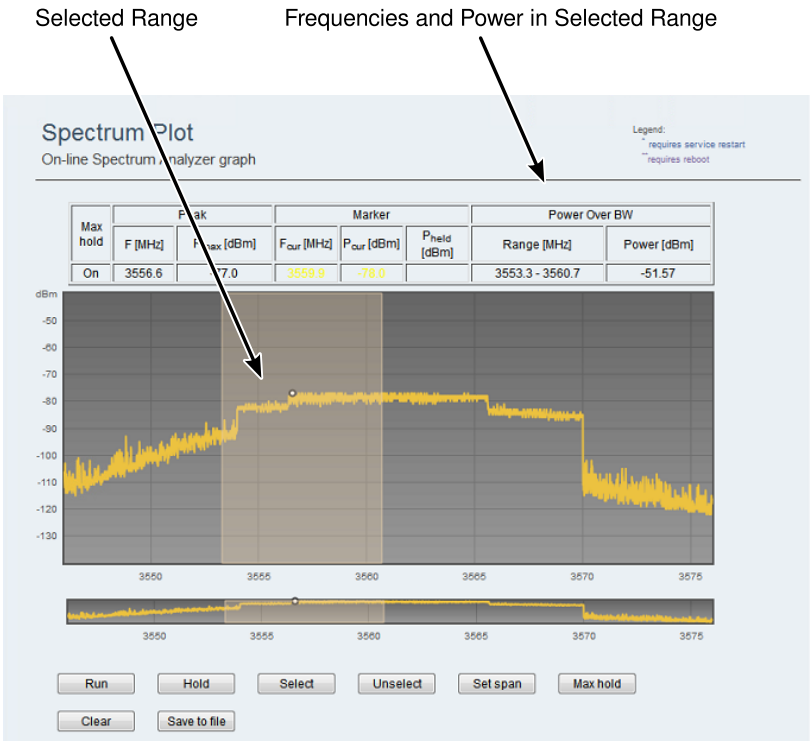


Figure 88: Spectrum Zoom Example

Section 5.7.1.4

Set Span

To set the base station to acquire signals in a selected span only, click and drag on the graph and click **Set Span**. A prompt appears to confirm that you want to set the scan region to the selected values; click **Yes**. The base station now acquires signals only within the selected bandwidth.

The power over the selected band and the frequency range of the selected range appear in the **Power Over BW** columns in the status information above the graph.

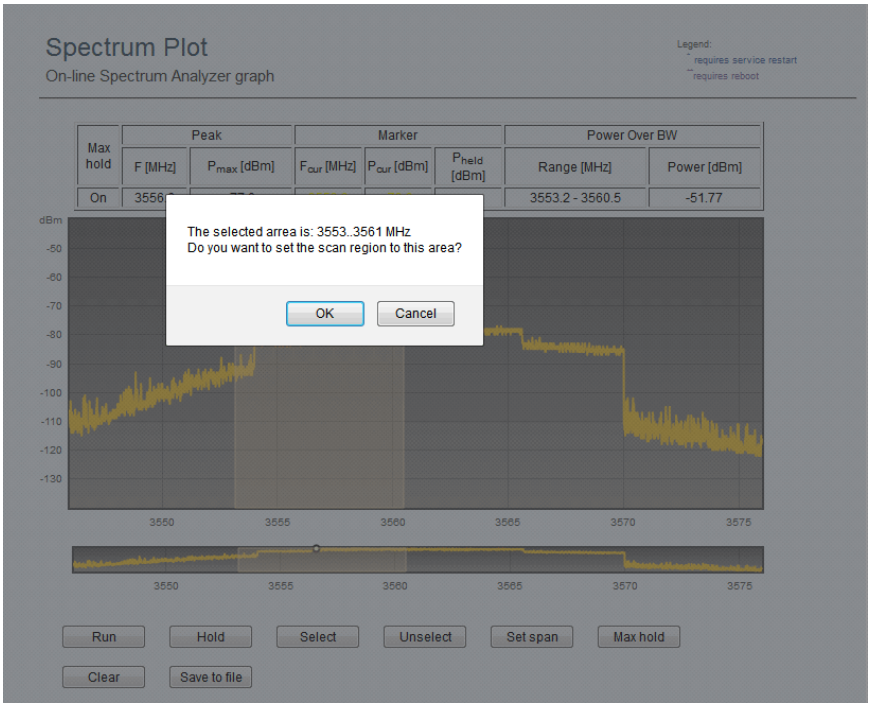


Figure 89: Spectrum Set Span Example

Section 5.7.1.5

Hold

To hold a signal, click **Hold**. The help signal appears in blue, and the continuous real time signal appears in yellow. The marker information of the help and the continuously acquired signals is appears in the **Marker** columns in the status information above the graph.

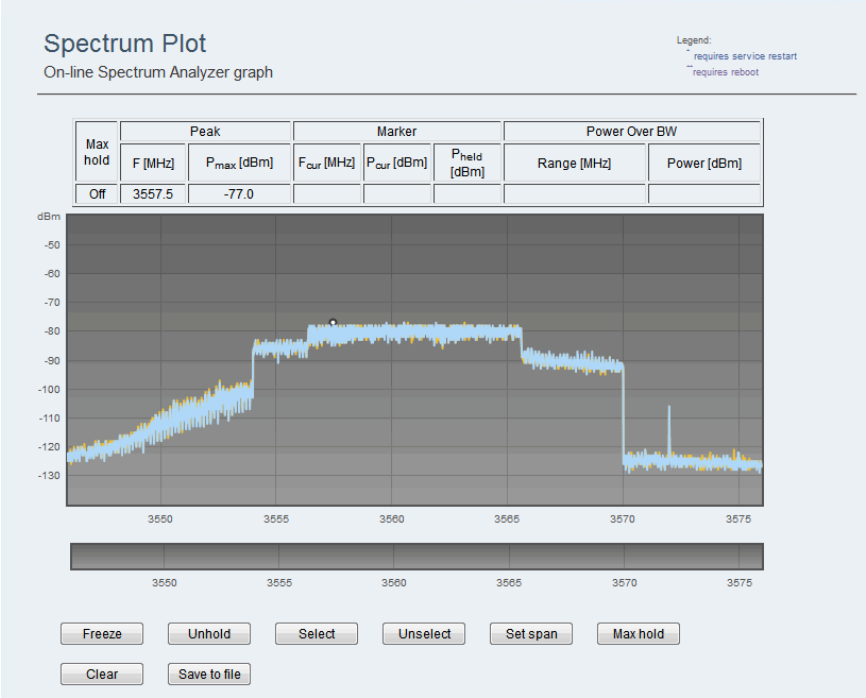


Figure 90: Spectrum Hold Example

Section 5.8

Management VLAN Configuration

On the **Management VLAN Configuration** pane, you configure the management VLAN options. The options include the VLAN number and the 802.1p priority value. Outgoing management frames are tagged with the configured VLAN number and priority. Incoming management frames must be tagged with the same values, or the base station drops the incoming frames.

NOTE
Prior to assigning the Management VLAN ID for the Base Station, make sure all other management traffic (AAA, DHCP, SNMP etc.) will be part of the same VLAN in your switch or router.

Procedure: Setting Management VLAN Configuration Options

1. Click **Admin**. The **Admin** options appear in the options pane.
2. In the options panel, click the **Management VLAN** link. The **Management VLAN Configuration** pane appears.

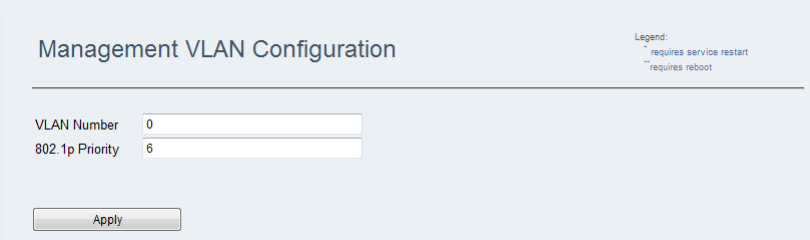


Figure 91: Management VLAN Configuration pane

3. Review and set the management VLAN parameters in the following fields:

Parameter	Description
VLAN Number	**Synopsis:** Any numeric value **Default:** 0 Displays an identifier for the management VLAN.
802.1p Priority	**Synopsis:** A number in the range of 0 to 7 **Default:** 6 Sets the 802.1p priority value for the management VLAN. Type a value from 0 to 7.

4. Click **Apply**.

Section 5.9
Managing Wireless Settings

The following sections describe how to manage wireless settings:

- Section 5.9.1, “Network Identifiers”
- Section 5.9.2, “Radio and Frame Parameters”
- Section 5.9.3, “Wireless Security Authentication Settings”
- Section 5.9.4, “MAC”

Section 5.9.1
Network Identifiers

On the **Network Identifiers** pane, set the base station name, unique identifier, and network access provider identifier.

Procedure: Setting the Network Identifiers

1. Click **Wireless**. The **Network Identifiers** pane appears.

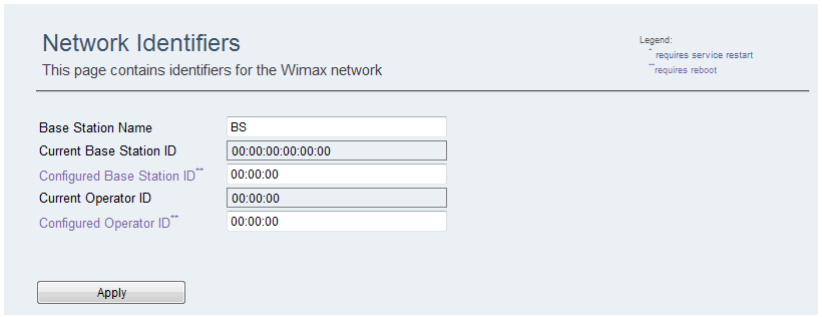


Figure 92: Network Identifiers pane

2. Review and set the network identifiers n the following fields:

Parameter	Description
Base Station Name	Displays the base station name. To change the name, type a name in this field.
Current Base Station ID	Displays the base station identifier.
Configured Base Station ID	To change the base station identifier, type the identifier in this field.
Current Operator ID	Displays the current Network Access Provider identifier.
Configured Operator ID	To change the Network Access Provider identifier, type the identifier in this field. Network Access Provider identifiers are unique to each operator and are managed by the IEEE Standards Association. For more information, refer to https://standards.ieee.org/develop/regauth/bopid/.

3. Click **Apply**.
4. If you changed the value in the **Configured Base Station ID** or **Configured Operator ID** fields, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 5.9.2
Radio and Frame Parameters

Radio and frame parameters are viewed and configured on the following panes:

- **Radio Capabilities** pane: displays the radio capabilities. For more information, refer toSection 5.9.2.1, “Radio Capabilities”.
- **Radio Settings** pane: configures the radio settings and displays the RF Channels table. For more information, refer toSection 5.9.2.2, “Radio Settings”.
- **Frame Settings** pane: configures the radio frame parameters. For more information, refer toSection 5.9.2.3, “Frame Settings”.

- **Link Adaptation** pane: configures the link adaptation parameters. For more information, refer toSection 5.9.2.4, “Link Adaptation”.
- **DL Modulation** pane: configures downlink modulation parameters. For more information, refer toSection 5.9.2.5, “DL Coding and Modulation”.
- **UL Modulation** pane: configures uplink modulation parameters. For more information, refer toSection 5.9.2.6, “UL Coding and Modulation”.
- **Interference Detection Settings** pane: configures the interference detection threshold. For more information, refer toSection 5.9.2.7, “Interference Detection”.

Radio parameters must be set within the valid range of values determined by local regulations, and in accordance with device capabilities.

Section 5.9.2.1
Radio Capabilities

The **Radio Capabilities** pane displays the device hardware radio configuration and capabilities.

The **Radio Capabilities** pane is read-only; there are no parameters to set on this pane.

Procedure: Viewing the Radio Capabilities

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link. The **Radio Capabilities** pane appears.

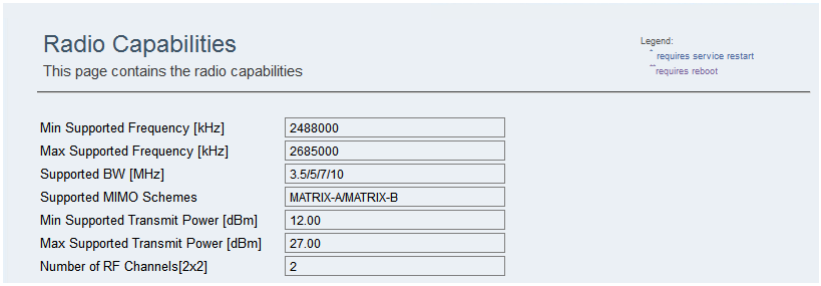


Figure 93: Radio Capabilities pane

3. Review the radio capabilities information in the following fields:

Parameter	Description
Min Supported Frequency [kHz]	Displays the minimum supported transmission frequency, in kilohertz.
Max Supported Frequency [kHz]	Displays the maximum supported transmission frequency, in kilohertz.
Supported BW [MHz]	Displays the supported bandwidths, in megahertz. Values are separated by/forward slashes. For example: **3.5/5/7/10** indicates supported bandwidths of 3.5 MHz, 5 MHz, 7 MHz, and 10 MHz.
Supported MIMO Schemes	Displays the supported multiple-input multiple output schemes. Values are separated by/forward slashes.

Parameter	Description
	For example, **MATRIX-A/MATRIX-B** indicates support for MIMO Matrix A and MIMO Matrix B.
Min Supported Transmit Power [dBm]	Displays the minimum supported transmission power, in dBm. Value for “Pico” base stations: 12 – *for 2.3GHz, 2.5GHz,3.3GHz, 3.5GHz, 3.65GHz*; 9 - *for 4.9GHz, 5.8GHz* Value for “Compact” base stations: 21
Max Supported Transmit Power [dBm]	Displays the maximum supported transmission power, in dBm. Value for “Pico” base stations: 27 – *for 2.3GHz, 2.5GHz, 3.3GHz,3.5GHz, 3.65GHz*; *24 - for 4.9GHz, 21 – for 5.8GHz* Value for “Compact” base stations: 36
Number of RF Channels[2x2]	Displays the number of RF transmission channels channels.

Section 5.9.2.2
Radio Settings

On the **Radio Settings** pane, review and set the radio parameters.

Procedure: Setting the Radio Parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link and then click the **Radio Settings** link. The **Radio Settings** pane appears.

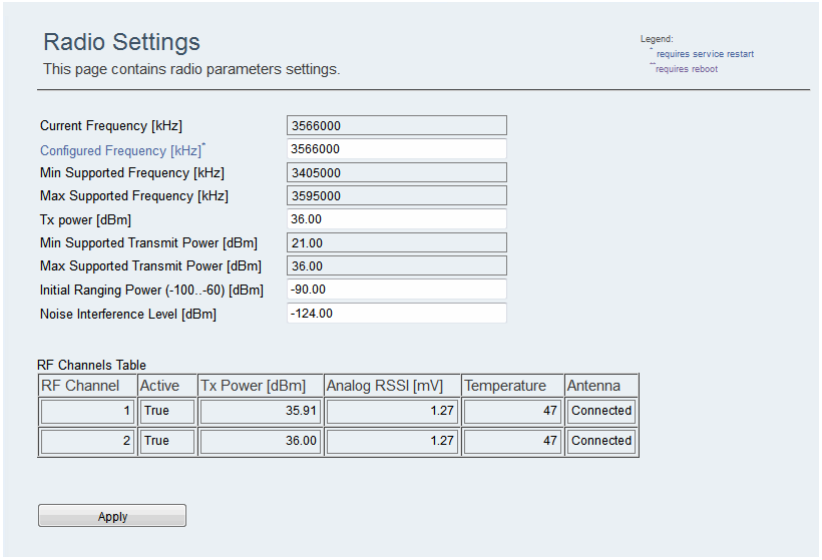


Figure 94: Radio Settings pane

3. Review and set the radio parameters in the following fields:

Parameter	Description
Current Frequency [kHz]	Displays the current base station radio frequency, in kilohertz.

Parameter	Description
Configured Frequency [kHz]	To set the base station radio frequency, type a value in this field. The value is applied after the next base station reboot or configuration flashing. The value must be between the values shown in the **Min Supported Frequency [kHz]** and **Max Supported Frequency [kHz]** fields.
Min Supported Frequency [kHz]	Displays the minimum supported transmission frequency, in kilohertz.
Max Supported Frequency [kHz]	Displays the maximum supported transmission frequency, in kilohertz.
Tx power [dBm]	To set the base station transmission power settings, type a value in this field. The value must be within the valid range determined by local regulations and in accordance with device capabilities. The value must be within the values shown in the **Min Supported Transmit Power [dBm]** and **Max Supported Transmit Power [dBm]** fields.
Min Supported Transmit Power [dBm]	Displays the minimum supported transmission power, in dBm. Value for “Pico” base stations: 12 – *for 2.3GHz, 2.5GHz,3.3GHz, 3.5GHz, 3.65GHz*; 9 - *for 4.9GHz, 5.8GHz* Value for “Compact” base stations: 21
Max Supported Transmit Power [dBm]	Displays the maximum supported transmission power, in dBm. Value for “Pico” base stations: 27 – *for 2.3GHz, 2.5GHz, 3.3GHz,3.5GHz, 3.65GHz*; 24 - *for 4.9GHz*, 21 – *for 5.8GHz* Value for “Compact” base stations: 36
Initial Ranging Power (-100..-60) [dBm]	Displays the Maximum Initial Ranging Power, in dBm. This feature minimizes possible interference by limiting the signal levels of third party equipment. If received signal power exceeds this value, the signal is not accepted. To set the Initial Ranging Power level, type a value in the range of -100 to -60.
Noise Interference Level (dBm)	Displays the noise interference level, in dBm.

4. The **RF Channels Table** displays the following information for each RF channel:

Parameter	Description
RF Channel	**Synopsis:** { 1, 2 } Displays the RF unit or name.
Active	**Synopsis:** { True, False } When true, displays the status of the RF Channel.
Tx Power [dBm]	Displays the RF unit transmission power, in dBm. Value will be within the values shown in the **Min Supported Transmit Power [dBm]** and **Max Supported Transmit Power [dBm]** fields.
Analog RSSI [mV]	Displays the analog received signal strength indication level, in millivolts. This is the analog value the unit is reading, and does not give a true picture of RSSI and should be discarded.

Parameter	Description
Temperature	Displays the unit temperature, in degrees Celsius.
Antenna	**Synopsis:** { Connected, Disconnected } Displays the antenna connectivity status.

5. Click **Apply**.
6. If you changed the value in the **Configured Frequency [kHz]** field, stop and restart the base station service:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Stop Service**, and then click **Start Service**.

Section 5.9.2.3
Frame Settings

On the **Frame Settings** pane, review and set the frame parameters.

Procedure: Setting the Frame Parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link and then click the **Frame Settings** link. The **Frame Settings** pane appears.

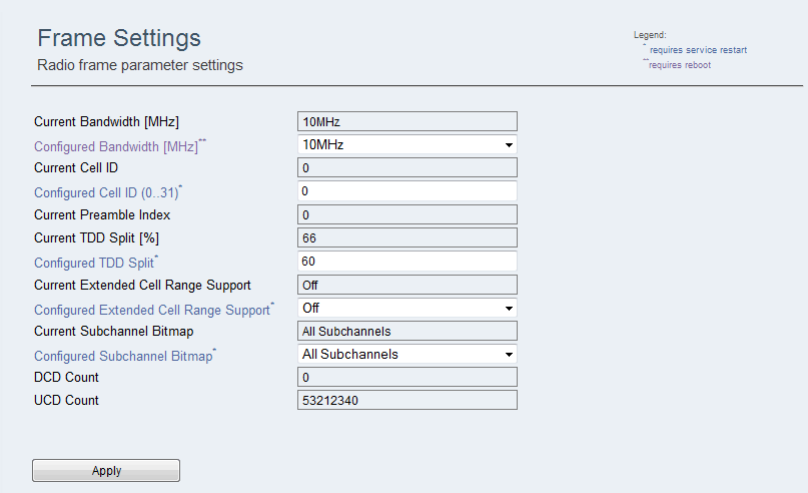


Figure 95: Frame Settings pane

3. Review and set the frame parameters in the following fields:

Table: Fields on the Frame Settings pane

Column	Description
Current Bandwidth [MHz]	Displays the current bandwidth setting, in megahertz. Values: 3.5MHz | 5MHz | 7MHz | 10Mhz Default: 10Mhz
Configured Bandwidth [MHz]	To set the frame bandwidth, select a value from the list.

Column	Description
	Values: 3.5 MHz | 5 MHz | 7 MHz | 10 Mhz Default: 10 Mhz
Current Cell ID	Displays the current base station cell identifier. Values: A number in the range of 0 to 31
Configured Cell ID (0..31)	To set the base station cell identifier, type a value in the range of 0 to 31 in this field. Values: A number in the range of 0 to 31
Current Preamble Index	Displays the current frame preamble index. The preamble index allows the subscriber station to perform frequency and time synchronization. This value should be different on neighboring base stations. Values: A number in the range of 0 to 113
Current TDD Split [%]	Displays the current frame TDD (Time Division Duplex) ratio between downlink and uplink. Values: A number in the range of 30 to 75. Default: 60
Configured TDD Split	To set the frame frame TDD (Time Division Duplex) ratio, type a value in the range of 30 to 75. For recommended values, refer to Table "Recommended TDD Split Values". **NOTE** *Supported TDD splits from previous versions can still be used. The recommended values provide the same uplink throughput, but with better download throughput due to more download symbols available from the same number of uplink symbols.* Values: A number in the range of 30 to 75. Default: 66
Current Extended Cell Range Support	Displays the current status of the Extended Cell Range Support feature. Values: On | Off Default: Off
Configured Extended Cell Range Support	To enable or disable Extended Cell Range Support, select a value from this list. Values: On | Off - see Table "Extended Cell Range Configuration Guidelines". Default: Off
Current Subchannel Bitmap	Displays the current Subchannel Bitmap setting. Values: All Subchannels | PUSC1 | PUSC2 | PUSC3 Default: All Subchannels
Configured Subchannel Bitmap	To change the Subchannel Bitmap, select a value from this list. Values: All Subchannels | PUSC1 1/3 | PUSC2 1/3 | PUSC3 1/3 | PUSC1 1/2 | PUSC2 1/2 Default: All Subchannels
DCD Count	Displays the Downlink Channel Descriptor Count. This parameter must be equal to the same parameter of the neighbor base station to optimize handover time.
UCD Count	Displays the Uplink Channel Descriptor Count. This parameter must be equal to the same parameter of the neighbor base station order to optimize handover time.

Table: Extended Cell Range Configuration Guidelines

Channel Bandwidth (MHz)	Subscriber Line of Site Distance from the Base Station (Km)	Extended Cell Range Configuration
5 MHz/10 MHz	Above 8 kilometers	ON
3.5 MHz/7 MHz	Above 19 kilometers	ON
5 MHz/10 MHz	Up to 8 kilometers	OFF
3.5 MHz/7 MHz	Up to 19 kilometers	OFF

Table: Recommended TDD Split Values

Channel	Non-Extended Cell Range			Extended Cell Range		
	Configured Split (%)	Actual Split (%)	Recommended Split (%)	Configured Split (%)	Actual Split (%)	Recommended Split (%)
5 MHz/10 MHz	30-34	32	36	30-31	29	33
	35-38	36	36	32-35	33	33
	39-42	40	40	36-39	38	38
	43-46	45	49	40-44	42	47
	47-51	49	49	45-48	47	47
	52-55	53	53	49-53	51	51
	56-59	57	62	54-57	56	60
	60-63	62	62	58-62	60	60
	64-68	66	66	63-66	64	64
	69-73	70	74	67-71	69	73
	74-75	74	74	72-75	73	73
3.5 MHz[a]/7 MHz	30	27	27	30-31	28	34
	31-36	33	33	32-37	34	34
	37-42	39	45	38-43	41	41
	43-48	45	45	44-49	47	53
	49-54	52	52	50-56	53	53
	55-60	58	64	57-62	59	59
	61-66	64	64	63-68	66	72
	67-72	70	70	69-74	72	72
	73-75	76	76	75	78	78

[a] *Configuration begins at 53% configured.*

4. Click **Apply**.
5. If you changed the values in the **Configured Cell ID (0..31)**, **Configured TDD Split**, **Configured Extended Cell Range Support**, or **Configured Subchannel Bitmap** fields, stop and restart the base station service:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Stop Service**, and then click **Start Service**.

6. If you changed the value in the **Configured Bandwidth** field, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

> **NOTE**
> *The TDD split in the uplink is as follows:*
> - *3.5 MHz is supported up to 47% in the uplink*
> - *5 MHz, 7 MHz and 10 MHz is supported up to 70% in the uplink*

Section 5.9.2.4
Link Adaptation

The **Link Adaptation Settings** pane displays and sets the downlink and uplink adaptation mode.

When the system is set to Auto mode, the downlink and uplink modulations, as well as the uplink sub-channels, are selected automatically (according to channel conditions; switching between modulations is seamless). This mode provides additional robustness at the expense of throughput.

When the base station is set to Manual mode, the download and uplink modulations are selected by the user. If the selected modulation does not match the current channel conditions, no data is transferred through the system.

Procedure: Setting the Link Adaptation Settings parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link and then click the **Link Adaptation** link. The **Link Adaptation Settings** pane appears.

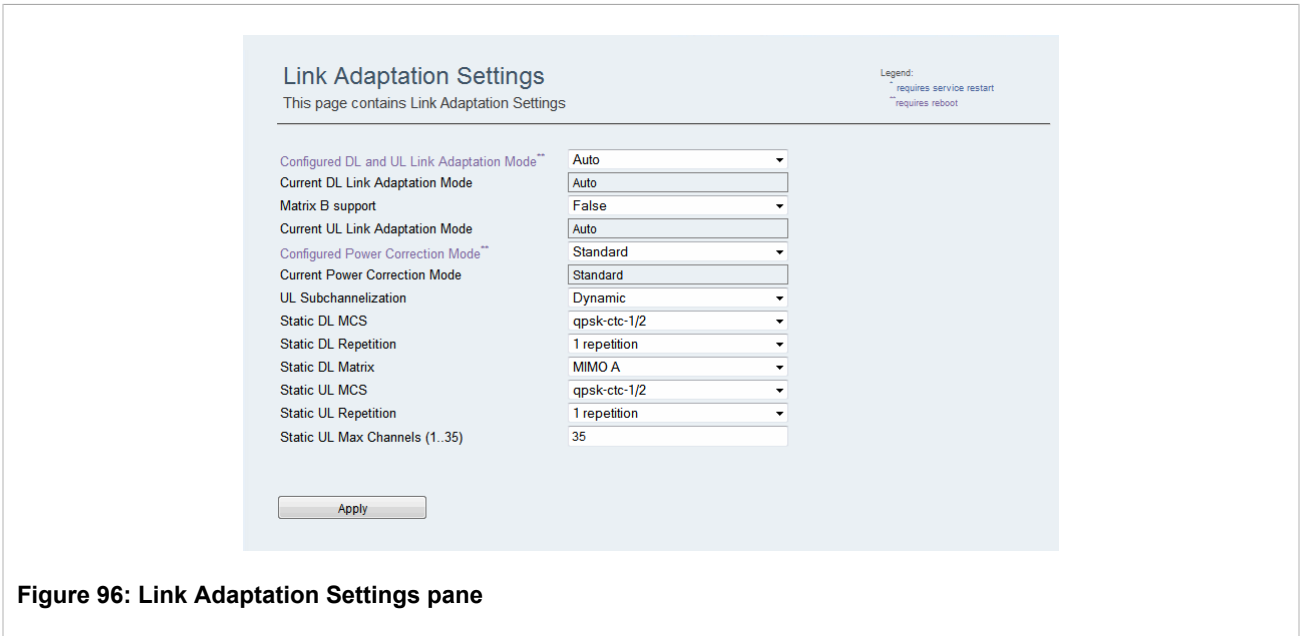


Figure 96: Link Adaptation Settings pane

3. Review and set the Link Adaptation parameters in the following fields:

Parameter	Description
Configured DL and UL Link Adaptation Mode	**Synopsis:** { Manual, Auto } **Default:** Auto To change the uplink link adaptation mode, select a value from this list. Both downlink and uplink should have the same settings. When choosing `Auto` for downlink, uplink will also be set to `Auto`.
Current DL Link Adaptation Mode	**Synopsis:** { Manual, Auto } **Default:** Auto Displays the current downlink link adaptation mode setting.
Matrix B Support	**Synopsis:** { True, False } **Default:** False To enable or disable MIMO Matrix B support for the entire base station, select a value from this list.
Current UL Link Adaptation Mode	Displays the current uplink link adaptation mode setting.
Configured Power Correction Mode	**Synopsis:** { Standard, Fast Fading } **Default:** Standard The power correction mode. Options include: • `Standard` – The default power correction algorithm. • `Fast Fading` – Power correction with no in-band interference.
UL Subchannelization	**Synopsis:** { Dynamic, All subchannels } **Default:** Dynamic To set the minimum allocated uplink sub-channels for automatic link adaptation, select a value from this list.
Static DL MCS	**Synopsis:** { qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6 } **Default:** qam64-ctc-5/6 This option applies to *static link adaptation*. To set the downlink modulation and coding scheme (MCS) for all subscriber stations, select a value from this list.
Static DL Repetition	**Synopsis:** { 1 repetition, 2 repetitions, 4 repetitions, 6 repetitions } **Default:** 1 repetition This option applies to *static link adaptation*. To set the downlink repetition for all subscriber stations, select a value from this list. This setting is valid only when downlink modulation is set to `qpsk-ctc-1/2`.
Static DL Matrix	**Synopsis:** { SISO, MIMO A, MIMO B } **Default:** MIMO A This option applies to *static link adaptation*. To set the MIMO configuration for all subscriber stations, select a value from this list.
Static UL MCS	**Synopsis:** { qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6 } **Default:** qam64-ctc-5/6 This option applies to *static link adaptation*.

Parameter	Description
	To set the uplink modulation and coding scheme (MCS) for all subscriber stations, select a value from this list.
Static UL Repetition	**Synopsis:** { 1 repetition, 2 repetitions, 4 repetitions, 6 repetitions } **Default:** 1 repetition This option applies to *static link adaptation*. To set the uplink repetition for all subscriber stations, select a value from this list. This setting is valid only when downlink modulation is set to `qpsk-ctc-1/2`.
Static UL Max Channels (1..35)	This option applies to *static link adaptation*. To set the maximum number of allocated uplink subchannels for all subscriber stations, type a value in the range of 1 to 35 in this field. **Synopsis:** { A number in the range of 1 to 35 } **Default:** 35

4. Click **Apply**.
5. If you changed the value in the **Configured DL and UL Link Adaptation Mode** field, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.
   b. Click **Reboot**.

Section 5.9.2.5
DL Coding and Modulation

On the **DL Coding and Modulation Settings** pane, review and configure the downlink coding and modulation settings.

Procedure: Setting the Downlink Coding and Modulation parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link and then click the **DL Modulation** link. The **DL Coding and Modulation Settings** pane appears.

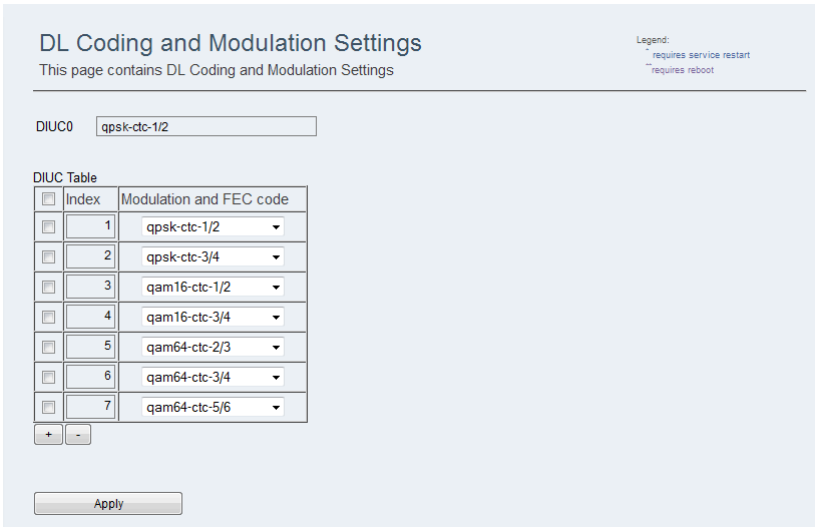


Figure 97: DL Coding and Modulation Settings pane

3. Review and set the Downlink Coding and Modulation settings in the **DIUC Table**:

Table: The DIUC Table

Column	Description
Index	Displays the DIUC (Downlink Interval Usage Code) Index. The burst profile in the downlink burst assignment is communicated through the Downlink Interval Usage Code. Index numbers 0 through 12 represent IUC 0 through IUC 12.
Modulation and FEC Code	Select a modulation and Forward Error Correction (FEC) code for each Index in the table. Values: qpsk-ctc-1/2 | qpsk-ctc-3/4 | qam16-ctc-1/2 | qam16-ctc-3/4 | qam64-ctc-2/3 | qam64-ctc-3/4 | qam64-ctc-5/6

4. To add a row to the table, click the + button.

   The table can contain up to 11 rows.

5. To remove a row from the table, select one or more rows from the table and click the - button.
6. Click **Apply**.

Section 5.9.2.6
UL Coding and Modulation

On the **UL Coding and Modulation Settings** pane, review and configure the uplink coding and modulation settings.

Procedure: Setting the Uplink Coding and Modulation parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link and then click the **UL Modulation** link. The **UL Coding and Modulation Settings** pane appears.

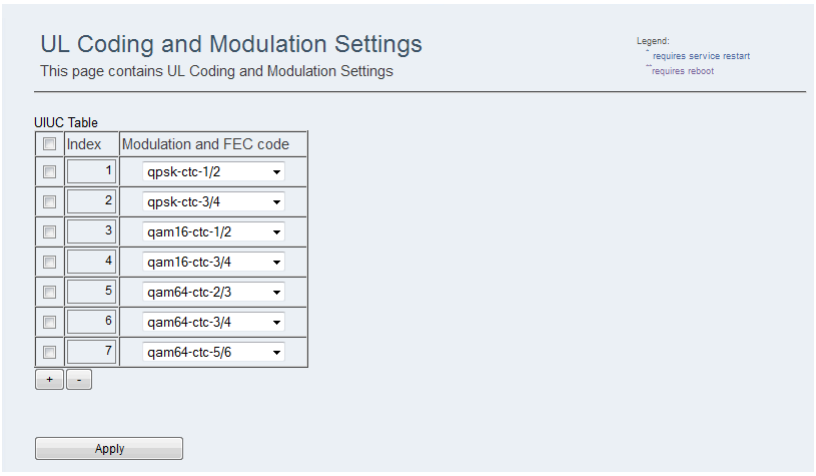


Figure 98: UL Coding and Modulation Settings pane

3. Review and set the Uplink Coding and Modulation settings in the **UIUC Table**:

Table: The UIUC Table

Column	Description
Index	Displays the UIUC (Uplink Interval Usage Code) Index. Index numbers 0 through 12 represent IUC 0 through IUC 12.
Modulation and FEC Code	Select a modulation and Forward Error Correction (FEC) code for each Index in the table. Values: qpsk-ctc-1/2 | qpsk-ctc-3/4 | qam16-ctc-1/2 | qam16-ctc-3/4 | qam64-ctc-2/3 | qam64-ctc-3/4 | qam64-ctc-5/6

4. To add a row to the table, click the + button.

   The table can contain up to 11 rows.

5. To remove a row from the table, click the - button.
6. Click **Apply**.

Section 5.9.2.7

Interference Detection

On the **Interference Detection Settings** pane, set the interference detection threshold.

Procedure: Setting the Interference Detection Threshold

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Radio and Frame** link and then click the **Interference Detection** link. The **Interference Detection Settings** pane appears.

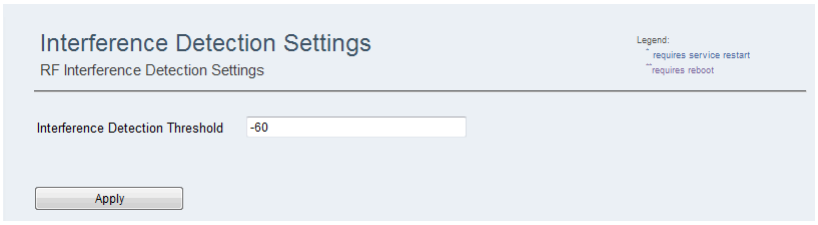


Figure 99: Interference Detection Settings pane

3. In the **Interference Detection Threshold** field, type a value. The default value is -60.
4. Click **Apply**.

Section 5.9.3

Wireless Security Authentication Settings

On the **Authentication Settings** pane, review and set the security protocol, timers, and counter settings.

The parameters you need to configure on this pane depend on the system operation mode:

- **Standalone mode:** requires the definition of AAA server parameters.
- **ASN-GW node:** requires the definition of just the operation and authentication mode parameters.

Procedure: Setting Wireless Authentication Settings

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **Wireless Security** link. The **Authentication Settings** pane appears.

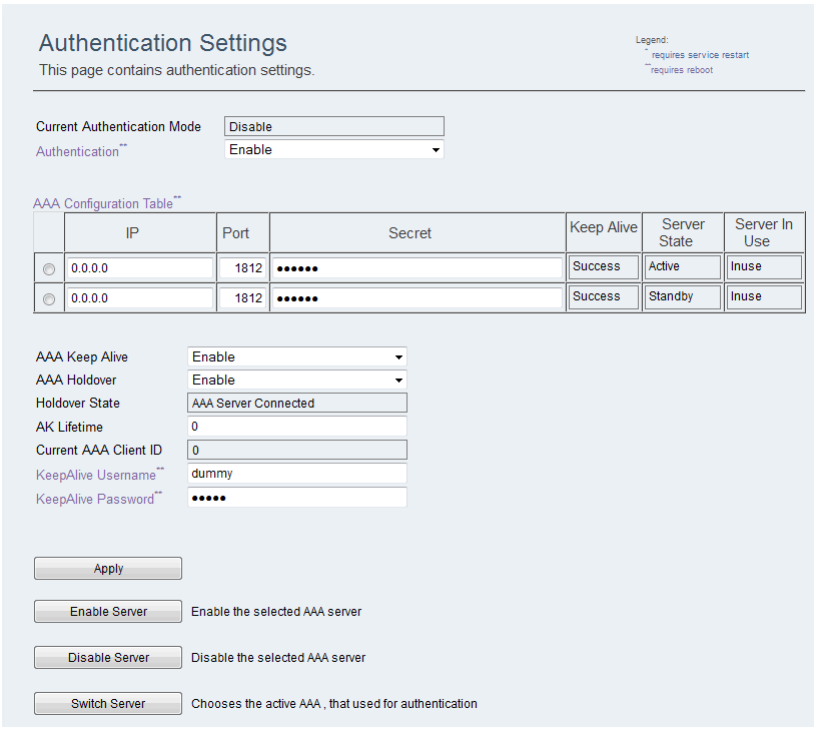


Figure 100: Wireless Security Authentication Settings pane

3. Review and set the authentication settings in the following fields:

Parameter	Description
Current Authentication Mode	**Synopsis:** { Enable, Disable } **Default:** Disable Displays the current authentication status.
Authentication	**Synopsis:** { Enable, Disable } **Default:** Disable To set the authentication mode, select a value from this list.

4. Review and set the authentication settings in the AAA Configuration Table:

Parameter	Description
IP	Displays the current Radius authentication server IP address. To change the IP address, type a value in this field. This field does not appear in ASN-GW mode.
Port	Displays the current AAA server port number. To change the port, type a value in this field. This field does not appear in ASN-GW mode.
Secret	Displays the current AAA server client secret. To change the secret, type a value in this field. This field does not appear in ASN-GW mode.
Keep Alive	**Synopsis:** { Success, Failed, N/A }

Parameter	Description
	Displays the Keep Alive status. This field does not appear in ASN-GW mode. The base station uses a defined KeepAlive username and password to check if the AAA server is active. If it is active, the Keep Alive status always appears as "success". If it is on standby, the status always appears as "failed".
Server State	**Synopsis:** { Active, Standby } Displays the server state. This field does not appear in ASN-GW mode. The active server is always in use. When the primary server is on standby, the base station switches to the secondary server. If both servers are on standby, the base station switches into holdover state until one of the servers becomes active again.
Server in Use	**Synopsis:** { Inuse, Disabled } Displays whether or not the server is in use. This field does not appear in ASN-GW mode.

5. Review and set the authentication settings in the following fields:

Parameter	Description
AAA Keep Alive	**Synopsis:** { Enable, Disable } To set the AAA Keep Alive mode, select a value from the list. This field does not appear in ASN-GW mode.
AAA Holdover	**Synopsis:** { Enable, Disable } To set the AAA Holdover mode, select a value from the list. This field does not appear in ASN-GW mode.
Holdover State	**Synopsis:** { Disabled, AAA Server Connected, In Holdover } Displays whether or not the AAA server is connected or in holdover state. This field does not appear in ASN-GW mode.
AK Lifetime	To set the AK Lifetime, type a value into this field. This field does not appear in ASN-GW mode.
Current AAA Client ID	Displays the current AAA server client identifier. This setting is read-only. This field does not appear in ASN-GW mode.
KeepAlive Username	Displays the KeepAlive username. To change the username, type a new username into this field. This field does not appear in ASN-GW mode.
KeepAlive Password	Displays the KeepAlive password. To change the password, type a new password into this field. This field does not appear in ASN-GW mode.

6. Click **Apply**.
7. If you changed the values in the **Authentication**, **IP**, **Port**, **Secret**, **Keep Alive**, **Server State**, **Server in Use**, **KeepAlive Username**, or **KeepAlive Password** fields, reboot the base station:
   a. Click **Quick Start**. The **Quick Start Settings** pane appears.

b. Click **Reboot**.

8. To enable a server, select a row from the table and click **Enable Server**.
9. To disable a server, select a row from the table and click **Disable Server**.
10. To switch servers, select a row from the table and click **Switch Server**.

Section 5.9.4
MAC

Different MAC configuration panes are available, depending on the base station operating mode:

Table: MAC Configuration Panes for each Operating Mode

Operating Mode	Available MAC Configuration Panes
Standalone mode	**MAC Settings** pane: configures the UCD/DCD (Uplink Channel Descriptor/Downlink Channel Descriptor) time interval and notifications.
ASN-GW mode	**MAC Settings** pane: configures the UCD/DCD (Uplink Channel Descriptor/Downlink Channel Descriptor) time interval and notifications. **Neighbor Settings** pane: configures neighbor base station information for handover. **DCD Triggers** pane: configures DCD (Downlink Channel Descriptor) triggers and timing for handover.

Section 5.9.4.1
MAC Settings

On the **MAC Settings** pane, configure general MAC settings, including message time intervals and formats.

Procedure: Setting the MAC Settings parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **MAC** link. The **MAC Settings** pane appears.

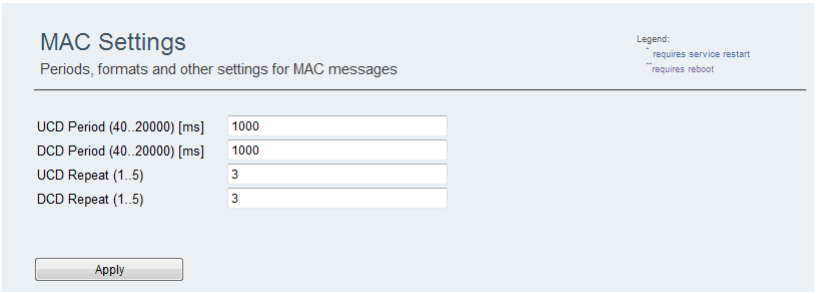


Figure 101: MAC Settings pane

3. Review and set the MAC settings in the following fields:

Parameter	Description
UCD Period	**Synopsis:** { A number in the range of 5 to 20000 } **Default:** 1000

Parameter	Description
	Sets the time interval, in milliseconds, after which the UCD (Uplink Channel Descriptor) appears. No user input is required here.
DCD Period	**Synopsis:** { A number in the range of 5 to 20000 } **Default:** 1000 Sets the time interval, in milliseconds, after which the DCD (Downlink Channel Descriptor) appears. No user input is required here.
UCD Repeat	**Synopsis:** { A number in range of 1 to 5 } **Default:** 3 Sets the number of UCD message notifications before a new message appears.
DCD Repeat	**Synopsis:** { A number in the range of 1 to 5 } **Default:** 3 Sets the number of DCD message notifications before new message appears.

4. Click **Apply**.

Section 5.9.4.2
Neighbor BS

The **Neighbor BS** pane is only available in ASN-GW mode. The **Neighbor BS Table** on this pane provides information about neighboring base stations. This information is used for handover between base stations.

Procedure: Setting Neighbor Base Station details

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **MAC** link and then click the **Neighbor BS** link. The **Neighbor Settings** pane appears.

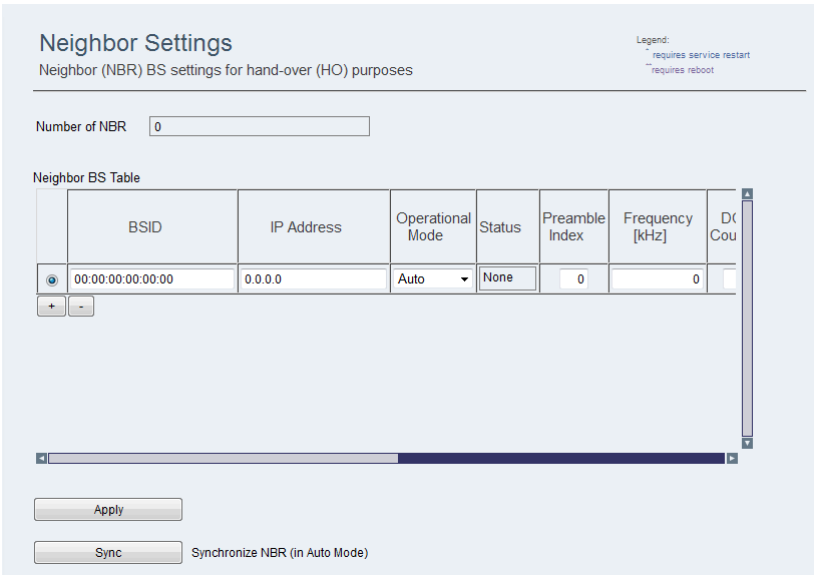


Figure 102: Neighbor Settings pane

3. Review and add neighboring base stations in the **Neighbor BS Table**.
4. To add a row to the table, click the + button.
5. To remove a row from the table, select a row from the table and click the - button.
6. After adding or editing neighboring base station information, click **Apply**.
7. To automatically synchronize information from neighboring base stations, click **Sync**.

Section 5.9.4.3
DCD Triggers

The **DCD Triggers** pane is only available in ASN-GW mode. The **DCD Table** on this pane displays DCD (Downlink Channel Descriptor) trigger settings. These provide timing and other parameters for handover triggers.

Procedure: Setting DCD Trigger parameters

1. Click **Wireless**. The **Network Identifiers** pane appears.
2. In the options pane, click the **MAC** link and then click the **DCD Triggers** link. The **DCD Triggers** pane appears.

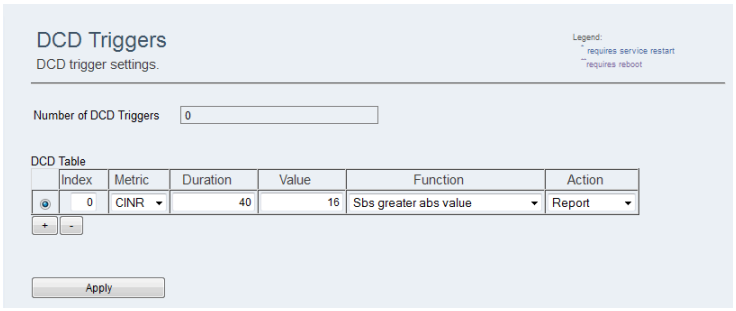


Figure 103: DCD Triggers pane

3. The **Number of DCD Triggers** field displays the number of configured DVD triggers.
4. Review and set the DCD trigger settings in the **DCD Table**:

Table: Fields on the DCD Triggers pane

Column	Description
Index	An index number for the DCD trigger. Default: 0
Metric	Sets the DCD metric. To set the metric, select a value from this list. Values: CINR | RSSI | RTD Default: CINR
Duration	Sets the average interval in frames duration. To set the duration, type a value in the range of 1 to 100. Values: A number in the range of 1 to 100. Default: 40
Value [1/2 dB]	Sets the trigger value used in comparing measured metric. To set the trigger value, type a value in the range of -100 to 100. Values: A number in the range of -100 to 100. Default: 16
Function	Sets the metric function. To set the metric function, select a value from this list. Values: Nbs greater abs value | Nbs less abs value | Nbs greater rel value | Nbs less rel value | Sbs greater abs value | Sbs less abs value Default: Sbs greater abs value
Action	Sets the action performed upon reaching the trigger condition. To set the action, select a value from this list. Values: Report | Handover | Scanning Default: Report

5. To add a row to the table, click the + button.
6. To remove a row from the table, select a row from the table and click the - button.
7. After adding or editing DCD trigger settings, click **Apply**.

6 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM WIN. It describes the following tasks:

IMPORTANT!
For further assistance, contact Siemens Customer Support.

Section 6.1
No IP connectivity

If there is no IP connectivity between the base station and the NMS, perform the following steps:

1. Connect the computer and the base station console connector (serial connection), located on the unit’s bottom panel.
2. In the terminal, type **`showIPAddr`** and press **Enter**. The base station’s IP address will be displayed.
3. Ping the base station IP address.
4. If connectivity is still not established, contact Siemens customer support.

Section 6.2
No Serial Connection

If there is no serial connection when using the serial cable, perform the following:

1. Verify IP connectivity using a ping to the base station IP address.
2. If there is no IP connectivity, verify the power connections.
3. If the power connections are okay, however, there is still no serial connection or IP connectivity, contact Siemens customer support.