SIEMENS

RUGGEDCOM WIN v5.1

User Guide

For WIN5114, WIN5114-AC-IS, WIN5114-V, WIN5114-V-GPS, WIN5118, WIN5118-AC-IS, WIN5123, WIN5123-AC-IS, WIN5125, WIN5125-AC-IS, WIN5135, WIN5135-AC-IS, WIN5137, WIN5137-AC-IS, WIN5137-V, WIN5137-V-GPS, WIN5149, WIN5149-AC-IS, WIN5151, WIN5151-AC-IS, WIN5151-V, WIN5151-V-GPS, WIN5158, WIN5158-AC-IS, WIN5158-V, WIN5158-V-GPS, WIN5214, WIN5214-IS, WIN5218, WIN5218-IS, WIN5223, WIN5223-IS, WIN5225, WIN5225-IS, WIN5235, WIN5235-IS, WIN5237, WIN5237-IS, WIN5249, WIN5249-IS, WIN5251, WIN5251-IS, WIN5258, WIN5258-IS

03/2018

RC1358-EN-01

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 https://www.siemens.com/industrialsecurity.

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

Warranty

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

For warranty details, visit https://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

https://www.siemens.com/ruggedcom

Table of Contents

Preface

This guide describes v5.1 of the RUGGEDCOM WIN Web-based user interface and software application running on RUGGEDCOM Subscriber Station (SS), or Customer Premises Equipment (CPE), devices. The WIN5100 and WIN5200 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 subscriber 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.

CONTENTS

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

Product Notes

Document Title	Link
RUGGEDCOM WIN v5.1 General Availability Patch Release	https://support.industry.siemens.com/cs/ww/en/view/109751397

User/Reference Guides

Document Title	Link
RUGGEDCOM WIN v5.1 User Guide for RUGGEDCOM WIN7000 subscriber stations	https://support.industry.siemens.com/cs/ww/en/view/109751373
RUGGEDCOM NMS User Guide	https://support.industry.siemens.com/cs/ww/en/ps/15399/man

FAQs

Document Title	Link
How to Configure Free Radius Server?	https://support.industry.siemens.com/cs/ww/en/view/103156513
How to Configure the NTP Settings for the CPEs?	https://support.industry.siemens.com/cs/ww/en/view/103155852
How to Load Dictionaries to Different AAAs?	https://support.industry.siemens.com/cs/ww/en/view/103156416
What are the Limitations and Workarounds related to Greenpacket 0x350i?	https://support.industry.siemens.com/cs/ww/en/view/103949465
What Impacts A Clock's Quality?	https://support.industry.siemens.com/cs/ww/en/view/104466716
Understanding Latency Between the RUGGEDCOM WIN Base Station (BS) and the RUGGEDCOM WIN Subscriber Station (SS)	https://support.industry.siemens.com/cs/ww/en/view/103948900
Understanding VoIP	https://support.industry.siemens.com/cs/ww/en/view/104466526
Understanding Propagation Models	https://support.industry.siemens.com/cs/ww/en/view/104466448
Understanding Partially Used Subchannels (PUSC)	https://support.industry.siemens.com/cs/ww/en/view/104466301
Understanding Reuse 1 Topology	https://support.industry.siemens.com/cs/ww/en/view/104466454
RUGGEDCOM WIN Network Interface Protocol API	https://support.industry.siemens.com/cs/ww/en/view/109741871

Installation Guides

Document Title	Link
RUGGEDCOM WIN5114 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96998873

Document Title	Link
RUGGEDCOM WIN5114-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751399
RUGGEDCOM WIN5114-V Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751400
RUGGEDCOM WIN5114-V-GPS Hardware	https://support.industry.siemens.com/cs/ww/en/view/109751401
RUGGEDCOM WIN5118 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97019959
RUGGEDCOM WIN5118-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751402
RUGGEDCOM WIN5123 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97012843
RUGGEDCOM WIN5123-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751403
RUGGEDCOM WIN5125 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96999539
RUGGEDCOM WIN5125-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751404
RUGGEDCOM WIN5135 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97012844
RUGGEDCOM WIN5135-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751405
RUGGEDCOM WIN5137 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97000003
RUGGEDCOM WIN5137-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751404
RUGGEDCOM WIN5137-V Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751407
RUGGEDCOM WIN5137-V-GPS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751408
RUGGEDCOM WIN5149 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97002225
RUGGEDCOM WIN5149-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751409
RUGGEDCOM WIN5151 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109480105
RUGGEDCOM WIN5151-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751410
RUGGEDCOM WIN5151-V Hardware Guide	https://support.industry.siemens.com/cs/ww/en/view/109751411
RUGGEDCOM WIN5151-V-GPS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751412
RUGGEDCOM WIN5158 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97000008
RUGGEDCOM WIN5158-AC-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751413
RUGGEDCOM WIN5158-V Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109739038
RUGGEDCOM WIN5158-V-GPS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109739041
RUGGEDCOM WIN5214 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96999797
RUGGEDCOM WIN5214-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751414
RUGGEDCOM WIN5218 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97012847
RUGGEDCOM WIN5218-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751415
RUGGEDCOM WIN5223 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96999542
RUGGEDCOM WIN5223-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751417
RUGGEDCOM WIN5225 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96999543
RUGGEDCOM WIN5225-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751418
RUGGEDCOM WIN5235 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97000010

Document Title	Link
RUGGEDCOM WIN5235-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751419
RUGGEDCOM WIN5237 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96999908
RUGGEDCOM WIN5237-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751420
RUGGEDCOM WIN5249 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/97002238
RUGGEDCOM WIN5249-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751421
RUGGEDCOM WIN5251 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109480108
RUGGEDCOM WIN5251-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751422
RUGGEDCOM WIN5258 Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/96999910
RUGGEDCOM WIN5258-IS Installation Guide	https://support.industry.siemens.com/cs/ww/en/view/109751423

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 https://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 v5.1 User Guide for RUGGEDCOM WIN5100 and WIN5200 series Out Door Unit (ODU) Subscriber Stations (SS). This guide describes the wide array of features made available by the RUGGEDCOM WIN software. These features include:

Software Features

- Intuitive user interface and parameter groupings
- Advanced communication monitoring and troubleshooting tools
- HTTPS
- SNMPv2 and SNMPv3
- Management VLAN
- Remote software upgrades via SFTP
- Antenna alignment with LEDs
- Network Interface Protocol
- QoS according to IEEE 802.16e-2009
- SSHv2
- Password Management - local and RADIUS
- Device Authentication via PKMv2 (EAP-TLS/TTLS)
- X.509 certificates
- NTP server
- Ethernet Lock feature
- MAC address list

Hardware Features

- Mobile WiMAX Wave 2 MIMO Features
- Time Division Duplexing (TDD)
- Coding Rates
- Modulation
- Convolution Turbo Coding Correction
- Deployment Models
- Service Flows

CONTENTS

Section 1.1

Features and Benefits

The following describes the many features available in RUGGEDCOM WIN and their benefits:

- **Mobile-WiMAX Compliance**
  Compliant with IEEE 802.16e standard and WiMAX Forum Wave 2 Profiles.
- **Voice, Video and Data Services**
  RUGGEDCOM WIN provides guaranteed voice, video and data services based on advanced Quality of Service (QoS).
- **NTP (Network Time Protocol)**
  NTP automatically synchronizes the internal clock of all RUGGEDCOM WIN devices on the network. This allows for correlation of time stamped events for troubleshooting.
- **Simple Network Management Protocol (SNMP)**
  SNMP provides a standardized method, for network management stations, to interrogate devices from different vendors. SNMP versions 2c and 3 are supported. SNMPv3 in particular provides security features (such as authentication, privacy, and access control) not present in earlier SNMP versions.
- **Event Logging and Alarms**
  RUGGEDCOM WIN records all significant events to a non-volatile system log allowing forensic troubleshooting. Events include link failure and recovery, unauthorized access, broadcast storm detection, and self-test diagnostics among others. Alarms provide a snapshot of recent events that have yet to be acknowledged by the network administrator. An external hardware relay is de-energized during the presence of critical alarms, allowing an external controller to react if desired.
- **HTML Web Browser User Interface**
  RUGGEDCOM WIN provides a simple, intuitive user interface for configuration and monitoring via a standard graphical Web browser or via a standard telcom user interface. All system parameters include detailed online help to facilitate setup and configuration. RUGGEDCOM WIN presents a common look and feel and standardized configuration process, allowing easy migration to other managed RUGGEDCOM products.

Section 1.2

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

- It is highly recommended to configure Brute Force Attack (BFA) protection to prevent a third-party from obtaining unauthorized access to the device. For more information, refer to Section 6.1, "Configuring Brute Force Attack Protection".
- 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.
- 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 1.3

Mobile WiMAX Wave 2 MIMO Features

Multiple-Input, Multiple-Output (MIMO) describes systems that use more than one radio and antenna system at each end of the wireless link. In the past it was too costly to incorporate multiple antennas and radios in a subscriber terminal. Recent advances in radio miniaturization and integration technology now make it feasible and cost effective. Combining two or more received signals has the immediate benefit of improving received signal strength, but MIMO also enables transmission of parallel data streams for greater throughput. For example, in a 2 × 2 MIMO (two transmit and two receive elements), dual polarization point-to-point system, the carrier's allocated frequency can be used twice, effectively doubling the throughput data rate.

In point-to-multipoint systems employing MIMO, each base station antenna transmits a different data stream and each subscriber terminal receives various components of the transmitted signals with each of its subscriber antennas. The subscriber terminal is able to algorithmically separate and decode the parallel simultaneously received data streams.

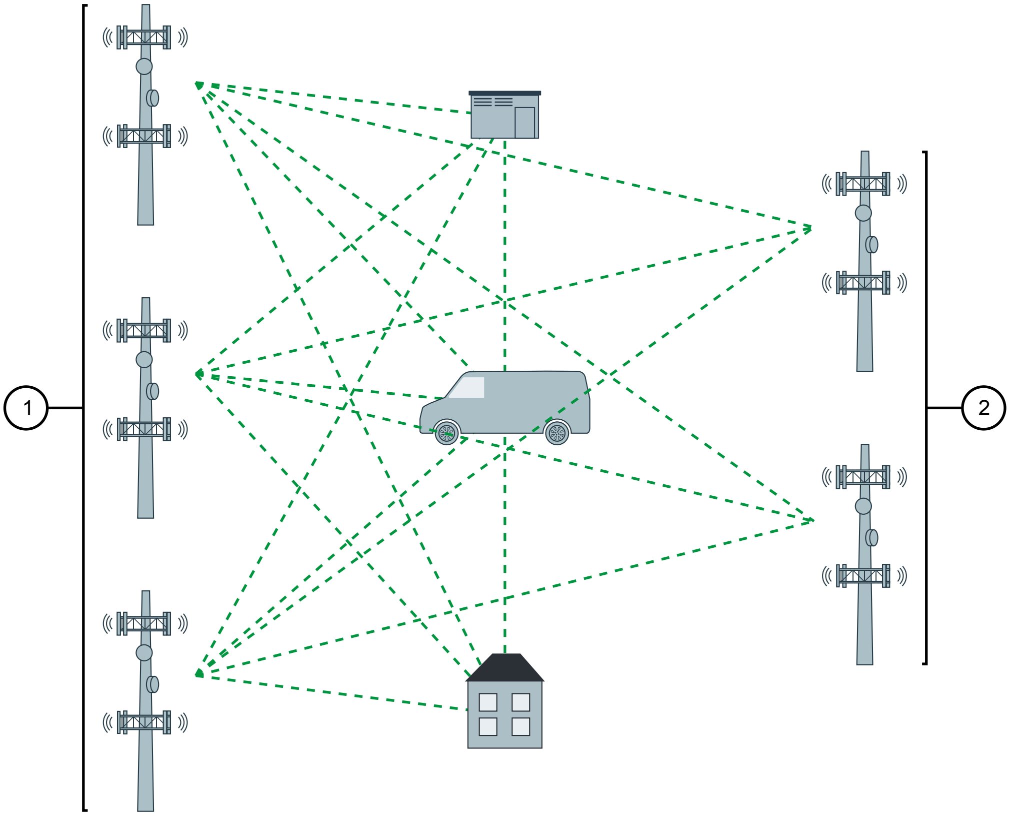


Figure 1: MIMO Antenna System

1. MIMO Transmitters with Antenna **2.** MIMO Receivers with Antenna

Section 1.4

Space-Time Coding

Space-Time Coding (STC) is a technique for implementing transmission diversity. Mobile WiMAX uses transmit diversity in the downlink direction to provide spatial diversity to enhance the signal quality to a specific subscriber located anywhere within the range of the antenna beam. Although providing less signal gain than beam-forming, transmit diversity is more robust for mobile users as it does not require prior knowledge of the path characteristics of a subscriber's particular frequency channel. One such STC technique, known as the Alamouti Code, is incorporated in the WiMAX IEEE 802.16e standard.

Section 1.5

Time Division Duplexing (TDD)

The subscriber station uses time division duplexing (TDD) to transmit and receive on the same RF channel. This is a non-contention based method for providing an efficient and predictable two-way Point-To-Point (PTP) or Point-To_Multipoint (PMP) cell deployment. All uplink and downlink transmission scheduling is managed by the base station. The base station sends data traffic to subscribers, polls for grant requests, and sends grant acknowledgements based on the total of all traffic to all subscribers.

Section 1.6

Coding Rates

Each burst of data transmitted over the wireless interface is padded with redundant information, making it more resistant to potential over-the-air errors. The coding rate is the ratio of user data to the total data transmitted including the redundant error correction data. The base station supports coding rates of 1/2, 2/3, and 3/4.

Section 1.7

Supported Modulation Techniques

The modulation technique specifies how the data is coded within the OFDMA carriers. The supports Quadrature Phase Shift Keying (QPSK), 16 Quadarature Amplitude Modulation (QAM), and 64 QAM modulations.

The following details the *over-the-air* data rate for each supported modulation type.

Modulation Type	MCS Index	Spatial Streams	Coding Rate	Data Rate			
				20 MHz Channel		40 MHz Channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
QPSK	1	1	1/2	13.0	14.4	27.0	30.0
QPSK	2	1	3/4	19.5	21.7	40.5	45.0
16-QAM	11	2	1/2	52.0	57.8	108.0	120.0
16-QAM	12	2	3/4	78.0	86.7	162.0	180.0
64-QAM	21	3	2/3	156.0	173.3	324.0	360.0

Modulation Type	MCS Index	Spatial Streams	Coding Rate	Data Rate			
				20 MHz Channel		40 MHz Channel	
				800 ns GI	400 ns GI	800 ns GI	400 ns GI
64-QAM	22	3	3/4	175.5	195.0	364.5	405.0
64-QAM	23	3	5/6	195.0	216.7	405.0	450.0

Section 1.8

Convolution Turbo Coding Correction

Convolution Coding (CC) error correction is enabled for all traffic rates. This low-level process can correct bursts of errors in received messages and reduce the number of retransmissions.

Section 1.9

Deployment Models

The subscriber station supports the following deployment scenarios.

- **PTP Deployment**
  When deployed in a Point-To-Point (PTP) configuration, the base station establishes a dedicated bidirectional link to a single subscriber. PTP deployments typically use a directional narrow beam antenna for both ends of the link.
- **PMP Deployment**
  When deployed in a Point-To-Multipoint (PMP) configuration, the base station establishes bi-directional links to more than one subscriber. PMP deployments typically use a wide beam (sector) antenna at the base station and a narrow beam antenna at the subscriber. Service flows are used to police service level agreements for each subscriber.

Section 1.10

Non Line-of-Sight

The RUGGEDCOM WIN product family supports line-of-sight (LOS) and non line-of-sight (NLOS) operation. A clear LOS link has no obstacles within 60% of the first Fresnel zone of the direct path.

A wireless link is considered non-LOS if natural or man-made structures block the visible path between the base station and the subscriber station. In this case, a wireless link can be established only if a reflective path can be established between the base station and subscriber station.

Section 1.11

Channelization

The subscriber station is a frequency-specific system, with the frequency band defined by the PHY (physical) unit. The use of the operating band must be in accordance with local regulation requirements.

The subscriber station divides the available frequency band into channels. Allocation of channels during deployment is dependent on spectrum availability in the licensed band and local licensing requirements and conditions. Channel selection allows planners to obtain the maximum geographic coverage, while avoiding frequency contention in adjacent sectors.

Section 1.12

Service Flows

Service flows are a key feature of the IEEE 802.16e standard. A service flow represents a unidirectional data flow having separate Quality of Service (QoS) settings for uplink and downlink. Service flows provide the ability to set up multiple connections to each subscriber in a sector.

Separate service flows can be established for uplink and downlink traffic, where each service flow is assigned a unique service level category and separate QoS settings. This feature allows segregation of high-speed/high-priority traffic from less time-critical flows.

›› Service Flow Classification

Data packets are forwarded based on classification rules. Classification rules examine each packet for pattern matches such as destination address, source address, IP TOS, or VLAN tag. All classification is defined at the base station and the classification parameters are downloaded to the subscriber.

›› Default Service Flows

Default uplink and downlink service flows are created automatically for each registered subscriber. These service flows are used to pass all traffic not matching any user-defined service flow (such as broadcast ARP) between the base station and subscribers. The default service flow capacity is limited for each subscriber.

›› Scheduling

The serving base station enforces QoS settings for each service flow by controlling all uplink and downlink traffic scheduling. This provides a non-contention based traffic model with predictable transmission characteristics. By analyzing the total of all requests from all subscribers, the base station makes sure uplink and downlink traffic conforms to the current Service Level Agreements (SLAs). Centralized scheduling increases predictability of traffic, eliminates contention, and provides the maximum opportunity for reducing overhead.

A regular period is scheduled for subscribers to register with the base station. These subscribers may be newly commissioned or have been deregistered due to service outage or interference on the wireless interface. This is the only opportunity for multiple subscribers to transmit simultaneously.

Section 1.13

User Permissions

The following actions can be performed by users with administrator or guest privileges.

Action	Privilege Level	
	Administrator	Guest
View statistics	•	•

Action	Privilege Level	
	Administrator	Guest
Clear statistics	•	•
Configure settings	•	
Add/remove users	•	
Update/downgrade software	•	
Manage system files	•	
Access developer mode	•	

2 Using WIN v5.1

This chapter describes how to use the RUGGEDCOM WIN interface.

CONTENTS

Section 2.1

Default User Names and Passwords

The following default user names and passwords are pre-configured for RUGGEDCOM WIN:

> ⚠ **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. To prevent unauthorized access to the subscriber station, change the default passwords before commissioning the device. For more information, refer to Section 5.3, “Managing Users and Passwords”.*

User Name	admin
Password	generic

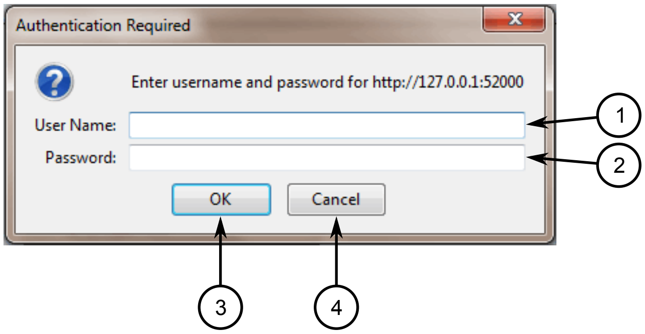
Section 2.2

Logging In

To log in to the subscriber station, do the following:

> **IMPORTANT!**
> *When accessing the device for the first time, use the factory default IP address, user name and password to access the RUGGEDCOM WIN user interface. For more information, refer to Section 3.2.1, “Default IP Address” and Section 2.1, “Default User Names and Passwords”.*

1. Launch a Web browser and request a connection to the subscriber station. The **Authentication Required** form appears.



Authentication Required

Enter username and password for http://127.0.0.1:52000

Figure 2: Authentication Required Form

1. User Name Box **2.** Password Box **3.** OK Button **4.** Cancel Button

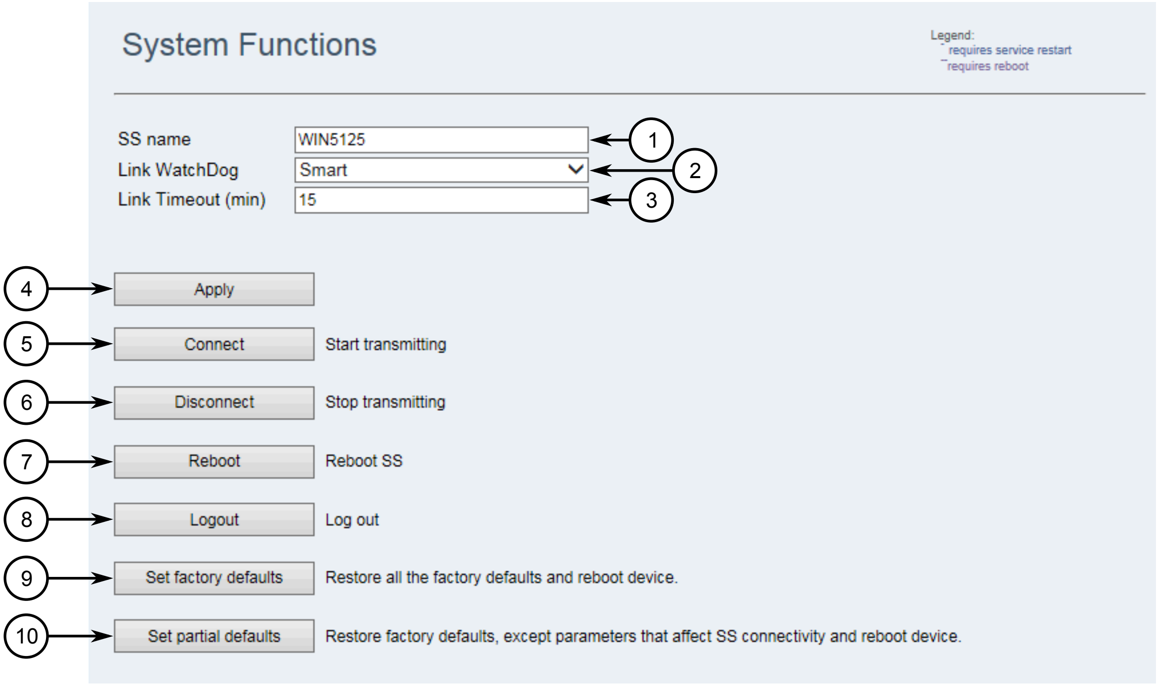
2. Under **User Name**, enter the user name.
3. Under **Password**, enter the password associated with the user name.
4. Click **OK**.

Section 2.3

Logging Out

To log out, do the following:

1. Navigate to ***Management***. The **System Functions** screen appears.



System Functions

Legend:
requires service restart
requires reboot

SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Apply

Connect: Start transmitting

Disconnect: Stop transmitting

Reboot: Reboot SS

Logout: Log out

Set factory defaults: Restore all the factory defaults and reboot device.

Set partial defaults: Restore factory defaults, except parameters that affect SS connectivity and reboot device.

Figure 3: System Functions Screen

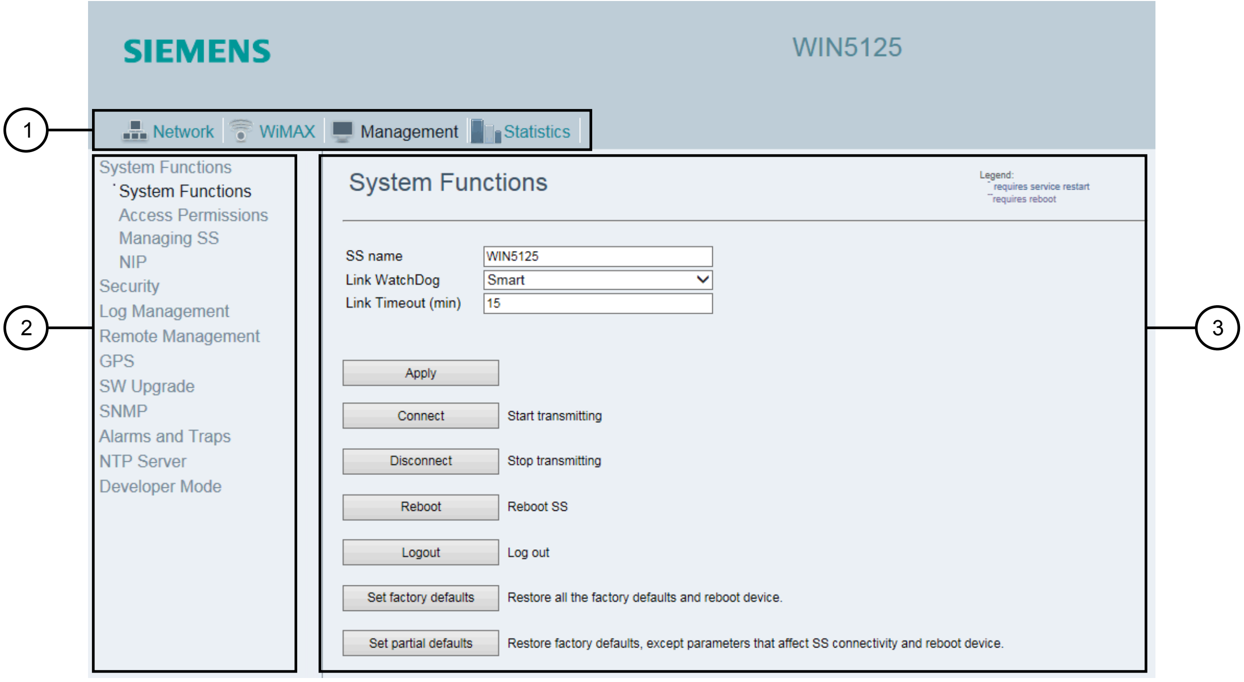
1. CPE Name Box **2.** Link Watchdog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Part Defaults Button

2. Click **Logout**.

Section 2.4

Using the Web-Based User Interface

The following is an example of the RUGGEDCOM WIN Web-based user interface.



SS name WIN5125
Link WatchDog Smart
Link Timeout (min) 15

Figure 4: Management Interface

1. Toolbar **2.** Menu Tree **3.** Main Screen

The user interface consists of the following areas:

- **Toolbar** – A series of links (i.e. Admin, Subscribers, etc.) that provide access to a specific feature set. For more information about using the toolbar, refer to Section 2.4.1, “Navigating the User Interface”.
- **Menu Tree** – Displays the various features that can be configured in tree structure. The relevant parameters and controls appear in the main screen.
- **Main Screen** – Displays the relevant parameters and controls for the selected feature.

CONTENTS

Section 2.4.1

Navigating the User Interface

Navigating to the various parameters and controls in RUGGEDCOM WIN starts at the toolbar. The toolbar features a series of links that provide access to a specific feature set. When clicked, the applicable screens are listed in the menu tree.

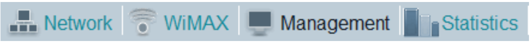


Figure 5: Toolbar

Toolbar Links

Link	Description
Network	Access to RUGGEDCOM WIN network settings.
WiMAX	Access to WiMAX scanner, authentication, mobility, and radio settings.
Management	Access to general RUGGEDCOM WIN management settings and functions.
Statistics	Displays general RUGGEDCOM WIN, RF, network, and service flow statistics.

Navigation Steps in this User Guide

Each task described in this User Guide will begin with a navigation step (e.g. *Navigate to...*) that instructs users to first click a link on the toolbar and then follow the menu tree to find the target screen. For example:

1. Navigate to ***Statistics » General » Device Info***.

Section 2.4.2

Using Tables

This section describes features common to most tables in the user interface.

Adding and Deleting Table Rows

Some tables allow for rows to be added or removed. These tables are followed by **Add** (⊞) and **Delete**⊟ buttons.

To add a row, click the ⊞ button.

To delete a row, select the desirec row and then click the ⊟ button.

Filtering Table Columns

Some tables feature controls for filtering content based on individual columns. These tables are preceded by a block similar to the following:

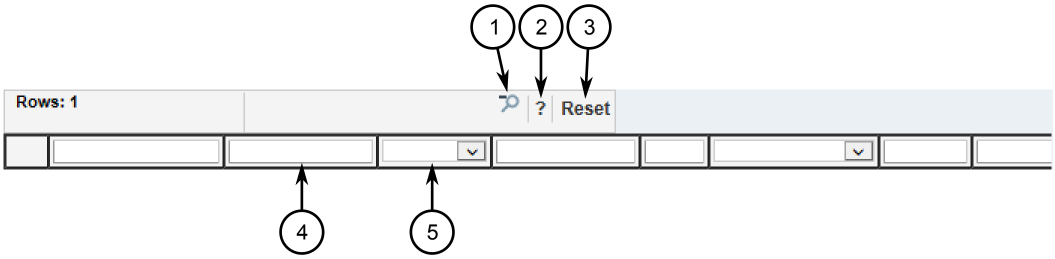


Figure 6: Table Filtering Controls (Example)

1. Filter Icon **2.** Help Icon **3.** Reset **4.** Box **5.** List

To filter the contents of a table, click the filtering icon (🔍). A new row appears above the table with a box or list in each cell.

- **Lists** filter the table based on the values available in a specific column. Click the list to display the full list and then select the desired text. Only rows that contain that text in that column appear.
- **Boxes** filter the table based on a search string. The string can be a full or partial text string. The table will be filtered based on cells in that column that match the text string.

  Select operators can also be used to further refine the filtering results. Click the Help icon (**?**) to display the following list of operators.

Operator	Description	Operator	Description
< X	Less than a specified value	X / Y	Starts with and ends with
<= X	Less than or equal to a specified value	||	OR
>	Greater than a specified value	&&	AND
>= X	Greater than or equal to a specified value	[empty]	Empty cells
= X	Equal to a specified value	[nonempty]	Non-empty cells

Filters can be added to multiple columns for more accurate results.

To reset all filtering, click **Reset**.

To turn off filtering, click the filtering icon again (🔍).

3 Getting Started

This section describes startup tasks to be performed during the initial commissioning of the subscriber station.

CONTENTS

Section 3.1

Basic Configuration

This section describes the basic steps required to connect the subscriber station to the network. Once these steps are completed, additional features can be enabled and configured either directly through the RUGGEDCOM WIN user interface or remotely via RUGGEDCOM NMS.

> **NOTE**
> *For more information about RUGGEDCOM NMS, refer to the RUGGEDCOM NMS User Guide [https://support.industry.siemens.com/cs/ww/en/ps/15399/man].*

To configure the initial settings for the subscriber station, do the following:

1. Establish a direct connection to the subscriber station. For more information, refer to Section 3.2.2, “Connecting Directly”.

2. Log in to the subscriber station using the default user name and password. For more information, refer to Section 2.2, “Logging In”.

   > **WARNING!**
   > *Radiation hazard – risk of Radio Frequency (RF) exposure. For GPS-enabled subscriber stations, the GPS receiver is enabled by default. While emitted radiation is minimal, to avoid exposure, stand at least 3.6 m (11.8 ft) from the subscriber station at all times.*
   >
   > *If operating the subscriber station in an enclosed environment, such as a lab, make sure the GPS receiver is disabled as soon as possible after powering on the device.*

3. If operating in an enclosed environment, such as a lab, disable the GPS receiver. This is done by setting `GPS Enabled` to `False`. For more information, refer to Section 4.11.1, “Enabling/Disabling the GPS”.

   > **NOTE**
   > *A system reboot is required after changing the operating mode.*

4. Configure the LAN (private) and WAN (public) IP addresses for the subscriber station. For more information, refer to Section 3.3, “Configuring the Subscriber Station's IP Interface”.

5. Replace the default SSH keys. For more information, refer to Section 6.4.3, "Generating SSH Keys".
6. [Optional] If the base station is to be remotely managed by a Network Management System (NMS), such as RUGGEDCOM NMS, create an SNMP trap destination for the associated workstation. For more information, refer to Section 10.1.4.3, "Configuring SNMP Trap Destinations".
7. Configure the scanner. For more information, refer to Section 8.3.2, "Configuring the Scanner".
8. Connect to a base station. For more information, refer to Section 8.1, "Connecting to a Base Station".
9. Review the statistics and verify the verify the network connection. For more information, refer to Section 4.5, "Viewing Statistics".
10. View the service flow information and make sure the service flows are created. For more information, refer to Section 4.5.3, "Viewing and Clearing Service Flow Statistics".
11. Further configure the subscriber station as needed.

Section 3.2

Connecting to the Subscriber Station

This section describes how to connnect to the subscriber station directly and remotely.

- **Direct Connections**
  Establish a direct (local) connection to the subscriber station during initial deployment. Physical access, an Ethernet cable, and a workstation are required.
- **Remote Connections**
  Establish a remote connection to the subscriber station using a Web browser or Telnet/SSH terminal. A network connection and workstation are required.

CONTENTS

Section 3.2.1

Default IP Address

The default IP address for the subscriber station is `192.168.254.251/24`.

This is referred to as the **LAN IP** address.

Section 3.2.2

Connecting Directly

RUGGEDCOM WIN can be accessed through a direct Ethernet connection for management and troubleshooting purposes. The Ethernet connection provides access to the Web user interface.

To establish a direct Ethernet connection to the device, do the following:

1. On the workstation being used to access the device, configure the IP address range and subnet mask for an Ethernet port. The range is typically the IP address for the subscriber station plus one, ending at *.*.*.254.

   For example, if the subscriber station's IP address is `192.168.254.251`, configure the workstation's Ethernet port with an IPv4 address in the range of 192.168.254.0/24 to 192.168.254.254/24.
2. Connect an Ethernet cable between the workstation and the **DC/ETH** port on the subscriber station.
3. Launch a Web browser. For a list of compatible Web browsers, refer to "System Requirements".
4. If using a proxy server, make sure the IP address and subnet for the device are included in the list of exceptions.
5. In the address bar, enter the subscriber station's IP address and then press **Enter**.

   IMPORTANT!
   Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.
6. If the device's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Confirm the connection to continue.
7. Log in to RUGGEDCOM WIN. For more information about logging in, refer to Section 2.2, "Logging In".

Section 3.2.3

Connecting Remotely

The subscriber station can be accessed over the network either through a Web browser, terminal or a workstation running terminal emulation software.

Using a Web Browser

To establish a connection through a Web browser, do the following:

1. On the workstation being used to access the device, configure the IP address range and subnet mask for an Ethernet port. The range is typically the IP address for the subscriber station plus one, ending at *.*.*.254.

   For example, if the subscriber station's IP address is `192.168.254.251`, configure the workstation's Ethernet port with an IPv4 address in the range of 192.168.254.250 to 192.168.254.254.
2. Make sure the workstation is connected to the network.
3. Launch a Web browser. For a list of compatible Web browsers, refer to "System Requirements".
4. If using a proxy server, make sure the IP address and subnet for the device are included in the list of exceptions.
5. In the address bar, enter the subscriber station's LAN IP address and then press **Enter**.

   IMPORTANT!
   Upon connecting to the device, some Web browsers may report the Web server's certificate cannot be verified against any known certificates. This is expected behavior, and it is safe to instruct the browser to accept the certificate. Once the certificate is accepted, all communications with the Web server through that browser will be secure.
6. If the device's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Confirm the connection to continue.

7. Log in to RUGGEDCOM WIN. For more information about logging in, refer to Section 2.2, “Logging In”.

Using an SSH Client

A Secure Shell (SSH) client provides access to the subscriber station's console interface.

To establish a connection using an SSH client, do the following:

1. Launch an SSH client and specify the following connection settings:

Host Name	The LAN IP address of the subscriber station or the LAN IP address prefixed with the desired user profile (e.g. admin@172.30.100.100)
Port	22

2. Connect to the subscriber station.
3. If the subscriber station's SSH key has not been cached to the workstation's registry, a confirmation message will appear asking if the host is trusted. Click **Yes** to continue. The login prompt appears.

```
login as:
```

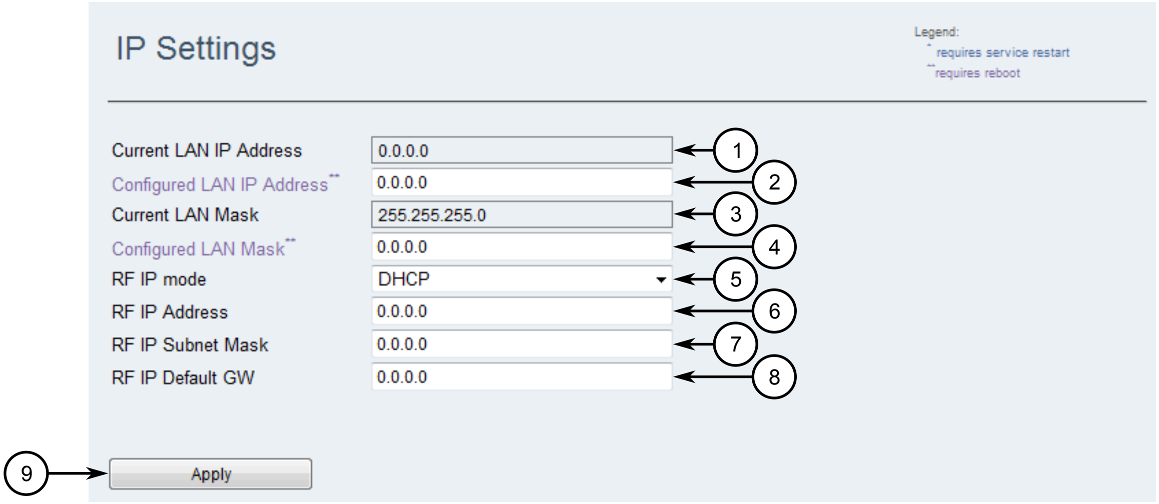
4. Log in to RUGGEDCOM WIN. For more information, refer to Section 2.2, “Logging In”.

Section 3.3

Configuring the Subscriber Station's IP Interface

To configure the subscriber station's IP address, subnet mask and/or default gateway IP address, do the following:

1. Navigate to ***Network » IP Settings » IP Settings***. The **IP Settings** screen appears.



IP Settings

Legend:
* requires service restart
** requires reboot

Current LAN IP Address: 0.0.0.0
Configured LAN IP Address**: 0.0.0.0
Current LAN Mask: 255.255.255.0
Configured LAN Mask**: 0.0.0.0
RF IP mode: DHCP
RF IP Address: 0.0.0.0
RF IP Subnet Mask: 0.0.0.0
RF IP Default GW: 0.0.0.0

Figure 7: IP Settings Screen

1. Current LAN IP Address **2.** Configure LAN IP Address Box **3.** Current LAN Mask **4.** Configured LAN Mask Box **5.** RF IP Mode List **6.** RF IP Address Box **7.** RF IP Subnet Mask Box **8.** RF IP Default GW Box **9.** Apply Button

2. Configure the following parameters as required:

Parameter	Description
Configured LAN IP Address	**Synopsis:** An IPv4 address **Default:** 192.168.254.251 The subscriber station's private IP address. The current IP address is setting is displayed under `Current LAN IP Address`.
Configured LAN Mask	**Synopsis:** An IPv4 address **Default:** 255.255.255.0 The associated private subnet. The current subnet address is setting is displayed under `Current LAN Mask` for the current subnet setting.
RF IP mode	**Synopsis:** { Static, DHCP } **Default:** DHCP The method in which the subscriber station's public IP address is obtained. Options include: • `Static` – The IP address is defined statically. Requires that `RF IP Address`, `RF IP Subnet Mask` and `RF IP Default GW` be configured. • `DHCP` – The IP address is assigned by a remote host using DHCP. **IMPORTANT!** *When the RF IP address is assigned by a DHCP server, the subscriber station does not release its IP address when the lease time is expired or update itself with a new IP address is allocated by the server. The subscriber station instead keeps the previous IP address.* *Using a pre-provisioned IP address is preferable as a pre-provisioned IP address does not require renewing. If not using a pre-provisioned IP, de-register the SS from the base station to get the new IP address configured at the DHCP server.*
RF IP Address	**Default:** 0.0.0.0 The subscriber station's public IP address. The address must be within the same subnet as the associated base station. Only configure this parameter if `RF IP Mode` is set to `Static`.
RF IP Subnet Mask	**Default:** 0.0.0.0 The associated public subnet. The subscriber station must be in the same subnet as the associated base station. Only configure this parameter if `RF IP Mode` is set to `Static`.
RF IP Default GW	**Default:** 0.0.0.0 The associated public default gateway. The subscriber station must use the same default gateway as the associated base station. Only configure this parameter if `RF IP Mode` is set to `Static`.

3. Click **Apply**.
4. If parameters marked with ** were configured, reboot the subscriber station. For more information, refer to Section 4.1, “Rebooting the Device”.

4 Device Management

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

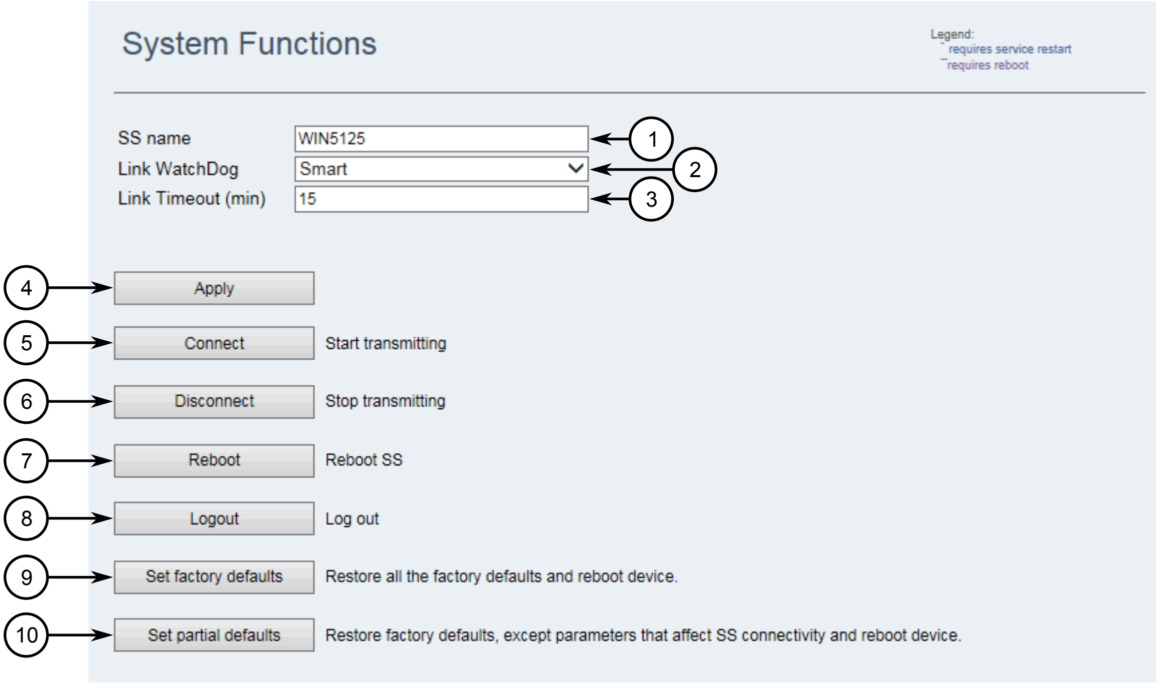
CONTENTS

Section 4.1

Rebooting the Device

To reboot the device, do the following:

1. Navigate to ***Management » System Functions***. The **System Functions** screen appears.



SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Connect: Start transmitting
Disconnect: Stop transmitting
Reboot: Reboot SS
Logout: Log out
Set factory defaults: Restore all the factory defaults and reboot device.
Set partial defaults: Restore factory defaults, except parameters that affect SS connectivity and reboot device.

Figure 8: System Functions Screen

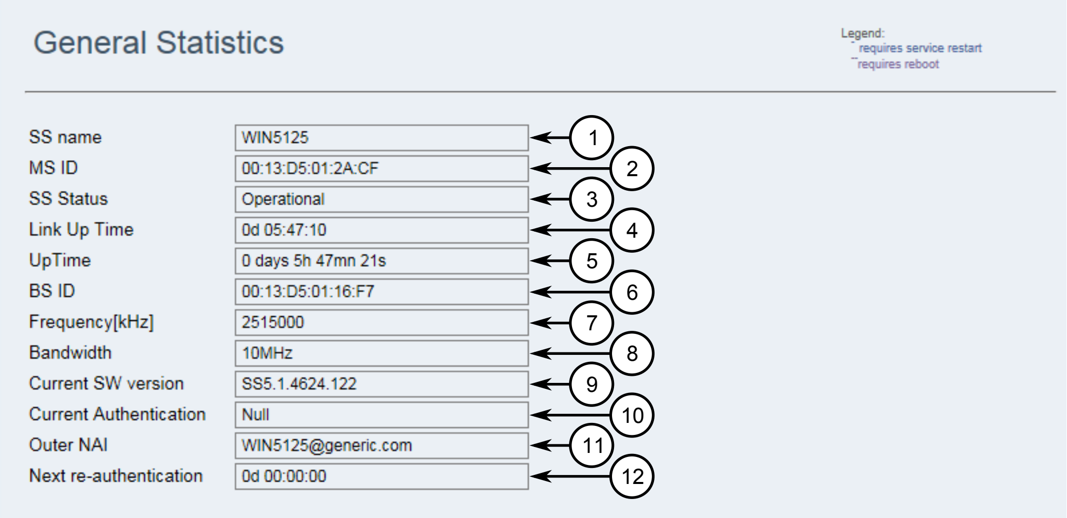
1. CPE Name Box **2.** Link Watchdog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Part Defaults Button

2. Click **Reboot**. The subscriber station starts to reboot.

Section 4.2

Displaying General Information

To display general information about the subscriber station, such as its current status, total up time, current software version, etc., navigate to ***Statistics » General » General Statistics***. The **General Statistics** screen appears.



General Statistics

Legend:
requires service restart
requires reboot

SS name	WIN5125
MS ID	00:13:D5:01:2A:CF
SS Status	Operational
Link Up Time	0d 05:47:10
UpTime	0 days 5h 47mn 21s
BS ID	00:13:D5:01:16:F7
Frequency[kHz]	2515000
Bandwidth	10MHz
Current SW version	SS5.1.4624.122
Current Authentication	Null
Outer NAI	WIN5125@generic.com
Next re-authentication	0d 00:00:00

Figure 9: General Statistics Screen

1. SS Name **2.** MS ID **3.** SS Status **4.** Link Up Time **5.** Up Time **6.** BS ID **7.** Frequency **8.** Bandwidth **9.** Current SW Version **10.** Current Authentication **11.** Outer NAI **12.** Next Re-Authentication

The parameters listed provide the following information:

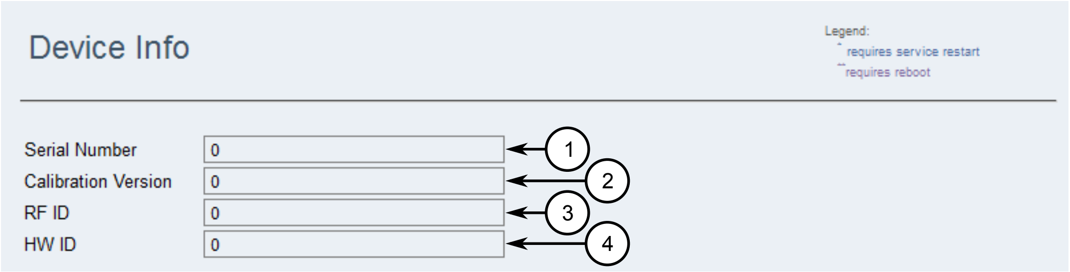
Parameter	Description
SS Name	The name of the subscriber station. The name identifies the subscriber station on the base station and in the base station management interface. For more information about setting the name, refer to Section 5.1, “Configuring the Device Name”.
MS ID	The mobile station MAC address.
SS Status	**Synopsis:** { Init, DL Synchronization, Handover DL acquisition, UL Acquisition, Ranging, Handover ranging, Capabilities negotiation, Authorization, Registration, DHCP, TOD, TFTP, Operational, Sleep, IDLE, Aborted } The subscriber station's current status. Possible values: `Init`, `DL Synchronization`, `Handover DL acquisition`, `UL Acquisition`, `Ranging`, `Handover ranging`, `Capabilities negotiation`, `Authorization`, `Registration` or `Operational`. >
Link Up Time	The time since the subscriber station became operational.
Up Time	The time since the subscriber station was powered on.
BS ID	The ID for the serving base station.
Frequency	The operating frequency in kilohertz (kHz).
Bandwidth	**Synopsis:** { 3.5MHz, 5MHz, 7MHz, 10MHz } The bandwidth setting.
Current SW version	The current version of RUGGEDCOM WIN installed.
Current Authentication	**Synopsis:** { Null, EAP-TTLS, EAP-TLS } The current authentication mode. Possible values: • `Null` – Authentication is disabled.

Parameter	Description
	• `EAP-TTLS` – EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) mode. • `EAP-TLS` – EAP-TTLS (Extensible Authentication Protocol - Transport Layer Security) mode.
Outer NAI	The outer Network Access Identifier (NAI).
Next re-authentication	The time remaining until the next re-authentication.

Section 4.3

Displaying Device Information

To view information about the subscriber station, such as the current boot version, hardware version etc., navigate to ***Statistics » General » Device Info***. The **Device Info** screen appears.



Device Info

Legend:
* requires service restart
** requires reboot

Serial Number: 0
Calibration Version: 0
RF ID: 0
HW ID: 0

Figure 10: Device Info Screen

1. Serial Number **2.** Calibration Version **3.** RF ID **4.** Hardware ID

The following information is displayed:

Parameter	Description
Serial Number	The serial number for the subscriber station.
Calibration Version	The version of the subscriber station calibration.
RF ID	The subscriber stations's radio frequency identification number.
HW ID	The subscriber station's hardware identification number.

Section 4.4

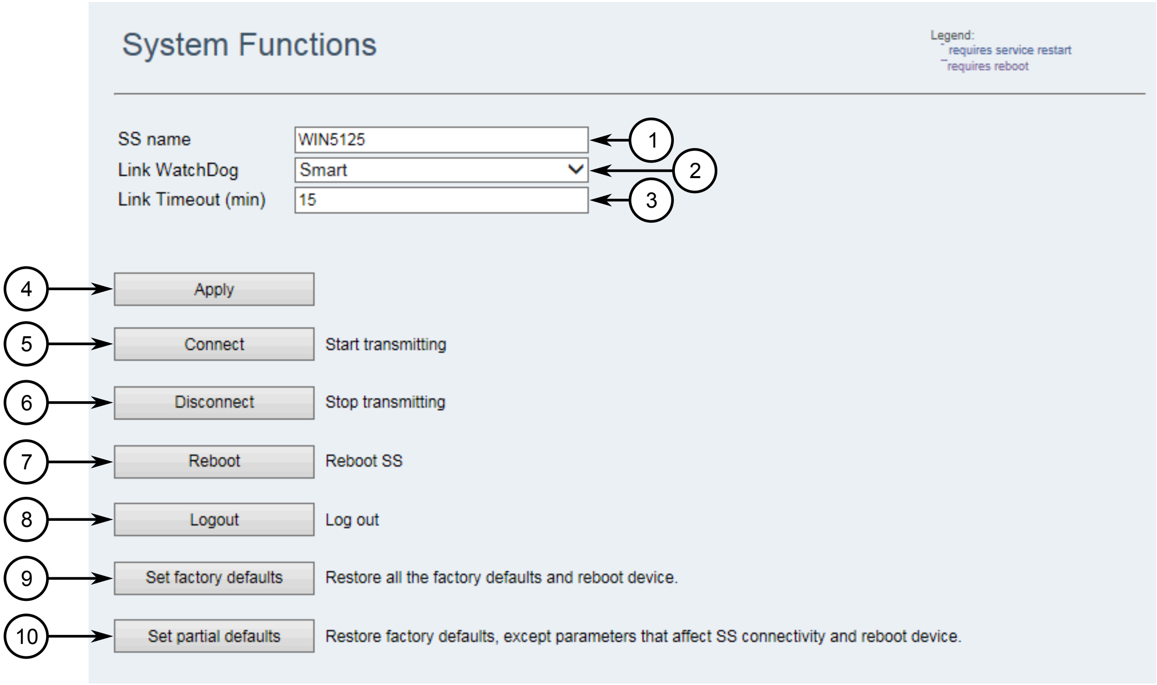
Configuring Link WatchDog

Link WatchDog reboots the subscriber station automatically if it is not in an operational state for a specific period of time.

NOTE
The timeout period is reset when the transmission is being restarted.

To configure Link WatchDog, do the following:

1. Navigate to ***Management » System Functions***. The **System Functions** screen appears.



System Functions

Legend:
requires service restart
requires reboot

SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Apply
Connect — Start transmitting
Disconnect — Stop transmitting
Reboot — Reboot SS
Logout — Log out
Set factory defaults — Restore all the factory defaults and reboot device.
Set partial defaults — Restore factory defaults, except parameters that affect SS connectivity and reboot device.

Figure 11: System Functions Screen

1. CPE Name Box **2.** Link Watchdog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Part Defaults Button

2. Configure the following parameters:

Parameter	Description
Link WatchDog	**Synopsis:** { Disabled, Smart, Always } **Default:** Smart Link WatchDog's operating state. Options include: • `Disabled` – Link WatchDog is disabled • `Smart` – Link WatchDog reboots the subscriber station when the timeout period expires unless transmissions have been stopped or when the Scanner Table is empty. • `Always` – Link WatchDog reboots the subscriber station when the timeout period expires if no RF link has been established
Link Timeout	**Synopsis:** An integer between 1 and 15 **Default:** 15 The time in minutes (min) before Link WatchDog reboots the device.

3. Click **Apply**.

Section 4.5

Viewing Statistics

RUGGEDCOM WIN records statistics on all uplink and downlink communications, including UL and DL signal strengths and carrier to interference plus noise ratios. Packet counters list UL and DL channels, bytes and packets transmitted and dropped, and packet rates.

This section describes how to view and control the statistics collected.

CONTENTS

Section 4.5.1

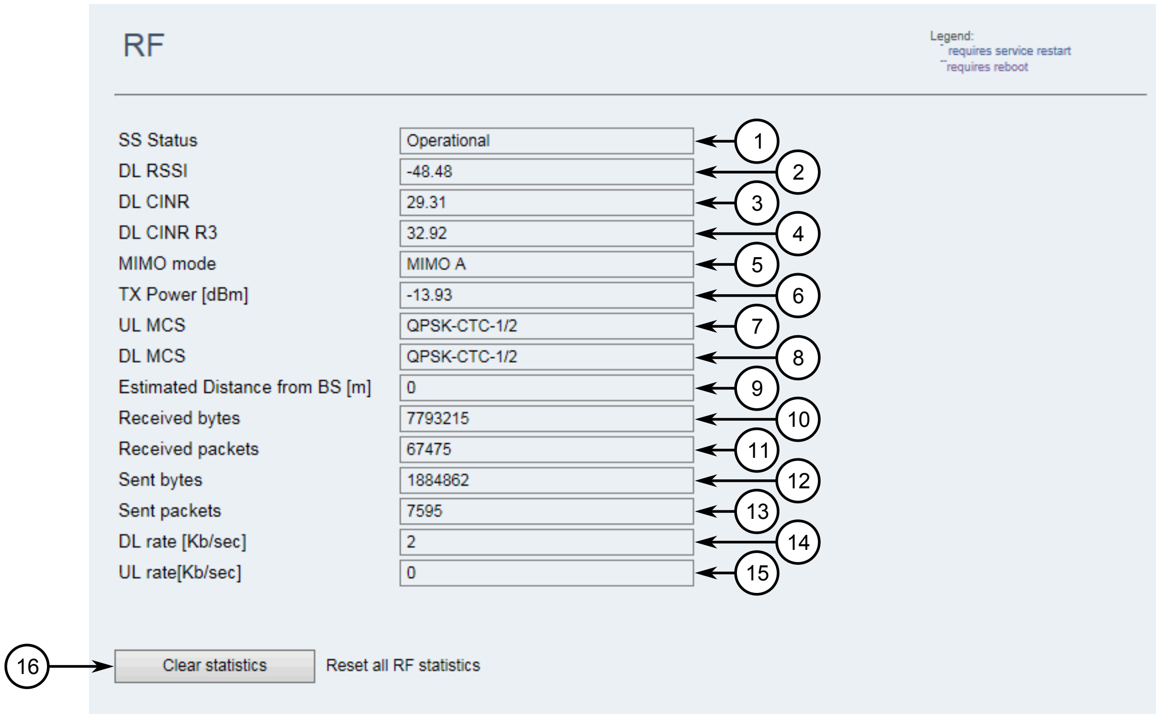
Viewing and Clearing RF Statistics

RUGGEDCOM WIN actively records statistics on the RF network.

To view and clear RF statistics, do the following:

›› Viewing the RF Statistics

To view the current Ethernet statistics, navigate to ***Statistics » RF » RF***. The **RF** screen appears.



RF

Legend:
requires service restart
requires reboot

SS Status	Operational
DL RSSI	-48.48
DL CINR	29.31
DL CINR R3	32.92
MIMO mode	MIMO A
TX Power [dBm]	-13.93
UL MCS	QPSK-CTC-1/2
DL MCS	QPSK-CTC-1/2
Estimated Distance from BS [m]	0
Received bytes	7793215
Received packets	67475
Sent bytes	1884862
Sent packets	7595
DL rate [Kb/sec]	2
UL rate[Kb/sec]	0

Figure 12: RF Screen

1. SS Status **2.** DL RSSI **3.** DL CINR **4.** DL CINR R3 **5.** MIMO Mode **6.** TX Power **7.** UL MCS **8.** DL MCS **9.** Estimated Distance from BS **10.** Received Bytes **11.** Received Packets **12.** Sent Bytes **13.** Sent Packets **14.** DL Rate **15.** UL Rate **16.** Clear Statistics

The parameters listed provide the following information:

Parameter	Description
SS Status	**Synopsis:** { Init, DL Synchronization, Handover DL acquisition, UL Acquisition, Ranging, Handover ranging, Capabilities negotiation, Authorization, Registration, DHCP, TOD, TFTP, Operational, Sleep, IDLE, Aborted } The subscriber station's current status. Possible values: `Init`, `DL Synchronization`, `Handover DL acquisition`, `UL Acquisition`, `Ranging`, `Handover ranging`, `Capabilities negotiation`, `Authorization`, `Registration` or `Operational`.
DL RSSI	The downlink received signal strength in decibels per minute (dBm).
DL CINR	The downlink carrier to interference and noise ratio in decibels (dB).
DL CINR R3	Displays Displays R3 downlink carrier to interference and noise ratio in decibels (dB).
MIMO mode	**Synopsis:** {SISO, MIMO A, MIMO B} The SS Multiple-Input, Multiple-Output mode.
TX Power [dBm]	The SS transmission power, in dBm.
UL MCS	**Synopsis:** { N/A, 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 Modulation and Coding Scheme (MCS) index value for uplink communications. For a details about each available option, refer to Section 1.7, "Supported Modulation Techniques".
DL MCS	**Synopsis:** {N/A, 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}

Parameter	Description
	The Modulation and Coding Scheme (MCS) index value for downlink communications. For a details about each available option, refer to Section 1.7, "Supported Modulation Techniques".
Estimated Distance from BS	The estimated distance in meters (m) from the subscriber station to the serving base station.
Received Bytes	The amount of data received by the subscriber station in bytes.
Received Packets	The number of packets received by the subscriber station.
Sent Bytes	Displays amount of data sent by the subscriber station in bytes.
Sent Packets	The number of packets sent by the subscriber station.
DL Rate	The downlink rate in kilobits per second (Kb/s).
UL Rate	The uplink rate in kilobits per second (Kb/s).

Clearing RF Statistics

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

Section 4.5.2

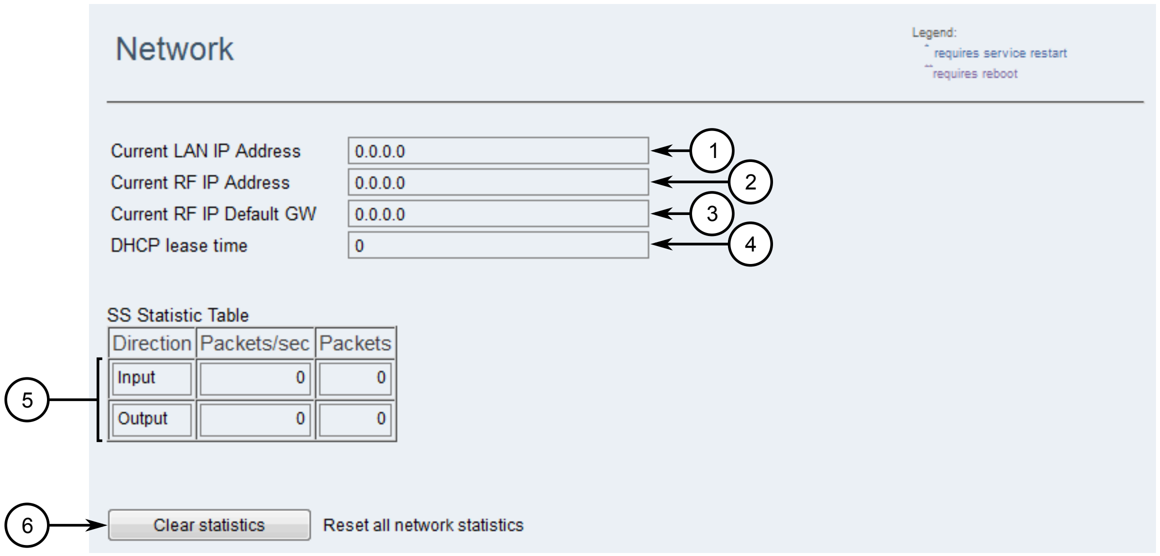
Viewing and Clearing Network Statistics

RUGGEDCOM WIN actively records statistics related to network traffic, including the number of packets sents/ received and at what rate.

Viewing the Network Statistics

To view the current network statistics, navigate to ***Statistics » Network » Network***. The **Network** screen appears.

> **NOTE**
> *The **Network** screen also displays the current IP address settings. For more information, refer to Section 5.5, "Displaying the Current IP Address Settings".*



Network

Legend:
* requires service restart
** requires reboot

Current LAN IP Address: 0.0.0.0
Current RF IP Address: 0.0.0.0
Current RF IP Default GW: 0.0.0.0
DHCP lease time: 0

SS Statistic Table

Direction	Packets/sec	Packets
Input	0	0
Output	0	0

Figure 13: Network Screen

1. Current LAN IP Address **2.** Current RF IP Address **3.** RF IP Default GW **4.** DHCP Lease Time **5.** SS Statistics **6.** Clear Statistics Button

The **SS Statistics Table** provides the following information:

Parameter	Description
Direction	**Synopsis:** { Input, Output } The traffic direction.
Packets/Sec	The traffic flow rate in packets per second (packets/s).
Packets	The total number of packets processed.

Clearing Network Statistics

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

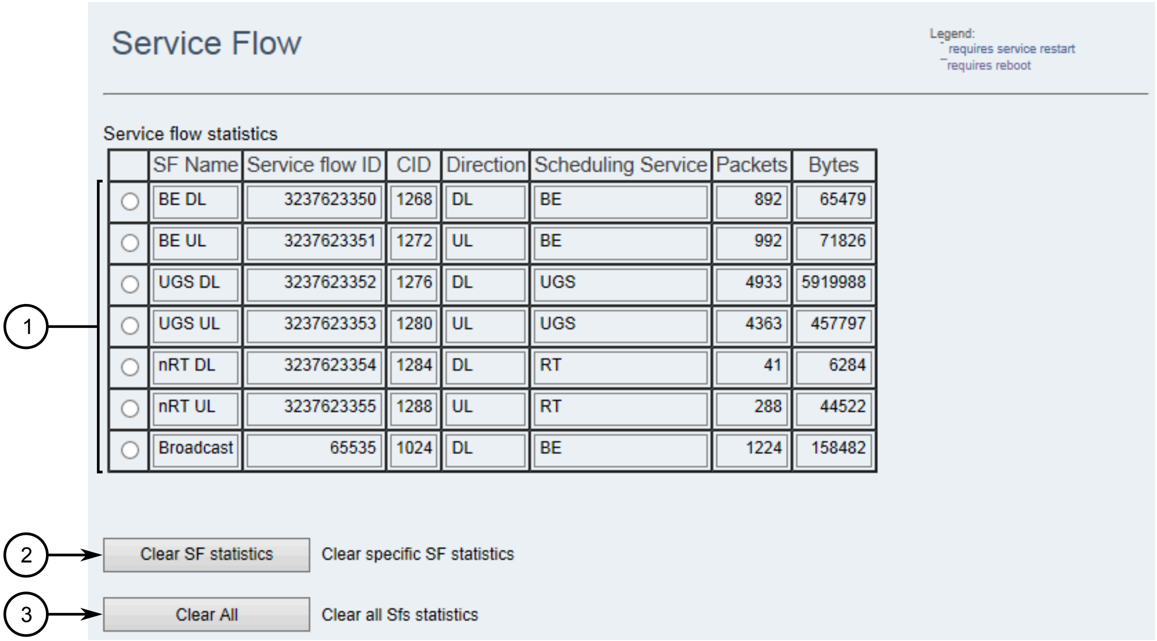
Section 4.5.3

Viewing and Clearing Service Flow Statistics

RUGGEDCOM WIN actively records statistics related to service flows, such as the CID, direction, scheduling service, etc.

Viewing the Service Flow Statistics

To view the current service flow statistics, navigate to ***Statistics » Service Flow » Service Flow***. The **Service Flow** screen appears.



Service flow statistics

	SF Name	Service flow ID	CID	Direction	Scheduling Service	Packets	Bytes
○	BE DL	3237623350	1268	DL	BE	892	65479
○	BE UL	3237623351	1272	UL	BE	992	71826
○	UGS DL	3237623352	1276	DL	UGS	4933	5919988
○	UGS UL	3237623353	1280	UL	UGS	4363	457797
○	nRT DL	3237623354	1284	DL	RT	41	6284
○	nRT UL	3237623355	1288	UL	RT	288	44522
○	Broadcast	65535	1024	DL	BE	1224	158482

Clear specific SF statistics

Clear all Sfs statistics

Figure 14: Service Flow Screen

1. Service Flow Statistics **2.** Clear SF Statistics **3.** Clear All Statistics

Service Flow Statistics

The **Service Flow Statistics** table provides the following statistics:

Parameter	Description
SF Name	The name of the service flow.
Service flow ID	Displays a numeric identifier for the service flow.
CID	The connection identifier for the service flow.
Direction	**Synopsis:** { DL, UL } The direction for the service flow. Possible values: • `UL` – Uplink • `DL` – Downlink
Scheduling Service	**Synopsis:** { BE, nRT, RT, eRT, UGS } The scheduling service for the service flow. Possible values: • `BE` – Best Effort • `nRT` – Near-Real Time • `RT` – Real Time • `eRT` – Extended Real Time • `UGS` – Unsolicited Grant Service
Packets	The number of packets handled by the service flow.
Bytes	The number of bytes handled by the service flow.

Clearing Statistics

To clear the current statistics, either click **Clear All** or select specific rows and then click **Clear SF Statistics**.

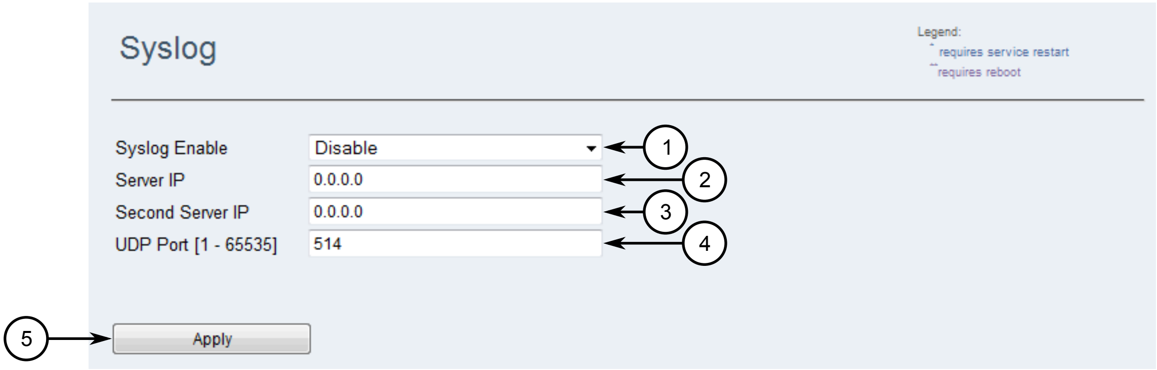
Section 4.6

Configuring Syslog

For redundancy, RUGGEDCOM WIN supports up to two remote Syslog server connections. The server defined under **Server IP** is considered the primary Syslog server. The server defined under **Second Server IP** is the secondary server. Should the connection with the primary server be lost, the Syslog service will automatically switch to the secondary server.

To configure the System log (Syslog), do the following:

1. Navigate to ***Management » Log Management***. The **Syslog** screen appears.



Syslog

Legend:
* requires service restart
** requires reboot

Syslog Enable: Disable
Server IP: 0.0.0.0
Second Server IP: 0.0.0.0
UDP Port [1 - 65535]: 514

Figure 15: Syslog Screen

1. Syslog Enable List **2.** Server IP Box **3.** Second Server IP **4.** UDP Port Box **5.** Apply Button

2. Under **Syslog Enable**, select `Enable` to enable the Syslog service.
3. Configure the following parameters:

Parameter	Description
Server IP	**Synopsis:** IPv4 Address **Default:** 0.0.0.0 The IP address for the primary Syslog server.
Secondary Server IP	**Synopsis:** IPv4 Address **Default:** 0.0.0.0 The IP address for the secondary Syslog server.
UDP Port	**Synopsis:** An integer between 1 and 65535 **Default:** 514 The UDP port on the primary and second syslog servers to use when uploading log files.

4. Click **Apply**.

Section 4.7

Managing System Files

This section describes how to upload, download and copy system files on the device. System files include:

File Type	Example	Description
Blob	microcode.blob.Z	Firmware for the WiMAX modem.
Web Resource	web.rc	The Web user interface configuration file.
Defaults	SS-Def.xml	The default configuration file.
UV	SS-Val-Unique.xml	The custom configuration file.
GUI	SS-Gui.xml	The GUI configuration file.

CONTENTS

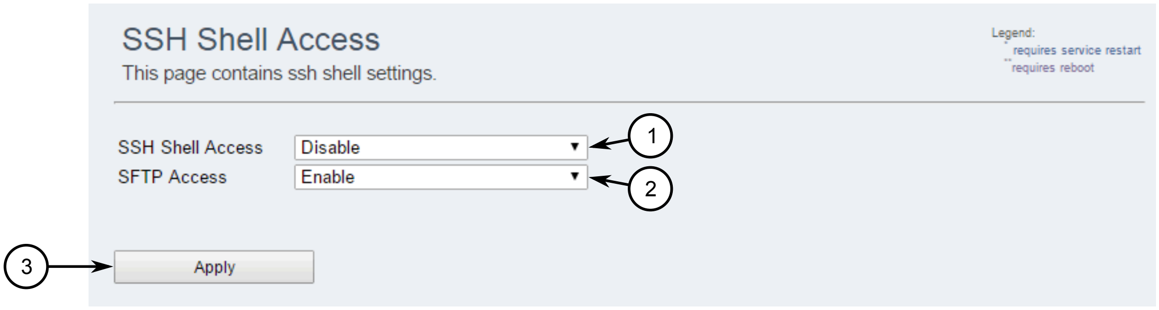
Section 4.7.1

Enabling/Disabling SFTP Sessions

Enabling SFTP sessions allows users to manage files on the subscriber station remotely using the Secure File Transfer Protocol (SFTP).

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

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



SSH Shell Access

This page contains ssh shell settings.

Legend:
* requires service restart
** requires reboot

SSH Shell Access: Disable
SFTP Access: Enable

Figure 16: SSH Shell Access Screen

1. SSH Shell Access List **2.** SFTP Access List **3.** Apply Button

2. Configure the following parameter:

Parameter	Description
SFTP Access	**Synopsis:** { Enable, Disable } **Default:** Enable Enables or disables file management via SFTP.

3. Click **Apply**.

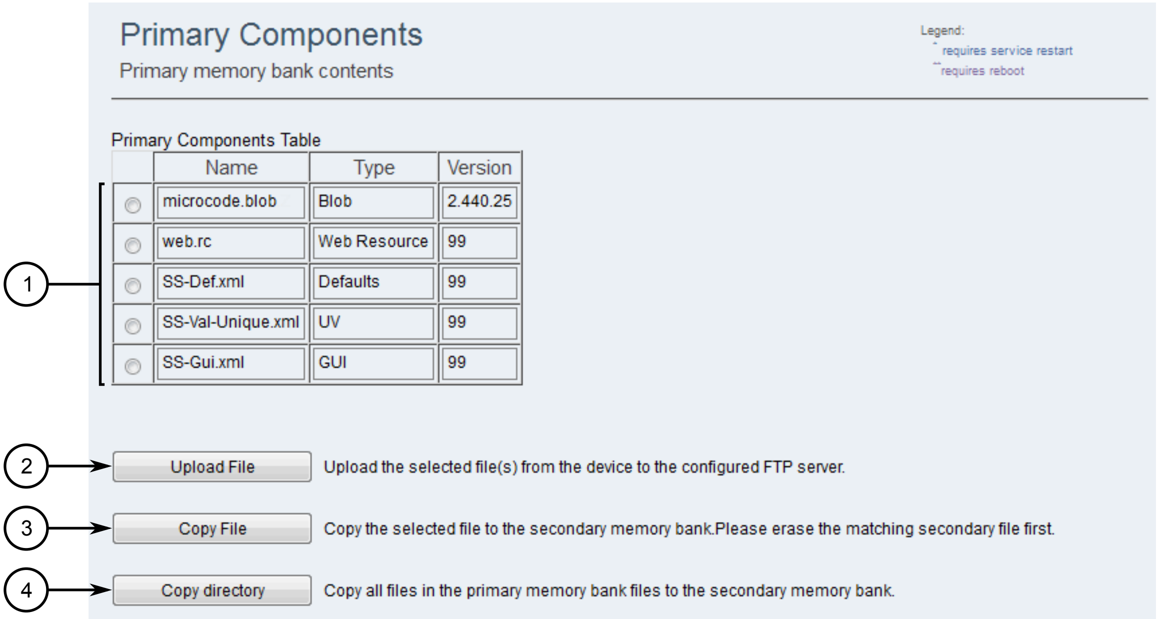
Section 4.7.2

Uploading Files to the FTP Server

To upload files from the *primary* or *secondary* memory banks to the FTP server, do the following:

1. Navigate to ***Management » SW Upgrade » Primary Bank or Secondary Bank***. The **Primary Components** or **Secondary Components** screen appears.

> **NOTE**
> *Files are only available on the **Secondary Components** screen if a software version has been downloaded to the **secondary** memory bank.*



Primary Components

Primary memory bank contents

Legend:
* requires service restart
** requires reboot

Primary Components Table

	Name	Type	Version
○	microcode.blob	Blob	2.440.25
○	web.rc	Web Resource	99
○	SS-Def.xml	Defaults	99
○	SS-Val-Unique.xml	UV	99
○	SS-Gui.xml	GUI	99

Upload the selected file(s) from the device to the configured FTP server.

Copy the selected file to the secondary memory bank.Please erase the matching secondary file first.

Copy all files in the primary memory bank files to the secondary memory bank.

Figure 17: Primary Components Screen (Example)

1. Available Files **2.** Upload File Button **3.** Copy File Button **4.** Copy Directory Button

> **NOTE**
> *File transfers can be viewed and, if needed, cancelled under **Management » SW Upgrade » Files Status**. For more information, refer to Section 4.7.6, "Viewing/Cancelling File Transfers".*

2. Select one or more files and then click **Upload File**. The selected file(s) is uploaded to the FTP server. The location on the FTP server is defined under ***Management » SW Upgrade » SW Download***.

Section 4.7.3

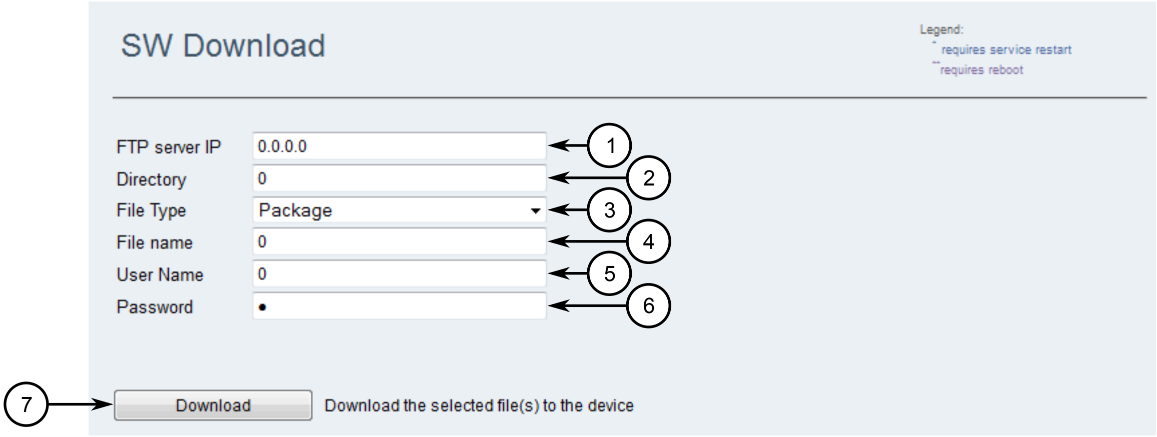
Downloading a File from the FTP Server

To download a file from the FTP server, do the following:

> **NOTE**
> *All files downloaded from the FTP server are saved on the* ***secondary*** *memory bank so as to protect the current running configuration.*

> **NOTE**
> *RUGGEDCOM NMS can be configured to download files from the FTP server to the subscriber station at a specific time and date. For more information, refer to the RUGGEDCOM NMS User Guide.*

1. Navigate to ***Management » SW Upgrade » SW Download***. The **SW Download** screen appears.



SW Download

Legend:
* requires service restart
** requires reboot

FTP server IP: 0.0.0.0
Directory: 0
File Type: Package
File name: 0
User Name: 0
Password: •

Download — Download the selected file(s) to the device

Figure 18: SW Download Screen

1. FTP Server IP Box **2.** Directory **3.** File Type List **4.** File Name Box **5.** User Name Box **6.** Password Box **7.** Download Button

2. Under **File Type**, select the type of file to be downloaded from the FTP server. Options include: `Package`, `VxWorks`, `Web Resource`, `CDC` and `UV`.
3. Under **File Name**, enter the full name of the file to download.

> **NOTE**
> *File transfers can be viewed and, if needed, cancelled under* ***Management » SW Upgrade » Files Status****. For more information, refer to Section 4.7.6, "Viewing/Cancelling File Transfers".*

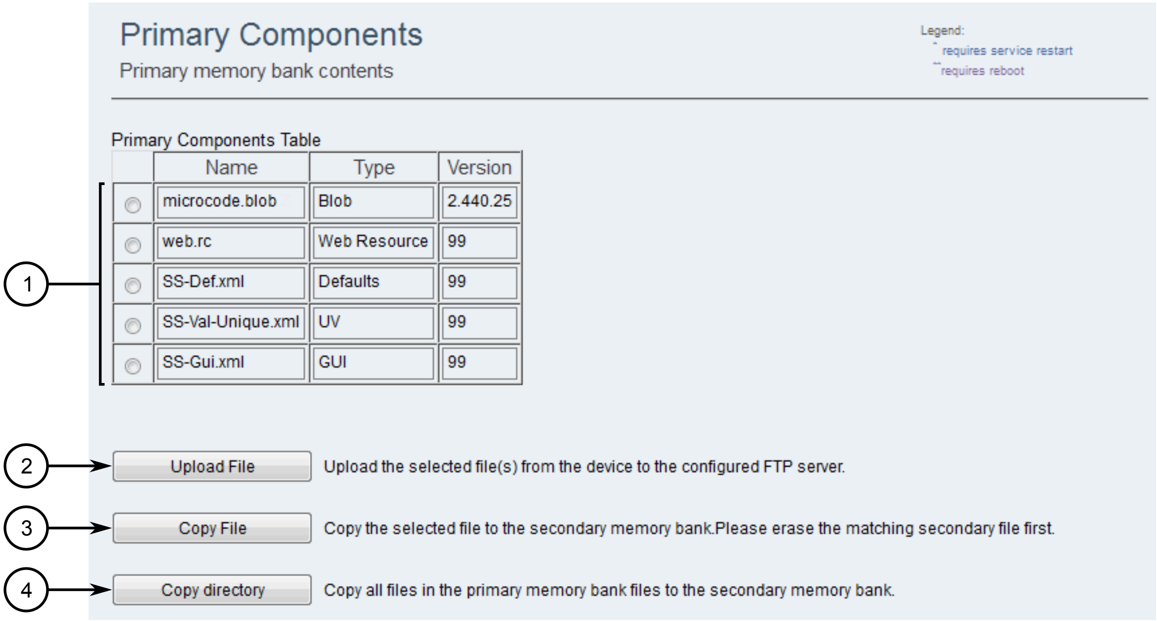
4. Click **Download**. The file is downloaded to the secondary memory bank.

Section 4.7.4

Copying Files from the Primary Memory Bank to the Secondary Memory Bank

To copy files from the *primary* memory bank to the *secondary* memory bank, do the following:

1. Make sure the desired file(s) does not already exist in the *secondary* memory bank. For information about deleting files from the *secondary* memory bank, refer to Section 4.7.5, "Deleting Files from the Secondary Memory Bank".
2. Navigate to ***Management » SW Upgrade » Primary Bank***. The **Primary Components** screen appears.



Primary Components
Primary memory bank contents

Legend:
* requires service restart
** requires reboot

Primary Components Table

	Name	Type	Version
○	microcode.blob	Blob	2.440.25
○	web.rc	Web Resource	99
○	SS-Def.xml	Defaults	99
○	SS-Val-Unique.xml	UV	99
○	SS-Gui.xml	GUI	99

Upload File — Upload the selected file(s) from the device to the configured FTP server.

Copy File — Copy the selected file to the secondary memory bank.Please erase the matching secondary file first.

Copy directory — Copy all files in the primary memory bank files to the secondary memory bank.

Figure 19: Primary Components Screen

1. Available Files **2.** Upload File Button **3.** Copy File Button **4.** Copy Directory Button

> **NOTE**
> *File transfers can be viewed and, if needed, cancelled under **Management » SW Upgrade » Files Status**. For more information, refer to Section 4.7.6, "Viewing/Cancelling File Transfers".*

3. Select one or more files and then click **Copy File**. The selected file(s) is copied to the *secondary* memory bank.

   Alternatively, click **Copy Directory** to copy all files to the *secondary* memory bank.

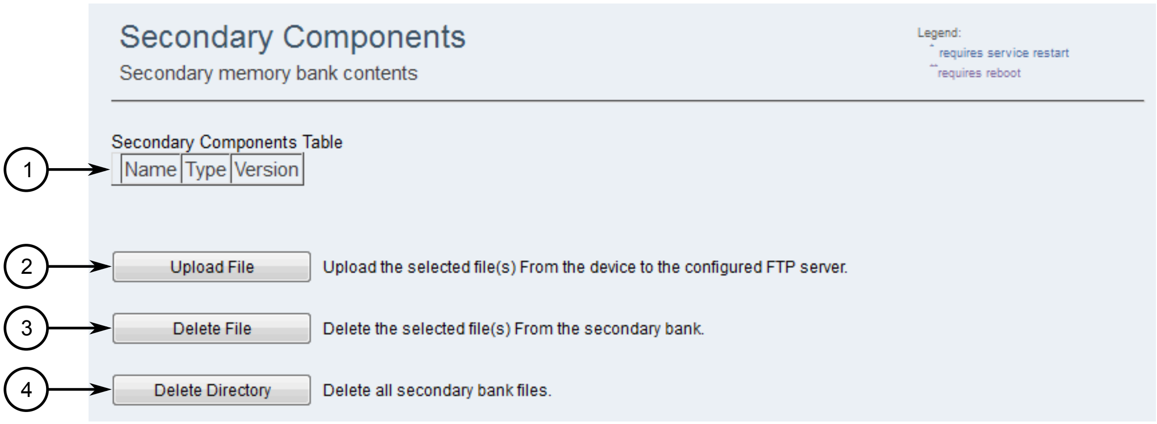
Section 4.7.5

Deleting Files from the Secondary Memory Bank

Files on the *secondary* memory bank must be deleted before files with the same name are copied from the *primary* memory bank.

To delete files from the *secondary* memory bank, do the following:

1. Navigate to ***Management » SW Upgrade » Secondary Bank***. The **Secondary Components** screen appears.



Secondary Components

Secondary memory bank contents

Legend:
* requires service restart
** requires reboot

Secondary Components Table

Name	Type	Version

Upload the selected file(s) From the device to the configured FTP server.

Delete the selected file(s) From the secondary bank.

Delete all secondary bank files.

Figure 20: Secondary Components Screen

1. Available Files **2.** Upload File Button **3.** Delete File Button **4.** Delete Directory Button

2. Select one or more files and then click **Delete File**. The selected file(s) is deleted from the *secondary* memory bank.

   Alternatively, click **Delete Directory** to delete all files from the *secondary* memory bank.

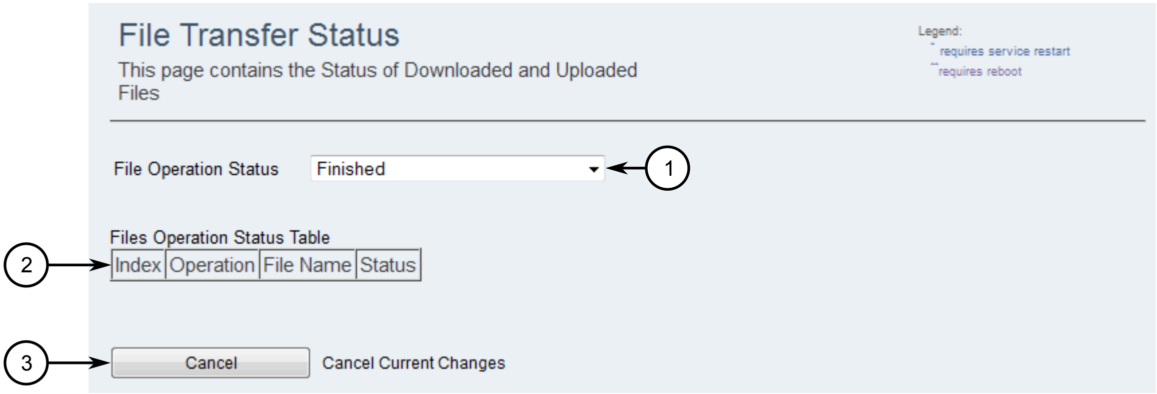
Section 4.7.6

Viewing/Cancelling File Transfers

To view active file transfers and optionally cancel them, do the following:

›› Viewing File Transfers

1. Navigate to ***Management » SW Upgrade » Files Status***. The **File Transfer Status** screen appears.



File Transfer Status

This page contains the Status of Downloaded and Uploaded Files

Legend:
* requires service restart
** requires reboot

File Operation Status Finished

Files Operation Status Table

Index	Operation	File Name	Status

Cancel Current Changes

Figure 21: File Transfer Status Screen

1. File Operation Status List **2.** List of Files **3.** Cancel Button

2. Under **File Operation Status**, select an operation state. Any files that match that state appear in the table below. Options include:
    - `Finished` – Displays all files that were successfully downloaded
    - `Not Started` – Displays all files that are waiting to be downloaded
    - `In Process` – Displays all files that are currently being downloaded
    - `Failure` – Displays all files that were not successfully downloaded

›› Cancelling a File Transfer

1. Under **File Operation Status**, select **In Process**. All files that are currently being downloaded appear in the table below.
2. Select one or more files and then click **Cancel**. A confirmation message appears.
3. Click **OK**. The selected file transfers are stopped.

Section 4.8

Managing Software

This section describes how to manage the verson of RUGGEDCOM WIN running on the subscriber station.

CONTENTS

Section 4.8.1

Updating RUGGEDCOM WIN

To upgrade the version of RUGGEDCOM WIN installed on the device, do the following:

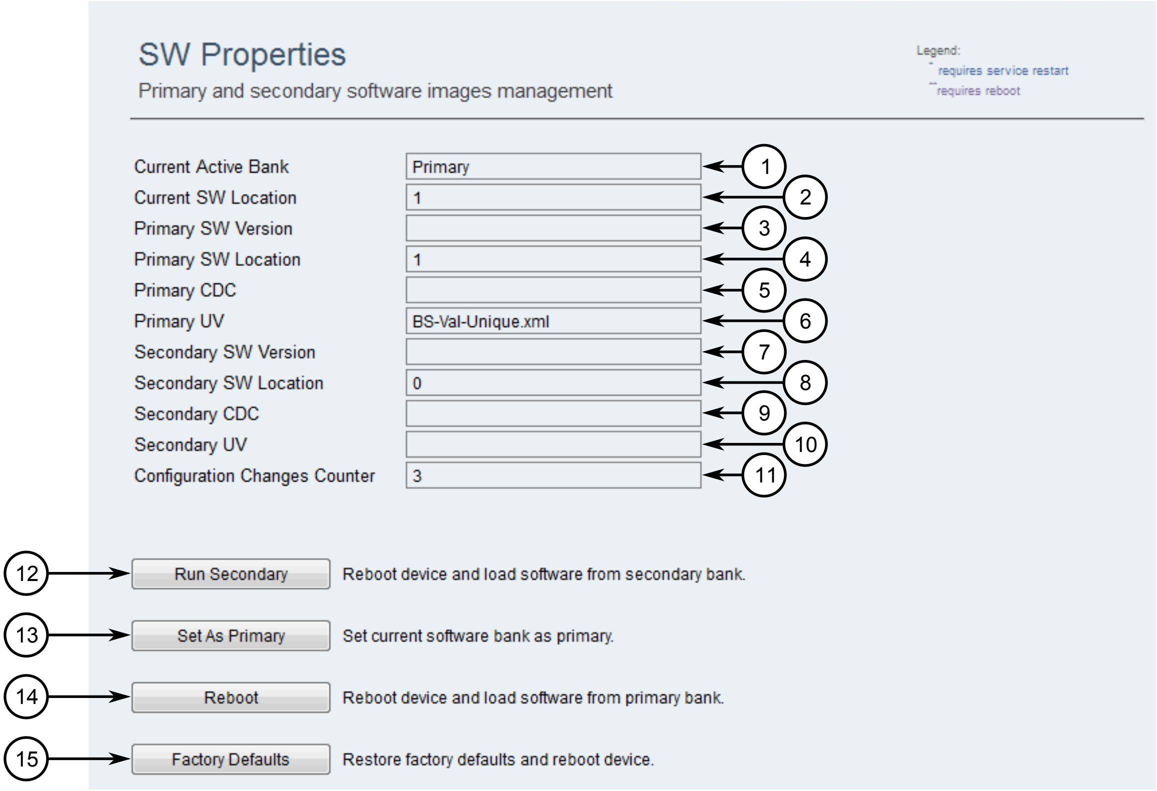
1. Establish a server that supports secure FTP (File Transfer Protocol) file transfers.
2. Submit a Support Request via Siemens Industry Online Support [https://support.industry.siemens.com]. Information will be provided by Siemens Customer Support on how to download the requested software package.
3. Download the software package to the FTP server.
4. Download the software package from the FTP server to the *secondary* memory bank. For more information, refer to Section 4.7.3, “Downloading a File from the FTP Server”.
5. Promote the *secondary* memory bank to the primary memory bank. For more information, refer to Section 4.8.2, “Changing the Active Software Version”.

Section 4.8.2

Changing the Active Software Version

To change version of RUGGEDCOM WIN is currently running on the subscriber station, do the following:

1. Navigate to ***Management » SW Upgrade***. The **SW Properties** screen appears.



SW Properties

Primary and secondary software images management

Legend:
* requires service restart
** requires reboot

Current Active Bank	Primary
Current SW Location	1
Primary SW Version	
Primary SW Location	1
Primary CDC	
Primary UV	BS-Val-Unique.xml
Secondary SW Version	
Secondary SW Location	0
Secondary CDC	
Secondary UV	
Configuration Changes Counter	3

Reboot device and load software from secondary bank.

Set current software bank as primary.

Reboot device and load software from primary bank.

Restore factory defaults and reboot device.

Figure 22: SW Properties Screen

1. Current Active Bank **2.** Current SW Location **3.** Primary SW Version **4.** Primary SW Location **5.** Primary CDC **6.** Primary UV **7.** Secondary SW Version **8.** Secondary SW Location **9.** Secondary CDC **10.** Secondary UV **11.** Configuraton Changes Counter **12.** Run Secondary Button **13.** Set As Primary Button **14.** Reboot Button **15.** Factory Defaults Button

2. Click **Run Secondary**. The device reboots with the *secondary* memory bank loaded.
3. Click **Set As Primary**. The current memory bank is now the *primary* memory bank. When the subscriber station reboots, this memory bank will be loaded automatically.

Section 4.8.3

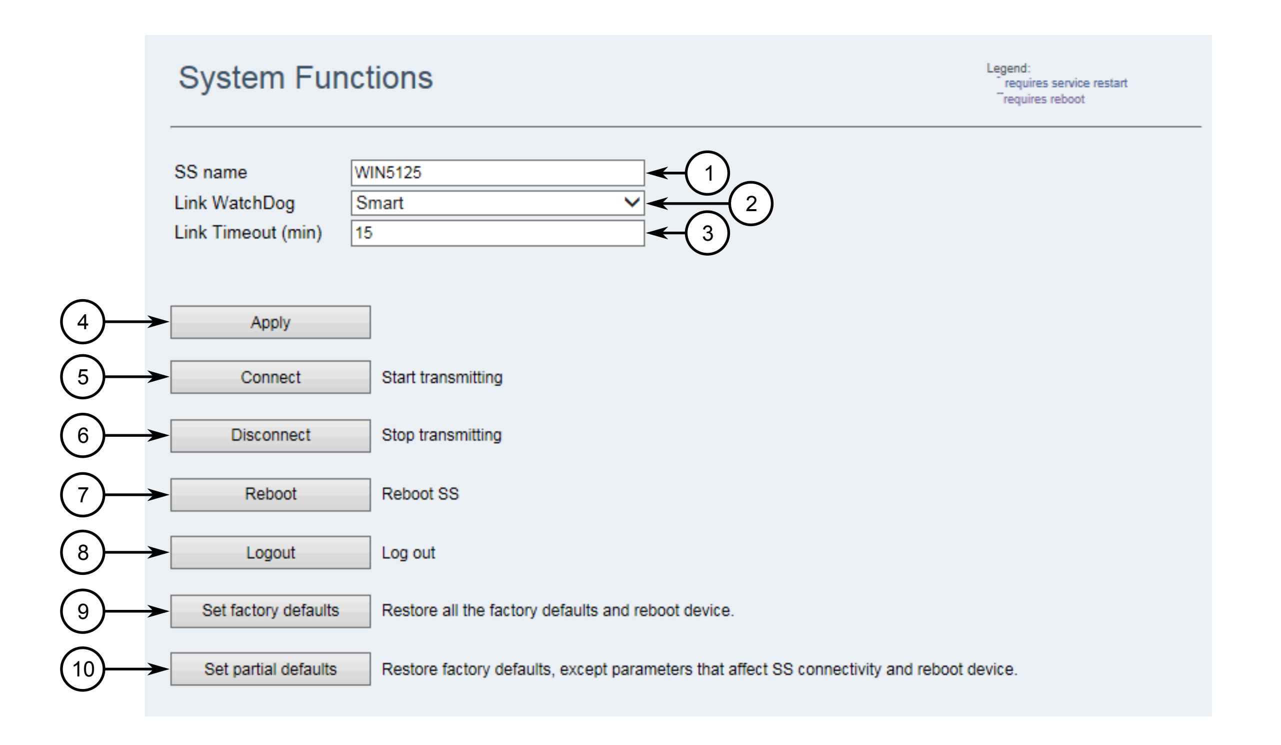
Restoring Factory Defaults

Settings for RUGGEDCOM WIN can be fully or partially set back to the original factory defaults. A partial reset restores all factory defaults except those that affect the device's connection to the network.

NOTE
The device is rebooted following each factory reset.

To restore factory defaults, do the following:

1. Navigate to ***Management » System Functions***. The **System Functions** screen appears.



System Functions

Legend:
requires service restart
requires reboot

SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Apply
Connect — Start transmitting
Disconnect — Stop transmitting
Reboot — Reboot SS
Logout — Log out
Set factory defaults — Restore all the factory defaults and reboot device.
Set partial defaults — Restore factory defaults, except parameters that affect SS connectivity and reboot device.

Figure 23: System Functions Screen

1. CPE Name Box **2.** Link Watchdog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Part Defaults Button

2. Click either **Set factory defaults** to restore all factory defaults or **Set partial defaults** to restore only factory defaults not related to connectivity. A confirmation message appears.
3. Click **Ok**. Factory defaults are restored (fully or partially) and the device is rebooted.

Section 4.9

Configuring the Maximum Transmission Unit (MTU)

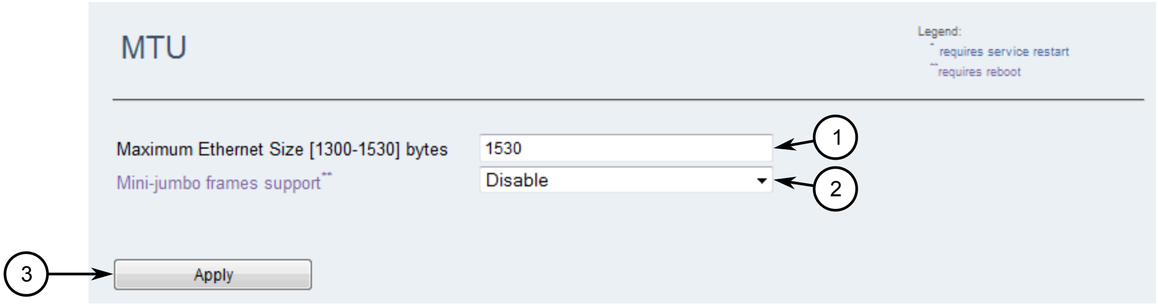
The Maximum Transmission Unit (MTU) specifies the size of the largest network layer protocol data unit that can traverse the base station in a single network transaction. The MTU value includes the Layer 2 header and Cyclic Redundancy Check (CRC).

The maximum size of a data unit is 1530 bytes. However, with mini-jumbo frames enabled, the maximum size is increased to 1599 bytes.

IMPORTANT!
When jumbo frames are enabled, the whole network must have the same MTU setting.

To configure the MTU, do the following:

1. Navigate to ***Network » Ethernet Settings » MTU***. The **MTU** screen appears.



MTU

Legend:
* requires service restart
** requires reboot

Maximum Ethernet Size [1300-1530] bytes: 1530
Mini-jumbo frames support**: Disable

Figure 24: MTU screen

1. Maximum Ethernet Size Box **2.** Mini-Jumbo Frames Support List **3.** Apply Button

2. Under **Mini-Jumbo Frames Support**, select `Enable` to enable mini-jumbo frames, or `Disable` to disable mini-jumbo frames.
3. Under **Maximum Ethernet Size**, enter the maximum MTU size in bytes.
4. Click **Apply**.
5. If **Mini-Jumbo Frames Support** was set to `Enabled`, reboot the base stattion.

Section 4.10

Configuring the Device as a Backhaul Subscriber Station

A backhaul subscriber station acts as a proxy for hosts on the LAN side of the station that require access to the serving base station. The host can be a AAA, DHCP or RUGGEDCOM NMS server.

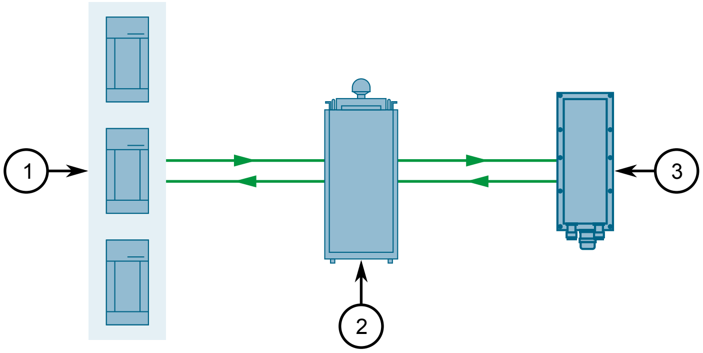


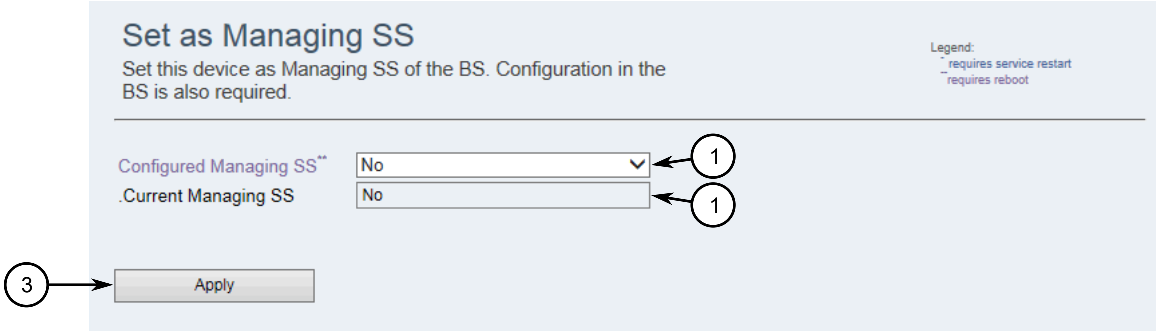
Figure 25: Device as a Backhaul Subscriber Station

1. Host **2.** Subscriber Station **3.** Base Station

IMPORTANT!
The base station must be configured to be managed by a backhaul subscriber station.

To configure the device as a backhaul subscriber station, do the following:

1. Make sure the serving base station is configured to be managed by a backhaul subscriber station. For more information, refer to the *RUGGEDCOM WIN User Guide* for the base station.
2. Navigate to ***Management » System Functions » Managing SS***. The **Set as Managing CPE** screen appears.



Set as Managing SS

Set this device as Managing SS of the BS. Configuration in the BS is also required.

Legend:
* requires service restart
** requires reboot

Configured Managing SS**: No
.Current Managing SS: No

Figure 26: Set as Managing CPE Screen

1. Configured Managing SS List **2.** Current Managing SS **3.** Apply Button

3. Under **Configured Managing SS**, select **Yes**. The current state is displayed under **Current Managing SS**.
4. Click **Apply** and then reboot the subscribe station.

Section 4.11

Managing GPS

The subscriber 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.

CONTENTS

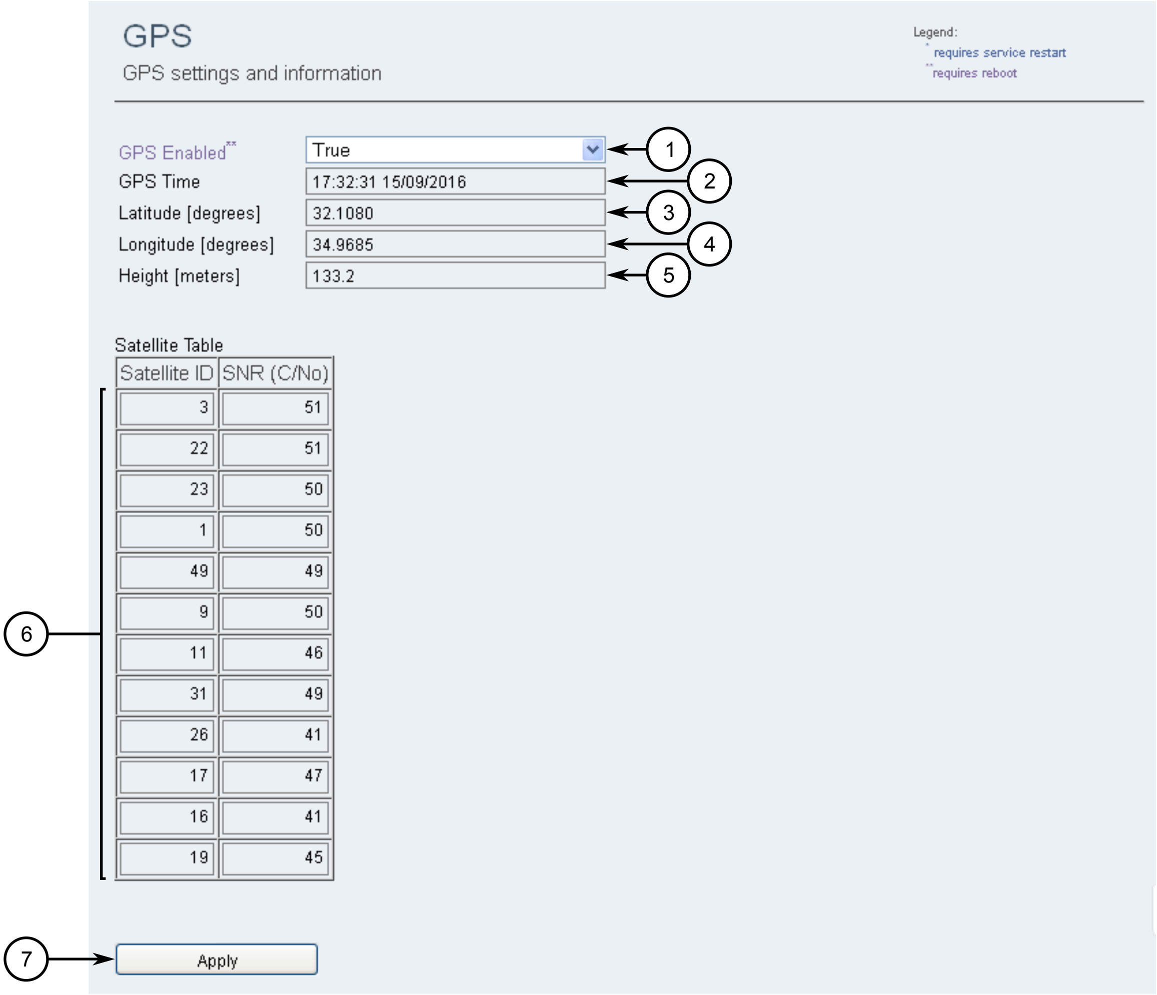
Section 4.11.1

Enabling/Disabling the GPS

If equipped with an integrated Global Positioning System (GPS), the device will transmit its position (latitude and longitude) to the serving base station every second. The base station can then be polled using SNMP for the device's coordinates, which can be plotted using third party tracking software.

To enable or disable the GPS, do the following:

1. Navigate to ***Management » GPS » GPS***. The **GPS** screen appears.



GPS

GPS settings and information

Legend:
* requires service restart
** requires reboot

GPS Enabled**	True
GPS Time	17:32:31 15/09/2016
Latitude [degrees]	32.1080
Longitude [degrees]	34.9685
Height [meters]	133.2

Satellite Table

Satellite ID	SNR (C/No)
3	51
22	51
23	50
1	50
49	49
9	50
11	46
31	49
26	41
17	47
16	41
19	45

Figure 27: GPS Screen

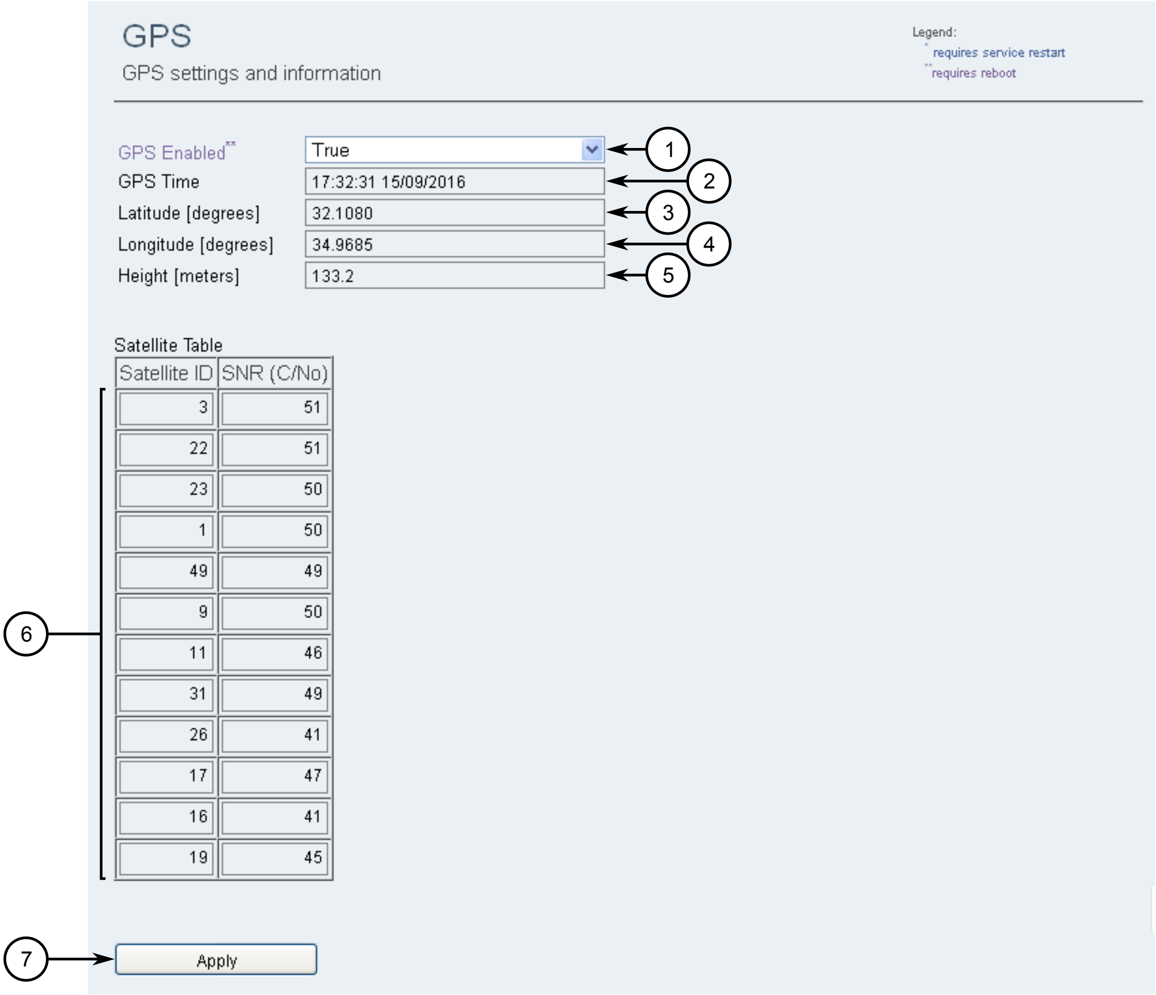
1. GPS Enabled List **2.** GPS Time **3.** Lattitude **4.** Longitude **5.** Height **6.** Satellite Data **7.** Apply Button

2. Under **GPS Enabled**, select either `True` to enable the GPS, or `False` to disable the GPS.
3. Click **Apply** and then reboot the subscriber station.

Section 4.11.2

Viewing Detected GPS Satellites

To view the GPS satellites detected by the subscriber station, navigate to ***Management » GPS » GPS***. The **GPS** screen appears.



GPS

GPS settings and information

GPS Enabled** True

GPS Time 17:32:31 15/09/2016

Latitude [degrees] 32.1080

Longitude [degrees] 34.9685

Height [meters] 133.2

Satellite Table

Satellite ID	SNR (C/No)
3	51
22	51
23	50
1	50
49	49
9	50
11	46
31	49
26	41
17	47
16	41
19	45

Figure 28: GPS Screen

1. GPS Enabled List **2.** GPS Time **3.** Lattitude **4.** Longitude **5.** Height **6.** Satellite Data **7.** Apply Button

The **Satellite Table** details the following information for each GPS satellite that is in view:

Parameter	Description
SatelliteID	The ID of the GPS satellite.
SNR (C/No)	The received signal strength in decibels/minute (dBm).

5 System Administration

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

CONTENTS

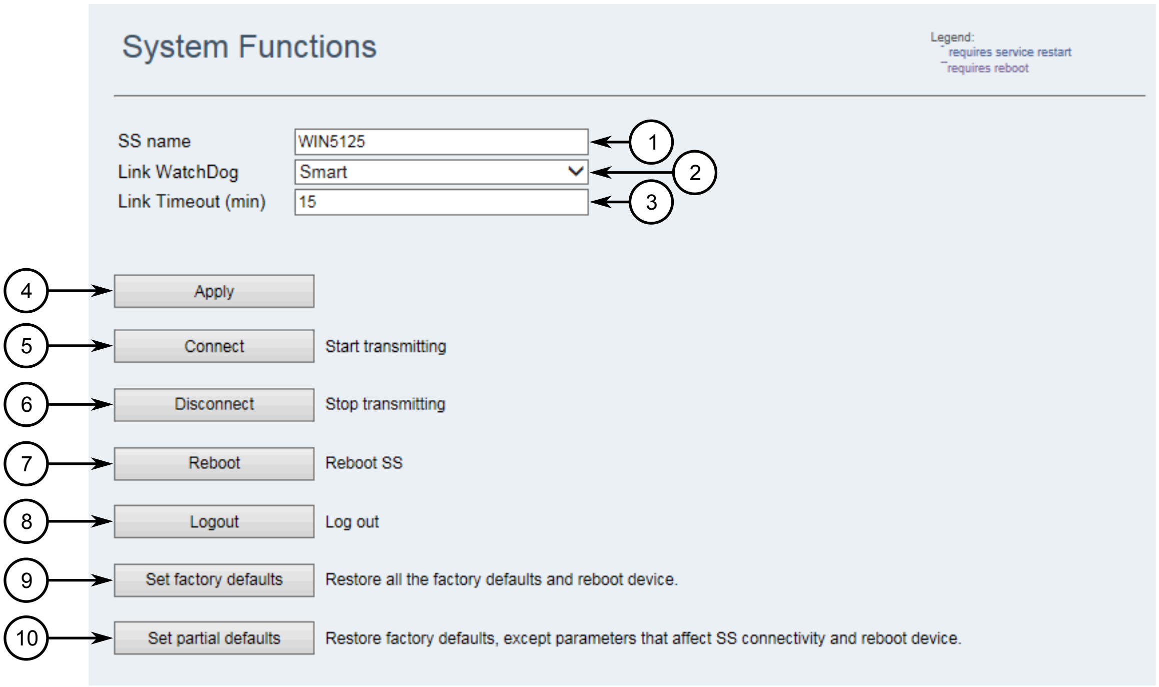
Section 5.1

Configuring the Device Name

> **NOTE**
> *The device name is read in SNMP and displayed in the management system. It is helpful to choose a name that helps identify the location of the subscriber station.*

To configure the name for the subscriber station, do the following:

1. Navigate to ***Management » System Functions » System Functions***. The **System Functions** screen appears.



System Functions

SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Figure 29: System Functions

1. SS Name Box **2.** Link WatchDog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Partial Defaults

2. Under **SS name**, enter the name for the subscriber station.
3. Click **Apply**. The name is displayed in the top right-hand corner of the screen.

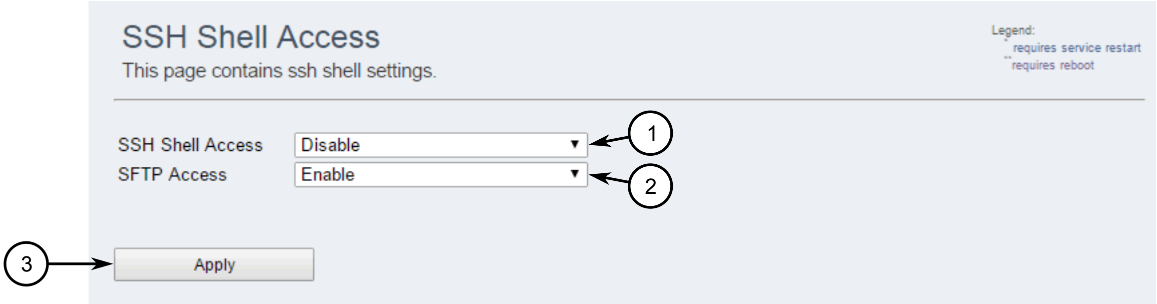
Section 5.2

Enabling/Disabling SSH Sessions

Enabling SSH sessions allows users to access the CLI remotely using Secure Shell (SSH).

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

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



SSH Shell Access

This page contains ssh shell settings.

SSH Shell Access: Disable

SFTP Access: Enable

Figure 30: SSH Shell Access Screen

1. SSH Shell Access List **2.** SFTP Access List **3.** Apply Button

2. Configure the following parameter:

Parameter	Description
SSH Shell Access	**Synopsis:** { Enable, Disable } **Default:** Disable Enables or disables remote access via SSH.

3. Click **Apply**.

Section 5.3

Managing Users and Passwords

This section describes how to manage users, including adding/removing user profiles and changing their passwords.

NOTE

Only users with administrator level access can manage user profiles and passwords.

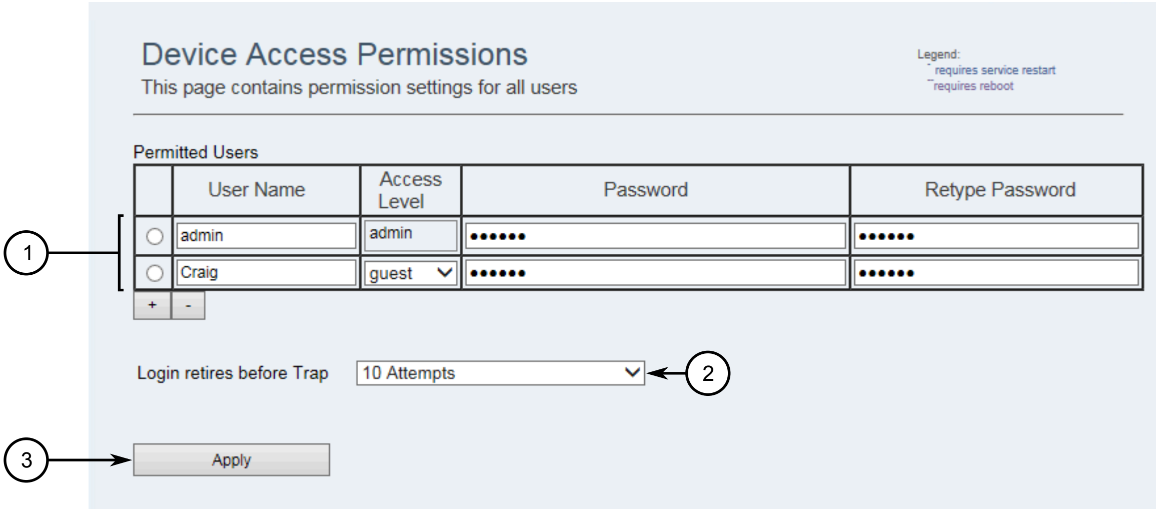
CONTENTS

Section 5.3.1

Adding Users

To add a user profile, do the following:

1. Navigate to ***Management » System Functions » Access Permissions***. The **Device Access Permissions** screen appears.



Device Access Permissions

This page contains permission settings for all users

Legend:
¯ requires service restart
¯¯ requires reboot

Permitted Users

	User Name	Access Level	Password	Retype Password
○	admin	admin	••••••	••••••
○	Craig	guest	••••••	••••••

Login retires before Trap: 10 Attempts

Figure 31: Device Access Permissions Screen

1. Users **2.** Login Retries Before Trap List **3.** Apply Button

2. Click +. A new row appears in the **Permitted Users** table.
3. Configure the following parameters:

Parameter	Description
User Name	A unique name assigned to the user profile. **NOTE** *The user name **admin** is reserved for the root administrator profile.*
Access Level	**Synopsis:** { admin, oper, guest } The user profiles access level. Options include: • `admin` – The user has full read/write priveleges • `guest` – The user has read priveleges only For information about the level of access offered by each privilege level, refer to Section 1.13, “User Permissions”.
Password	The user's password. It is recommended to use a strong password that meets the following criteria: • One lower case character • One upper case character • One number • One special character (i.e. !@#$%^&*()_+-={}[];:',<>/?|`~)

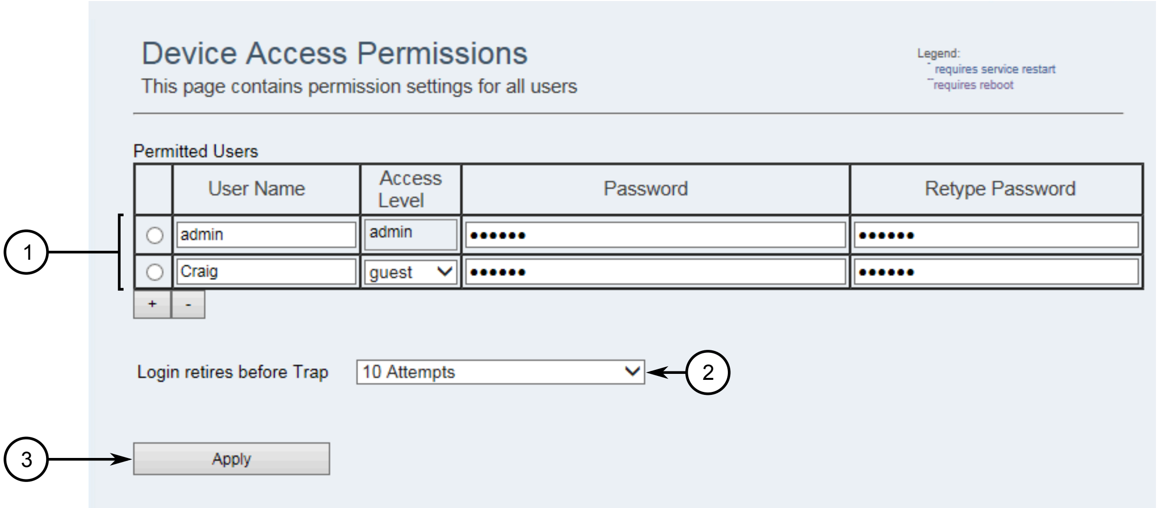
4. Under **Retype Password**, enter the user's password again the same as it was written under **Password**.
5. Click **Apply**.

Section 5.3.2

Removing Users

To remove a user profile, do the following:

1. Navigate to ***Management » System Functions » Access Permissions***. The **Device Access Permissions** screen appears.



Device Access Permissions

This page contains permission settings for all users

Legend:
requires service restart
requires reboot

Permitted Users

	User Name	Access Level	Password	Retype Password
○	admin	admin	••••••	••••••
○	Craig	guest	••••••	••••••

Login retires before Trap: 10 Attempts

Figure 32: Device Access Permissions Screen

1. Users **2.** Login Retries Before Trap List **3.** Apply Button

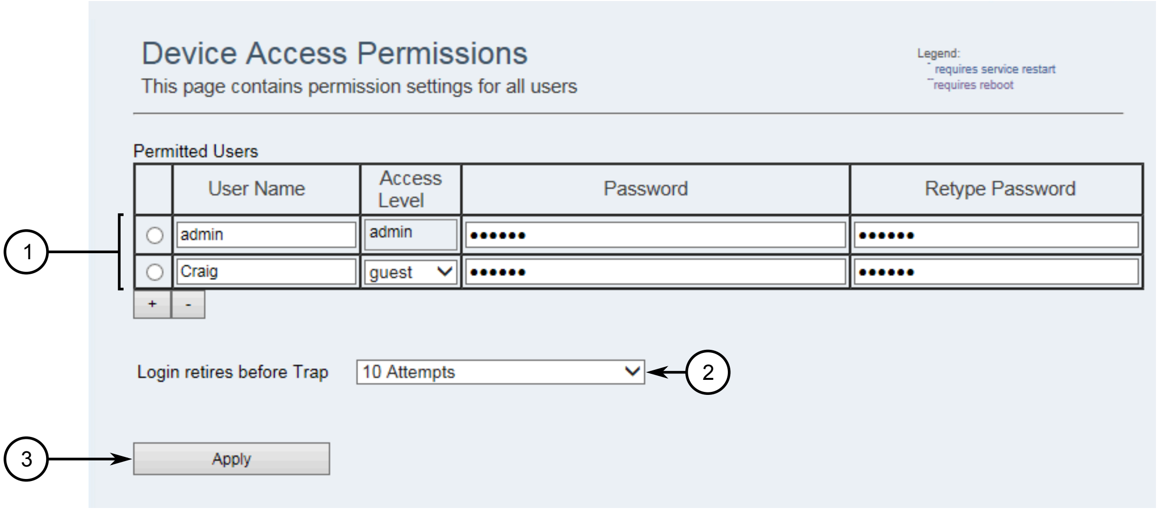
2. Select a user profile and then click -. The selected profile is removed.
3. Click **Apply**.

Section 5.3.3

Changing User Passwords

To change the password associated with a user profile, do the following:

1. Navigate to ***Management » System Functions » Access Permissions***. The **Device Access Permissions** screen appears.



Device Access Permissions

This page contains permission settings for all users

Legend:
requires service restart
requires reboot

Permitted Users

	User Name	Access Level	Password	Retype Password
○	admin	admin	••••••	••••••
○	Craig	guest	••••••	••••••

Login retires before Trap: 10 Attempts

Figure 33: Device Access Permissions Screen

1. Users **2.** Login Retries Before Trap List **3.** Apply Button

2. Under **Password**, enter a new password for the desired user. A strong password that meets the following criteria is recommended:
   - One lower case character
   - One upper case character
   - One number
   - One special character (i.e. !@#$%^&*()_+-={}[];:',<>/?\|`~)
3. Under **Retype Password**, enter the new password again the same as it was written under **Password**.
4. Click **Apply**.

Section 5.4

Managing Alarms

The alarm system in RUGGEDCOM WIN notifies users when events of interest occur. The system includes an extensive list of predefined alarms that can be enabled/disabled as needed.

CONTENTS

Section 5.4.1

Alarm Categories and Severities

Each alarm is organized by category and assigned a severity level.

Categories

Category	Description
Communication	Alarms related to the subscriber station's ability to communicate with the Local Area Network (LAN) and external sources, such as AAA servers, master clock, etc.
HW	Alarms related to hardware faults.
Radio	Alarms related to radio transmission faults.
Redundancy	Alarms related to network redundancy.
Other	Alarms related to the general operational state of the subscriber station

Severity Levels

Severity Level	Description
Clear	Clear alarms are notifications that a previous condition has been cleared.
Critical	Critical alarms represent events that disable all radio transmissions.
Major	Warning alarms represent events that may disable all radio transmissions and/or affect traffic flows.
Warning	Warning alarms represent events that only affect traffic flows.

Section 5.4.2

Available Alarms

RUGGEDCOM WIN features the following predefined alarms:

Alarm	ID	Category
LAN connectivity	4	Communication
Default HTTPs certificate is used	20	Communication
SSH connection was established	21	Communication
CLI connection was established	22	Communication

All alarms are listed under ***Management » Alarms and Traps***. For more information about viewing alarms, refer to Section 5.4.3, “Viewing/Clearing Alarms”.

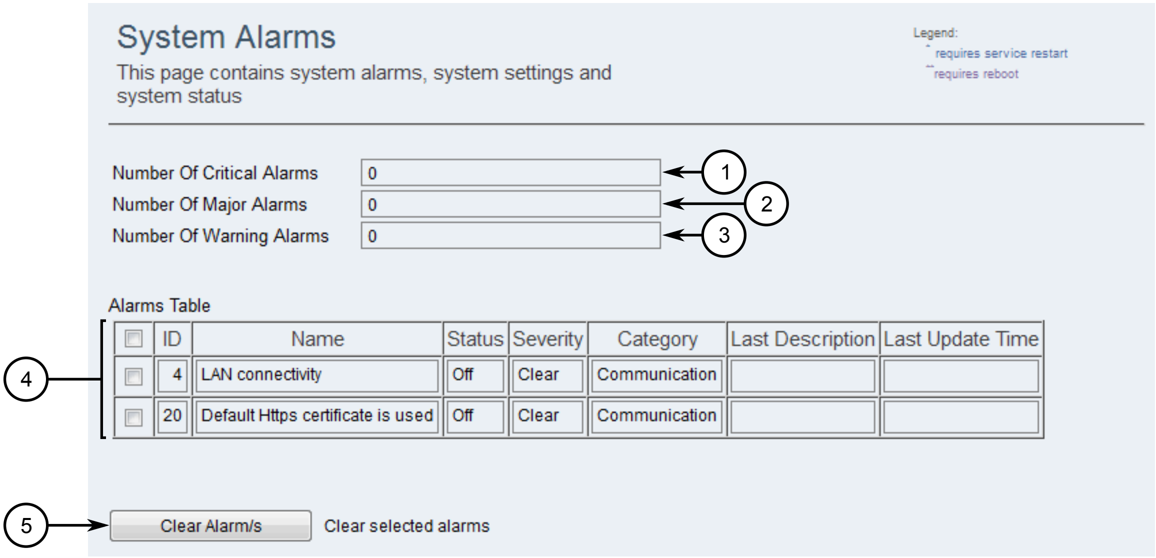
Section 5.4.3

Viewing/Clearing Alarms

Active system alarms are displayed in the user interface and can be cleared once resolved.

Viewing Alarms

To view the list of all predefined alarms, navigate to ***Management » Alarms and Traps***. The **System Alarms** screen appears.



System Alarms

This page contains system alarms, system settings and system status

Legend:
* requires service restart
** requires reboot

Number Of Critical Alarms: 0
Number Of Major Alarms: 0
Number Of Warning Alarms: 0

Alarms Table

□	ID	Name	Status	Severity	Category	Last Description	Last Update Time
□	4	LAN connectivity	Off	Clear	Communication		
□	20	Default Https certificate is used	Off	Clear	Communication		

Clear Alarm/s — Clear selected alarms

Figure 34: System Alarms Screen

1. Number of Critical Alarms **2.** Number of Major Alarms **3.** Number of Warning Alarms **4.** Alarms **5.** Clear Alarm/s Button

The **Number of Critical Alarms**, **Number of Major Alarms** and **Number of Warning Alarms** boxes indicate the number of active alarms based on their severity.

The **Alarms Table** provides additional information about each alarm:

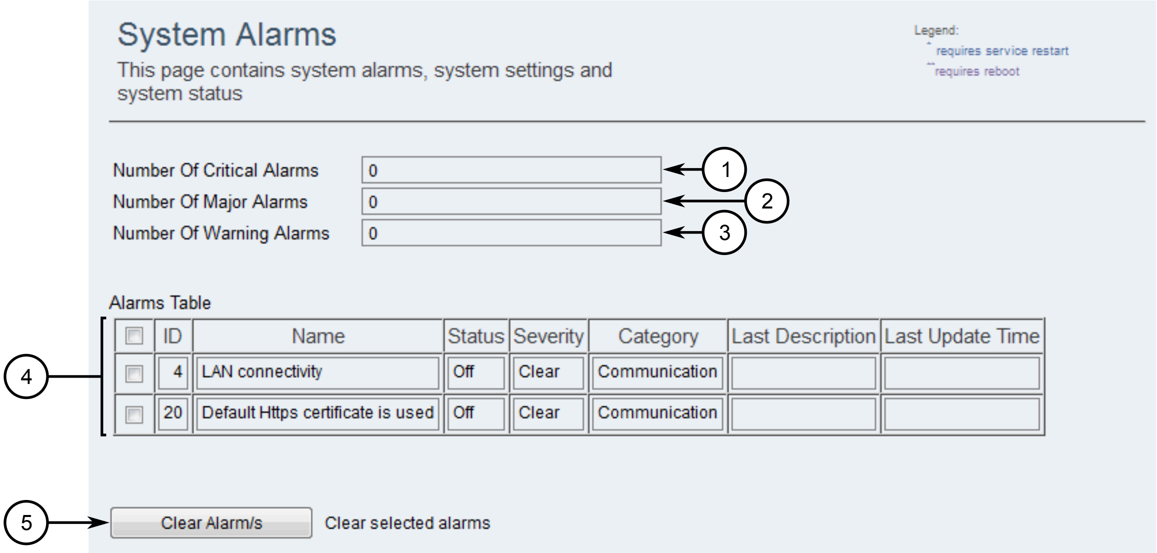
Column	Description
ID	The identification number assigned to the alarm.
Name	The alarm type. For information about each alarm type, refer to Section 5.4.2, “Available Alarms”.
Status	**Synopsis:** { On, Off } Indicates if the alarm type is enabled (On) or disabled (Off).
Severity	**Synopsis:** { Clear, Critical, Major, Warning } The severity of the alarm.
Category	**Synopsis:** { Restart, Communication, RF, Hardware, Security, Environmental, Redundancy, Services, Link Status } The category for the alarm type.
Last Description	A message describing the alarm.

Column	Description
Last Update Time	The date and time when the alarm was last activated.

Clearing Alarms

To clear alarms that have been resolved, do the following:

1. Navigate to ***Management » Alarms and Traps***. The **System Alarms** screen appears.



System Alarms

This page contains system alarms, system settings and system status

Legend:
* requires service restart
** requires reboot

Number Of Critical Alarms: 0
Number Of Major Alarms: 0
Number Of Warning Alarms: 0

Alarms Table

□	ID	Name	Status	Severity	Category	Last Description	Last Update Time
□	4	LAN connectivity	Off	Clear	Communication		
□	20	Default Https certificate is used	Off	Clear	Communication		

Figure 35: System Alarms Screen

1. Number of Critical Alarms **2.** Number of Major Alarms **3.** Number of Warning Alarms **4.** Alarms **5.** Clear Alarm/s Button

2. Select one or more alarms.
3. Click **Clear Alarm/s**. Each of the selected alarms is marked as **Clear** under the **Severity** column.

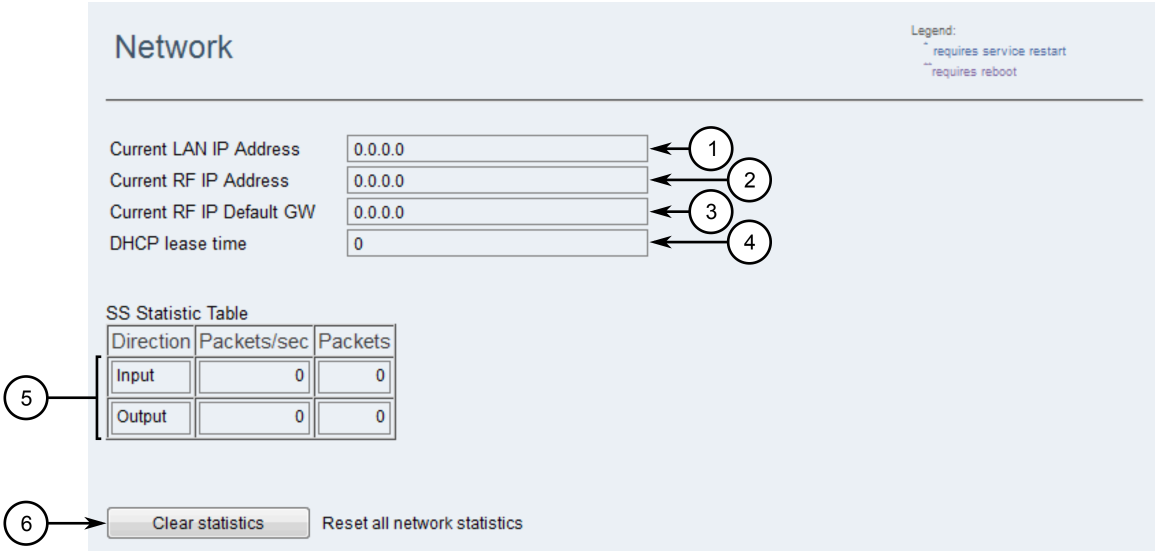
Section 5.5

Displaying the Current IP Address Settings

To view the current LAN and RF IP address settings, navigate to ***Statistics » Network » Network***. The **Network** screen appears.

NOTE

*The **Network** screen also displays network statistics. For more information, refer to Section 4.5.2, "Viewing and Clearing Network Statistics".*



Network

Legend:
* requires service restart
** requires reboot

Current LAN IP Address: 0.0.0.0
Current RF IP Address: 0.0.0.0
Current RF IP Default GW: 0.0.0.0
DHCP lease time: 0

SS Statistic Table

Direction	Packets/sec	Packets
Input	0	0
Output	0	0

Figure 36: Network Screen

1. Current LAN IP Address **2.** Current RF IP Address **3.** RF IP Default GW **4.** DHCP Lease Time **5.** SS Statistics **6.** Clear Statistics Button

The following parameters define the current IP address settings:

Parameter	Description
Current LAN IP Address	The current LAN IP address.
Current RF IP Address	The current RF IP address.
RF IP Default GW	The default gateway on the RF network.
DHCP Lease Time	The default DHCP lease time.

6 Security

This chapter describes how to configure and manage the security-related features of RUGGEDCOM WIN.

CONTENTS

Section 6.1

Configuring Brute Force Attack Protection

Protect against Brute Force Attacks (BFA) by configurig the maximum number of failed login attempts a host is allowed before an SNMP trap is triggered.

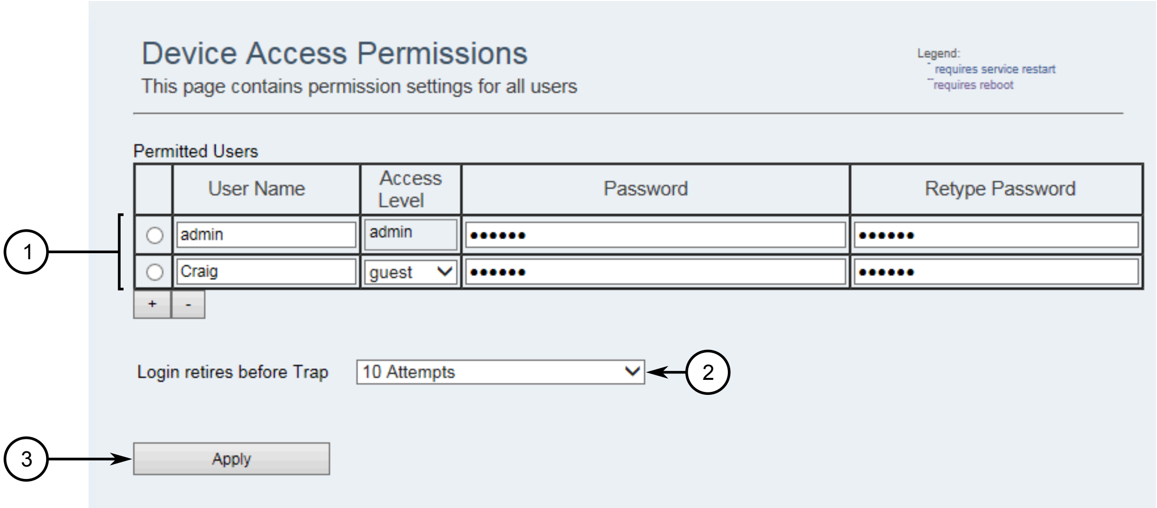
IMPORTANT!

BFA protection is not applicable to SNMP. Folow proper security practices for configuring SNMP. For example:

- *Do not use SNMP over the Internet*
- *Use a firewall to limit access to SNMP*
- *Do not use SNMPv1*

To configure the maximum number of failed login attempts, do the following:

1. Navigate to ***Management » System Functions » Access Permissions***. The **Device Access Permissions** screen appears.



Device Access Permissions

This page contains permission settings for all users

Legend:
- requires service restart
-- requires reboot

Permitted Users

	User Name	Access Level	Password	Retype Password
○	admin	admin	••••••	••••••
○	Craig	guest	••••••	••••••

Login retires before Trap: 10 Attempts

Figure 37: Device Access Permissions Screen

1. Users **2.** Login Retries Before Trap List **3.** Apply Button

2. Configure the following parameter:

Parameter	Description
Login Retries Before Trap	**Synopsis:** { Never Send Trap, 1 Attempt, 3 Attempts, 10 Attempts } **Default:** 10 Attempts The maximum number of times a host can attempt to login to the subscriber station before an SNMP trap is triggered. Options include: • `Never Send Trap` – disabled Brute Force Attack (BFA) protection • `1 Attempt` – hosts have only one chance to successfully login to the subscriber station • `3 Attempts` – hosts have three chances to successfully login to the subscriber station • `10 Attempts` – hosts have 10 chances to successfully login to the subscriber station

3. Click **Apply**.

Section 6.2

Enabling Ethernet Lock Mode

The subscriber station can be put in an *Ethernet Lock* mode that will automatically *lock* all ports when the following events occur:

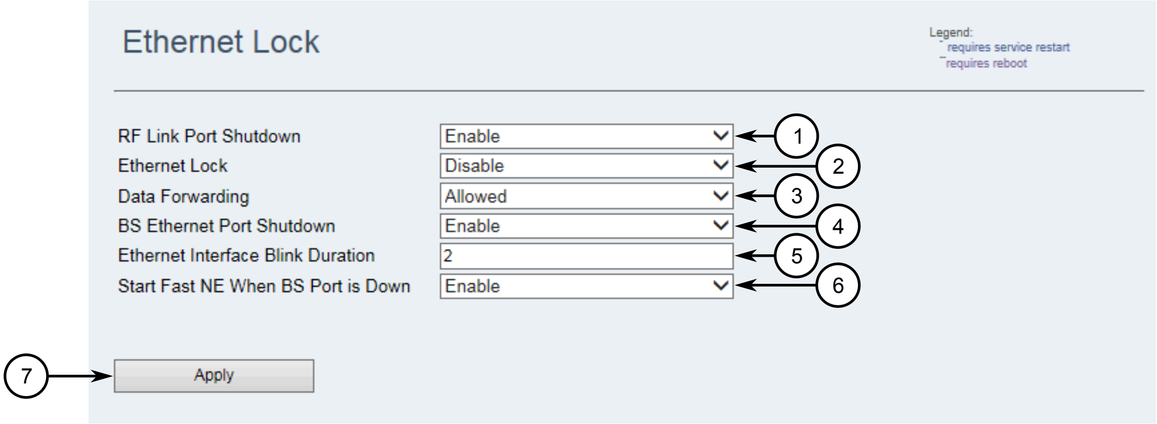
- The CAT-5e Ethernet cable is disconnected.
- During system start-up, with the following exceptions:
  - The reason for the system reboot was a software exception
  - The reboot was initiated by Link WatchDog
  - The reboot was initiated by a user
  - The reboot was initiated by the serving base station

NOTE
Management traffic to and from the subscriber station will always pass through.

NOTE
The subscriber station can be unlocked locally via RUGGEDCOM WIN, or remotely via the serving base station.

To enable Ethernet Lock mode, do the following:

1. Navigate to ***Management » Security » Ethernet Lock***. The **Ethernet Lock** screen appears.



Ethernet Lock

Legend:
requires service restart
requires reboot

RF Link Port Shutdown: Enable
Ethernet Lock: Disable
Data Forwarding: Allowed
BS Ethernet Port Shutdown: Enable
Ethernet Interface Blink Duration: 2
Start Fast NE When BS Port is Down: Enable

Figure 38: Ethernet Lock Screen

1. RF Link Port Shutdown List **2.** Ethernet Lock List **3.** Data Forwarding List **4.** BS Ethernet Port Shutdown List **5.** Ethernet Interface Blink Duration Box **6.** Start Fast NE When BS Port is Down List **7.** Apply Button

2. Configure the following parameters:

CAUTION!
*Configuration hazard – risk of data loss. Do not enable **Port Shutdown** and **Ethernet Lock** at the same time. All data packets will be dropped by the subscriber station if the RF link is lost.*

Parameter	Description
Port Shutdown	**Synopsis:** { Enable, Disable } **Default:** Disabled When enabled, the Ethernet ports are temporarily disabled for 3 seconds if the subscriber station loses its RF link to the serving base station. This indicates to a connected Layer 2 switch the subscriber station is down. To better understand this feature, consider the following scenario. Two subscriber stations are connected to the same base station, and to one another via a Layer 2 switch, creating a basic ring topology. If the first subscriber station loses its RF link with the base station, the switch (via STP) will route all traffic through the second subscriber station. If the second subscriber station *also* loses its RF link to the base station, the only way to indicate this to the switch is to temporarily disable the connected Ethernet port on the subscriber station. STP will detect this and automatically reroute traffic through the first subscriber station.

Parameter	Description
	NOTE *This feature should be disabled for fixed or single mobile subscriber stations.*
Ethernet Lock	**Synopsis:** { Enable, Disable } **Default:** Disabled When enabled, puts the Ethernet ports in Lock mode.
Data Forwarding	**Synopsis:** { Allowed, Blocked } **Default:** Allowed Controls whether traffic is forwarded through the Ethernet ports, with the exception of management traffic. Options include: • `Allowed` – The subscriber station is unlocked and traffic can be forwarded • `Blocked` – The subscriber station is locked and traffic cannot be forwarded

3. Click **Apply**.

Section 6.3

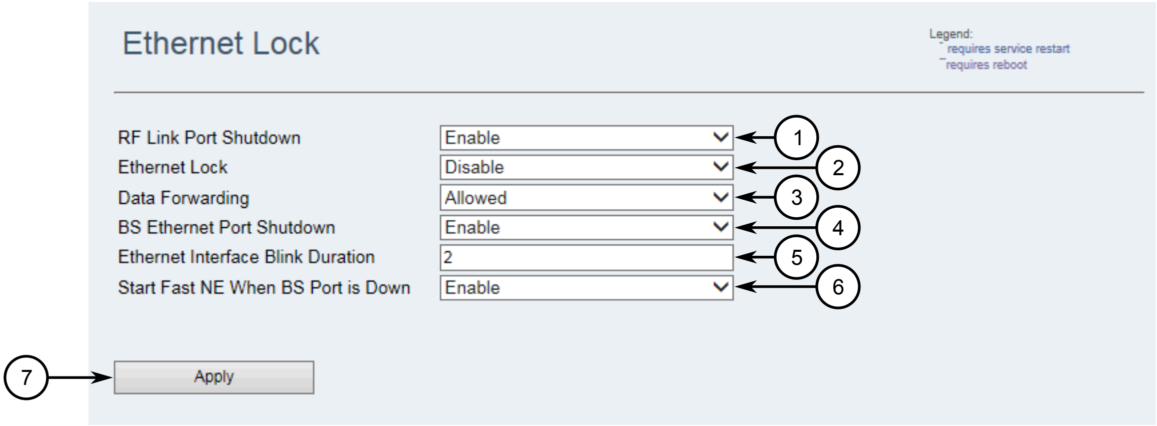
Halting Traffic When an Ethernet Port Shutdown Message is Received

When *Ethernet Port Shutdown* mode is enabled for the serving base station, the base station will advertise an *Eth Down* message to all registered subscriber stations when its physical Ethernet connection has been disconnected. Subscriber stations configured to handle the *Eth Down* message will halt all traffic to the serving base station for a specified period of time. Traffic will resume when the time expires if the same message is not received from the base station.

Subscriber stations can also be configured to immediately scan for a new base station when this event occurs.

To determine the subscriber station's response to *Eth Down* messages, do the following:

1. Navigate to ***Management » Security » Ethernet Lock***. The **Ethernet Lock** screen appears.



Ethernet Lock

Legend:
- requires service restart
- requires reboot

RF Link Port Shutdown: Enable
Ethernet Lock: Disable
Data Forwarding: Allowed
BS Ethernet Port Shutdown: Enable
Ethernet Interface Blink Duration: 2
Start Fast NE When BS Port is Down: Enable

Figure 39: Ethernet Lock Screen

1. RF Link Port Shutdown List **2.** Ethernet Lock List **3.** Data Forwarding List **4.** BS Ethernet Port Shutdown List **5.** Ethernet Interface Blink Duration Box **6.** Start Fast NE When BS Port is Down List **7.** Apply Button

2. Configure the following parameters:

Parameter	Description
BS Ethernet Port Shutdown	**Synopsis:** { Enable, Disable } **Default:** Disable Determines if the subscriber station can receive Ethernet port shutdown messages from the serving base station. These messages are sent when the base station's physical Ethernet connection is disconnected. Options include: • `Enable` – The subscriber station can receive Ethernet port shutdown messages • `Disable` – The subscriber station cannot receive Ethernet port shutdown messages
Ethernet Interface Blink Duration	**Default:** 2 The time in seconds (s) to wait after the serving base station advertises that its physical Ethernet connection has been disconnected. No packets will be sent during this time. If no messages are received from the serving base station before this timer expires, the subscriber station assumes the physical connection has been restored and resumes sending packets.
Start Fast NE When BS Port is Down	**Synopsis:** { Enable, Disable } **Default:** Disable Determines if the subscriber station will connect to a different base station when the serving base station's physical Ethernet connection has been disconnected. Options include: • `Enable` – The subscriber station will seek a different serving base station • `Disable` – The subscriber station does not seek a different serving base station

3. Click **Apply**.

Section 6.4

Managing Certificates and Keys

RUGGEDCOM WIN uses X.509v3 certificates and keys to establish secure connections for remote logins (SSH) and Web access (SSL).

To allow for initial configuration, all RUGGEDCOM WIN subscriber stations are shipped from the factory with a default HTTPS certificate and private key. Siemens recommends these be replaced by a certificate and private key signed by a trusted Certificate Authority (CA).

NOTE
Only admin users can read/write certificates and keys on the device.

CONTENTS

Section 6.4.1

Updating the Certificate and Private Key

To load certificates and/or keys, do the following:

NOTE
Replacement certificates and private keys must meet the following requirements:

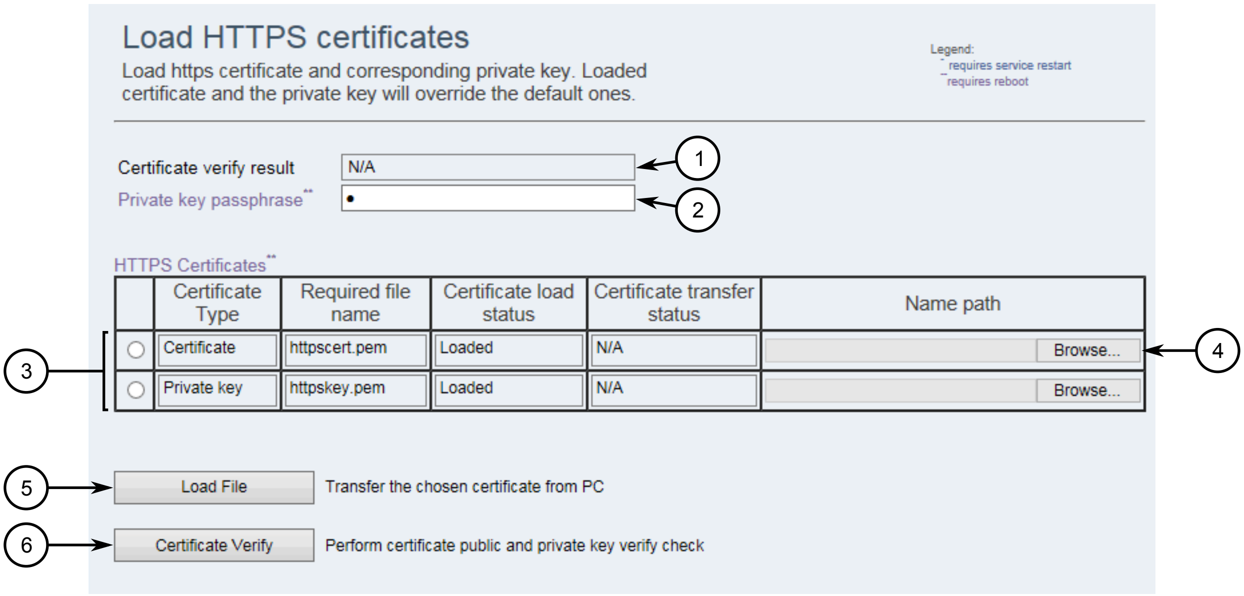
Certificate Requirements

- *Format: PEM*
- *File Name: httpscert.pem*
- *Maximum Size: 20 kb*

Key Requirements

- *Format: PEM*
- *File Name: httpskey.pem*
- *Maximum Size: 4 kb*
- *Password: 1 to 16 characters long*

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



Load HTTPS certificates

Load https certificate and corresponding private key. Loaded certificate and the private key will override the default ones.

Legend:
* requires service restart
** requires reboot

Certificate verify result: N/A

Private key passphrase**: •

HTTPS Certificates**

	Certificate Type	Required file name	Certificate load status	Certificate transfer status	Name path
○	Certificate	httpscert.pem	Loaded	N/A	Browse...
○	Private key	httpskey.pem	Loaded	N/A	Browse...

Load File — Transfer the chosen certificate from PC

Certificate Verify — Perform certificate public and private key verify check

Figure 40: Load HTTPS Certificates Screen

1. Certificate Verify Result **2.** Prviate Key Passphrase Box **3.** Certificates and Keys **4.** Browse Button **5.** Load File Button **6.** Certificate Verify Button

2. Select the certificate or private key, and then click **Browse**. A dialog box appears.
3. Use the dialog box to locate and select the new certificate or private key.
4. Click **Load File**. If the file is loaded successfully, *Success* appears in the **Certificate Transfer Status** column.

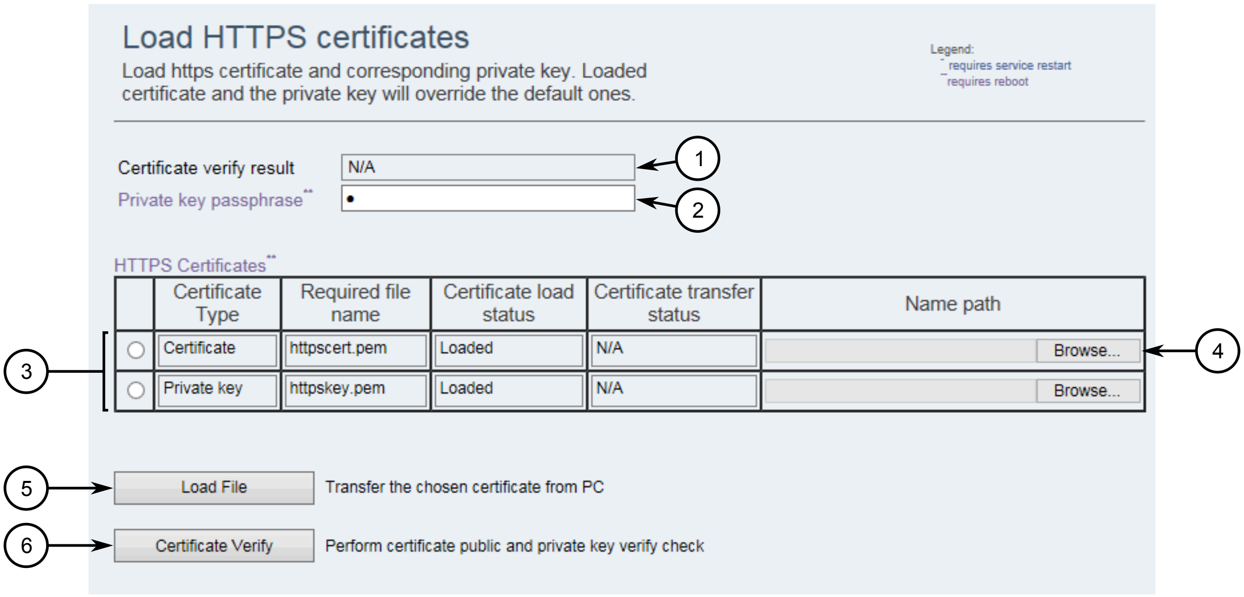
Section 6.4.2

Setting the Private Key Passphrase

To verify the authenticity of the private key, the passphrase set in RUGGEDCOM WIN must match the passphrase in the key file.

To the set the passphrase, do the following:

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



Load HTTPS certificates

Load https certificate and corresponding private key. Loaded certificate and the private key will override the default ones.

Legend:
* requires service restart
** requires reboot

Certificate verify result	N/A
Private key passphrase**	•

HTTPS Certificates**

	Certificate Type	Required file name	Certificate load status	Certificate transfer status	Name path
○	Certificate	httpscert.pem	Loaded	N/A	Browse...
○	Private key	httpskey.pem	Loaded	N/A	Browse...

Load File — Transfer the chosen certificate from PC

Certificate Verify — Perform certificate public and private key verify check

Figure 41: Load HTTPS Certificates Screen

1. Certificate Verify Result **2.** Prviate Key Passphrase Box **3.** Certificates and Keys **4.** Browse Button **5.** Load File Button **6.** Certificate Verify Button

2. Under **Private Key Passphrase**, enter the expected passphrase.
3. Click **Certificate Verify**. The verification results are displayed under **Certificate Verify Result**.

Section 6.4.3

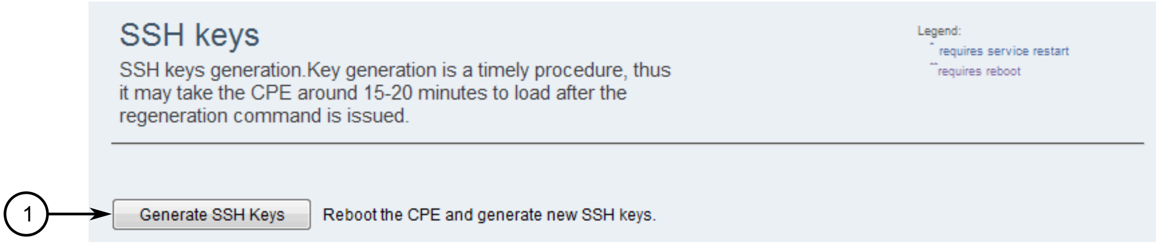
Generating SSH Keys

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

> **CAUTION!**
> *Security hazard – risk of unauthorized access and/or exploitation. It is important to generate new SSH keys when commissioning the subscriber station to prevent unauthorized access by users using the default SSH keys.*

> **NOTE**
> *Key generation can take up to 15 minutes to complete.*

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



SSH keys

SSH keys generation.Key generation is a timely procedure, thus it may take the CPE around 15-20 minutes to load after the regeneration command is issued.

Legend:
* requires service restart
** requires reboot

Generate SSH Keys — Reboot the CPE and generate new SSH keys.

Figure 42: SSH Keys Screen

1. Generate SSH Keys Button

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

Section 6.5

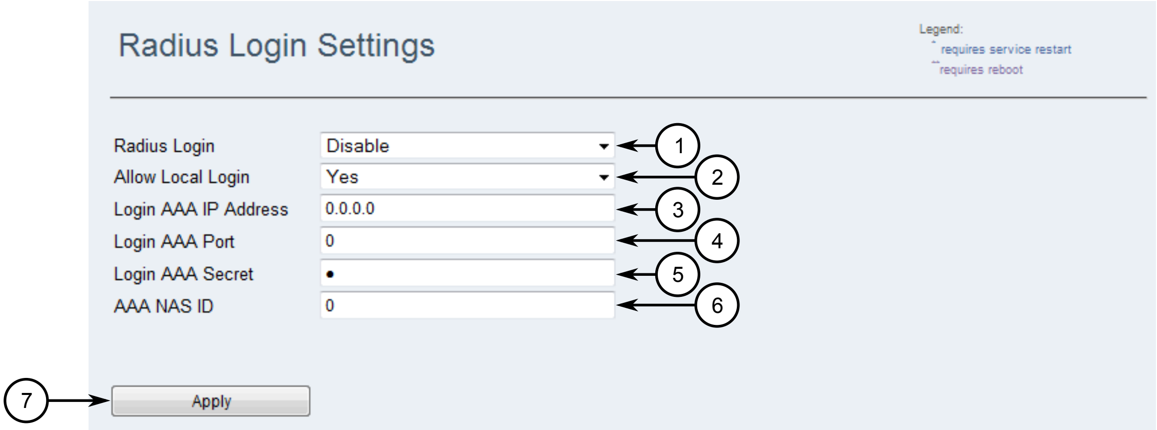
Configuring RADIUS Authentication

When RUGGEDCOM WIN is configured to use a Remote Authentication Dial-In User Service (RADIUS), all Web logins are verified against a AAA (Authentication, Authorizing and Accounting) authentication server.

If RADIUS authentication is not enabled, Web logins are authenticated locally by the subscriber station.

To configure RADIUS authentication, do the following:

1. Navigate to ***Management » Security » Radius Login Settings***. The **Radius Login Settings** screen appears.



Radius Login Settings

Legend:
* requires service restart
** requires reboot

Radius Login: Disable
Allow Local Login: Yes
Login AAA IP Address: 0.0.0.0
Login AAA Port: 0
Login AAA Secret: •
AAA NAS ID: 0

Figure 43: Radius Login Settings Screen

1. RADIUS Login List **2.** Allow Local Login List **3.** Login AAA IP Address Box **4.** Login AAA Port Box **5.** Login AAA Secret Box **6.** NAS ID Box **7.** Apply Button

2. Configure the following parameter:

Parameter	Description
RADIUS Login	**Synopsis:** { Enable, Disable } **Default:** Disable

Parameter	Description
	Enables or disables RADIUS Authentication mode.
Allow Local Login	**Synopsis:** { Yes, No } **Default:** Yes Allows or prevents users to log in using *admin@local*. Options include: • `Yes` – Users can login using *admin@local*. • `No` – Users cannot login using *admin@local*. Only user names defined under ***Management » System Functions » Access Permissions*** can access the subscriber station. Users will also be unable to access options under ***Management » Security*** to enable local login access while there is an active connection to the RADIUS server. Only If the connection to the configured AAA servers is lost is access restored.
Login AAA IP Address	The IP address of the RADIUS server.
Login AAA Port	The port on the RADIUS server used for remote authentication.
Login AAA Secret	The secrete key shared between the subscriber station and RADIUS server. This is used to encrypt passwords and exchange responses.
NAS ID	The Network Access Server (NAS) ID. This ID is used by the RADIUS server to determine the correct policy to use for the authentication request. The value can be an FQDN of the NAS or any unique string to identify the NAS.

3. Click **Apply**.

7 Time Synchronization

This chapter describes how to configure the subscriber station as a time source for other devices.

CONTENTS

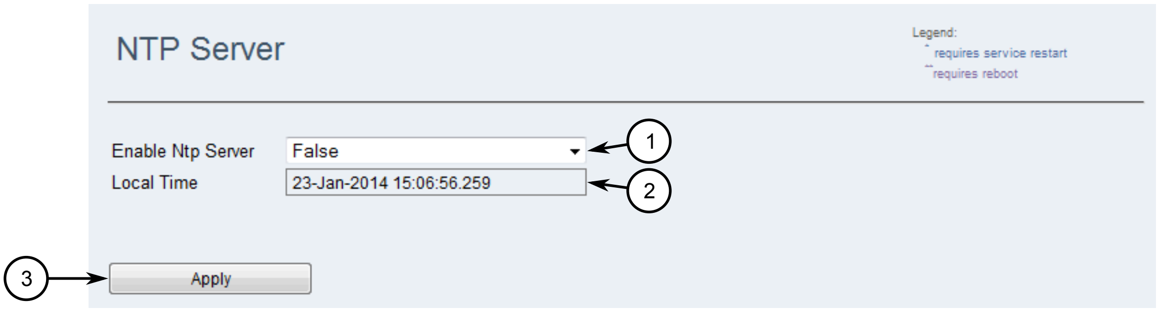
Section 7.1

Enabling the NTP Server

Enabling the NTP server allows the subscriber station to forward the current date and time to other devices on the network.

To enable the NTP server, do the following:

1. Make sure `Time Advertisement Enabled` is enabled for the serving base station. For more information, refer to the *RUGGEDCOM WIN User Guide* for the base station.
2. Navigate to ***Management » NTP Server***. The **NTP Server** screen appears.



NTP Server

Legend:
* requires service restart
** requires reboot

Enable Ntp Server: False
Local Time: 23-Jan-2014 15:06:56.259

Figure 44: NTP Server Screen

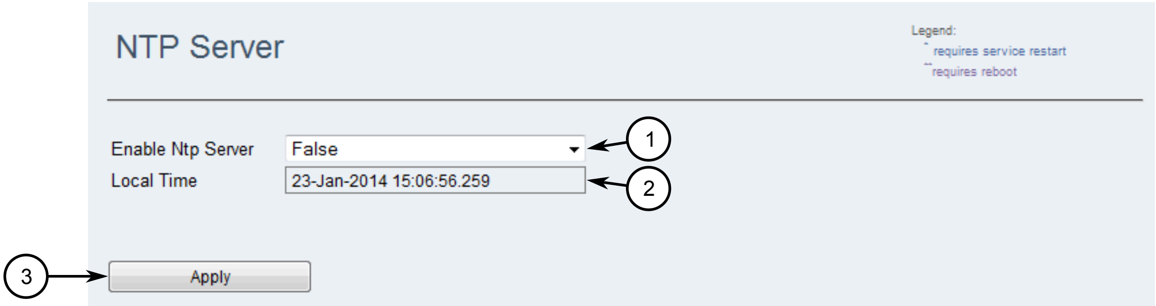
1. Enable NTP Server List **2.** Local Time **3.** Apply Button

3. Under **Enable NTP Server**, select `True`.
4. Click **Apply**.

Section 7.2

Displaying the Current Local Time

To display the current local time broadcast by the serving base station and forward by the subscribers station to other devices, navigate to ***Management » NTP Server***. The **NTP Server** screen appears.



NTP Server

Enable Ntp Server: False

Local Time: 23-Jan-2014 15:06:56.259

Figure 45: NTP Server Screen

1. Enable NTP Server List **2.** Local Time **3.** Apply Button

The current local time is displayed under **Local Time**.

8 Base Stations

This section describes how to manage the subscriber station's connection with a serving base station.

CONTENTS

Section 8.1

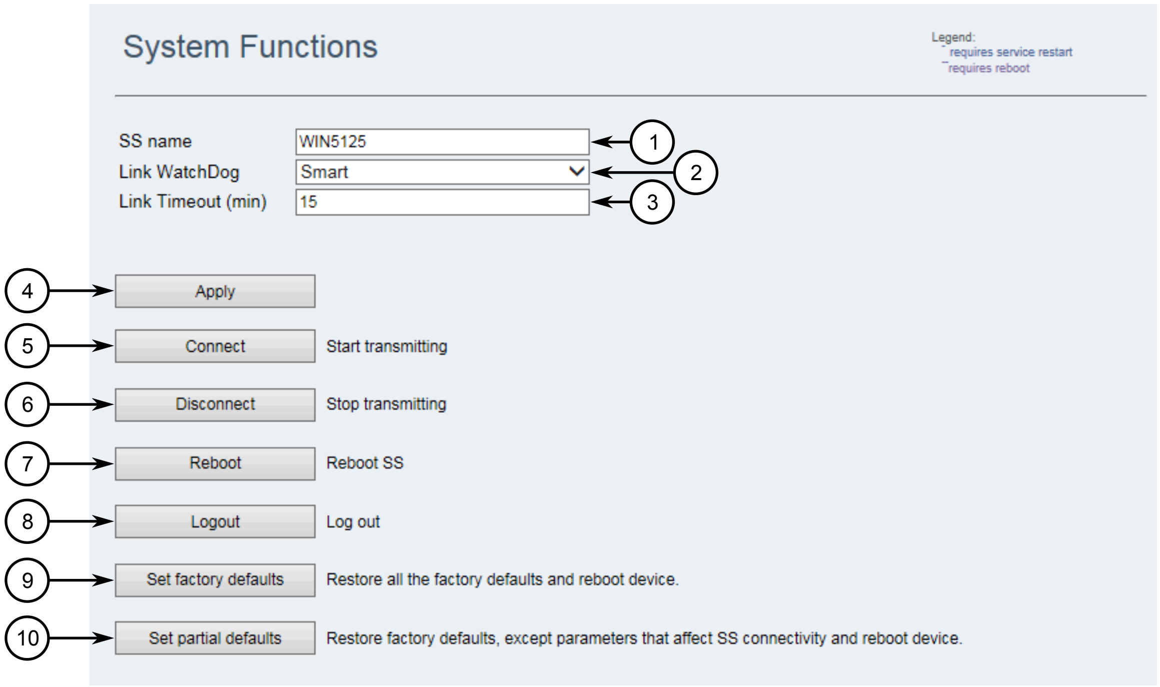
Connecting to a Base Station

The procedure for connecting the subscriber station to a base station is dependent on whether or not the `Connect Only to Allowed BS` parameter is enabled. When enabled, the subscriber station only connects to devices in the *Allowed BS* list.

›› Connecting to a Base Stations When `Connect Only to Allowed BS` is Not Enabled

To connect to a base station, do the following:

1. Navigate to ***Management » System Functions » System Functions***. The **System Functions** screen appears.



System Functions

Legend:
requires service restart
requires reboot

SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Apply

Connect — Start transmitting

Disconnect — Stop transmitting

Reboot — Reboot SS

Logout — Log out

Set factory defaults — Restore all the factory defaults and reboot device.

Set partial defaults — Restore factory defaults, except parameters that affect SS connectivity and reboot device.

Figure 46: System Functions

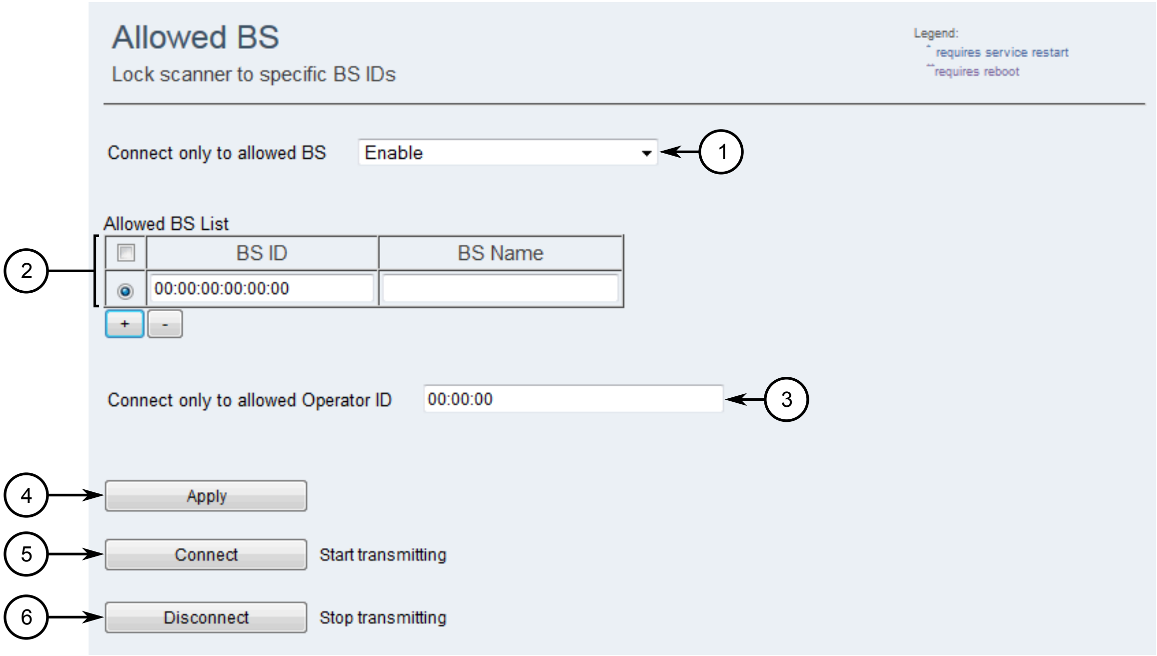
1. SS Name Box **2.** Link WatchDog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Partial Defaults

2. Click **Connect**. The subscriber station starts scanning for a viable base station. It will connect to the one that offers the best signal quality and strength at the time.

Connecting to a Base Station When `Connect Only to Allowed BS` is Enabled

To connect to a base station, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Allowed BS***. The **Allowed BS** screen appears.



Allowed BS

Lock scanner to specific BS IDs

Legend:
* requires service restart
** requires reboot

Connect only to allowed BS: Enable

Allowed BS List

☐	BS ID	BS Name
●	00:00:00:00:00:00	

Connect only to allowed Operator ID: 00:00:00

Figure 47: Allowed BS Screen

1. Connect Only to Allowed BS List **2.** Allowed BS List Table **3.** Connect Only to Allowed Operator ID Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button

2. Make sure the scanner is configured to only scan specific base stations and base stations have been added to the *Allowed BS* list. For more information, refer to Section 8.3.5, “Locking the Scanner on Specific Base Stations”.

3. Select one or more base stations from the **Allowed BS List** table and then click **Connect**. The subscriber station starts scanning the selected base station(s). It will connect to the one that offers the best signal quality and strength at the time.

Section 8.2

Disconnecting from the Base Station

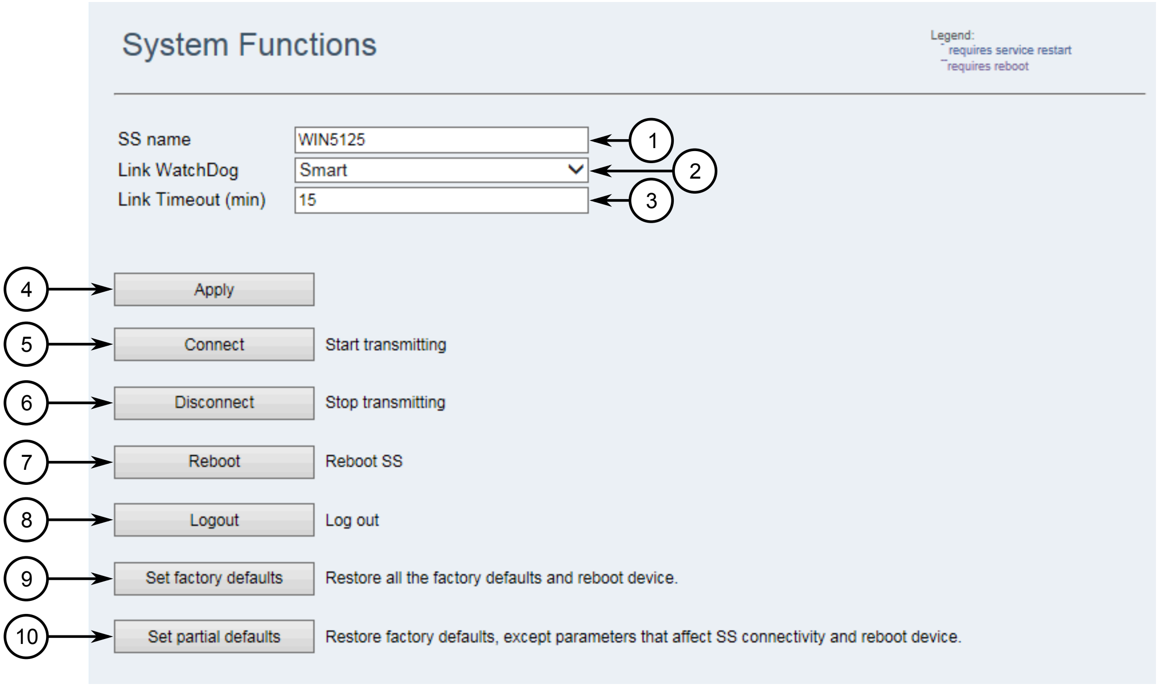
The procedure for disconnecting the subscriber station from its serving base station is dependent on whether or not the `Connect Only to Allowed BS` parameter is enabled. When enabled, the subscriber station only connects to devices in the *Allowed BS* list.

> ⚠ **CAUTION!**
> *Configuration hazard – risk of losing the connection with current base station. Do not click **Disconnect** if using the RF Interface. The subscriber station will stop transmitting and lose its connection to the serving base station. A hard reset (shutting down and then powering up) or a site visit will be required to reboot the device.*

Disconnecting from Base Stations When `Connect Only to Allowed BS` is Not Enabled

To disconnect the subscriber station from its serving base station, do the following:

1. Navigate to ***Management » System Functions » System Functions***. The **System Functions** screen appears.



System Functions

SS name: WIN5125
Link WatchDog: Smart
Link Timeout (min): 15

Figure 48: System Functions

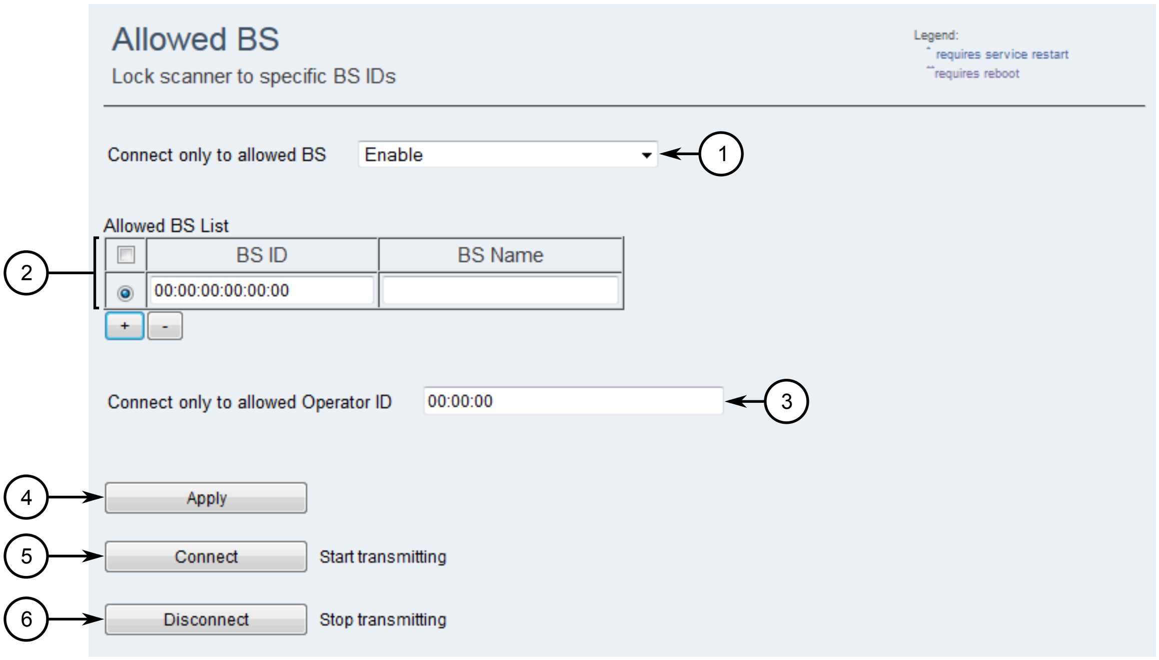
1. SS Name Box **2.** Link WatchDog List **3.** Link Timeout Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button **7.** Reboot Button **8.** Logout Button **9.** Set Factory Defaults Button **10.** Set Partial Defaults

2. Click **Disconnect**.

Disconnecting from a Base Station When `Connect Only to Allowed BS` is Enabled

To disconnect the subscriber station from its serving base station, do the following:

1. Navigate to ***WiMAX » Allowed BS***. The **Allowed BS** screen appears.



Allowed BS

Lock scanner to specific BS IDs

Legend:
* requires service restart
** requires reboot

Connect only to allowed BS: Enable

Allowed BS List

☐	BS ID	BS Name
●	00:00:00:00:00:00	

Connect only to allowed Operator ID: 00:00:00

Figure 49: Allowed BS Screen

1. Connect Only to Allowed BS List **2.** Allowed BS List Table **3.** Connect Only to Allowed Operator ID Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button

2. Click **Disconnect**.

Section 8.3

Scanning for Base Stations

This section describes how to configure the subscriber station to scan for target base stations. Scanning is initiated when the signal strength and/or quality from the serving base station degrades past a defined a threshold, or if the serving base station goes offline.

> **NOTE**
> *The scanner is not initiated during handover.*

CONTENTS

Section 8.3.1

Understanding the Scanner

The scanner searches for base stations that either emit a signal that exceeds the Carrier to Interference + Noise Ratio (CINR) threshold or meet the frequency criteria. Both the CINR threshold and frequency criteria are user defined.

When configuring the scanner, it is recommend to define the desired minimum CINR threshold and one or more frequencies. Up to 32 single frequencies or frequency ranges can be defined.

CONTENTS

Section 8.3.1.1

Scanning Process

The scanner follows the following process when scanning for base stations:

1. **Scan By CINR**
   The scanner scans for base stations with a high CINR. If base stations are discovered that have a CINR above the defined CINR threshold, the subscriber station automatically connects to the base station with the highest CINR.

   If none of the discovered base stations have a CINR that meets or exceeds the CINR threshold, the scanner resorts to scanning specific frequencies (if defined).

2. **Scan By Frequency**
   The scanner scans for base stations operating on a specific frequency. Frequency ranges or specific frequencies can be defined. Priority can also be granted to specific frequencies.

   If base stations are discovered operating on the defined frequencies, the subscriber station will connect to the base station with the highest CINR.

Section 8.3.1.2

Single Frequencies and Frequency Ranges

The scanner can be configured to search for base stations operating on specific frequencies. Up to 32 single frequencies or frequency ranges can be defined.

A **single frequency** is defined by setting the start and the end frequency to the same value and the number of steps to zero (0).

A **frequency range** is defined by setting a start frequency, an end frequency, and a step. The smallest possible step is 250 Khz.

Defining a start frequency as 3.473 Ghz and an end frequency of 3.583 Ghz with a step of 11 Mhz is similar to defining singular frequencies as 3.473 Ghz, 3.484 Ghz, 3. 495 Ghz ..., 3.583 Ghz. The scanner will scan all available frequencies in the range and try to connect to the base station with the highest CINR.

> **NOTE**
> *PUSC (Partial Usage of the Sub Channel) mode can be configured for single frequency or frequency range. For more information about PUSC mode, refer to Section 8.3.1.3, "PUSC Mode".*

Section 8.3.1.3

PUSC Mode

Set the PUSC (Partial Usage of the Sub Channel) mode on a specific frequency or frequency range when searching for base stations that work in PUSC mode. This setting may help the subscriber station lock on to a specific base station when if it is located on the border edge between two different PUSC segments. However, this setting should be used carefully, as it may cause a subscriber station to connect to a weaker signal if the wrong PUSC segment is defined.

Section 8.3.2

Configuring the Scanner

To configure the scanner, do the following:

1. Set the minimum CINR threshold. The subscriber station will automatically connect to base stations whose CINR exceeds this threshold.

   For more information, refer to Section 8.3.3, "Setting the Minimum CINR Threshold".

2. Choose whether to allow the scanner to search for base stations based on operating frequency or restrict the scanner to a list of specific base stations.

   - **Scanning Based on Operating Frequency**
     Define one or more target frequencies. The scanner will resort to scanning specific frequencies if a base station with a CINR at or above the minimum threshold cannot be found.

     For more information, refer to Section 8.3.4, "Configuring Target Frequencies".

   - **Scanning Only Specific Base Stations**
     Enable *`Connect Only to Allowed BS`*. The scanner will only scan base stations defined in the **Allowed BS List** table.

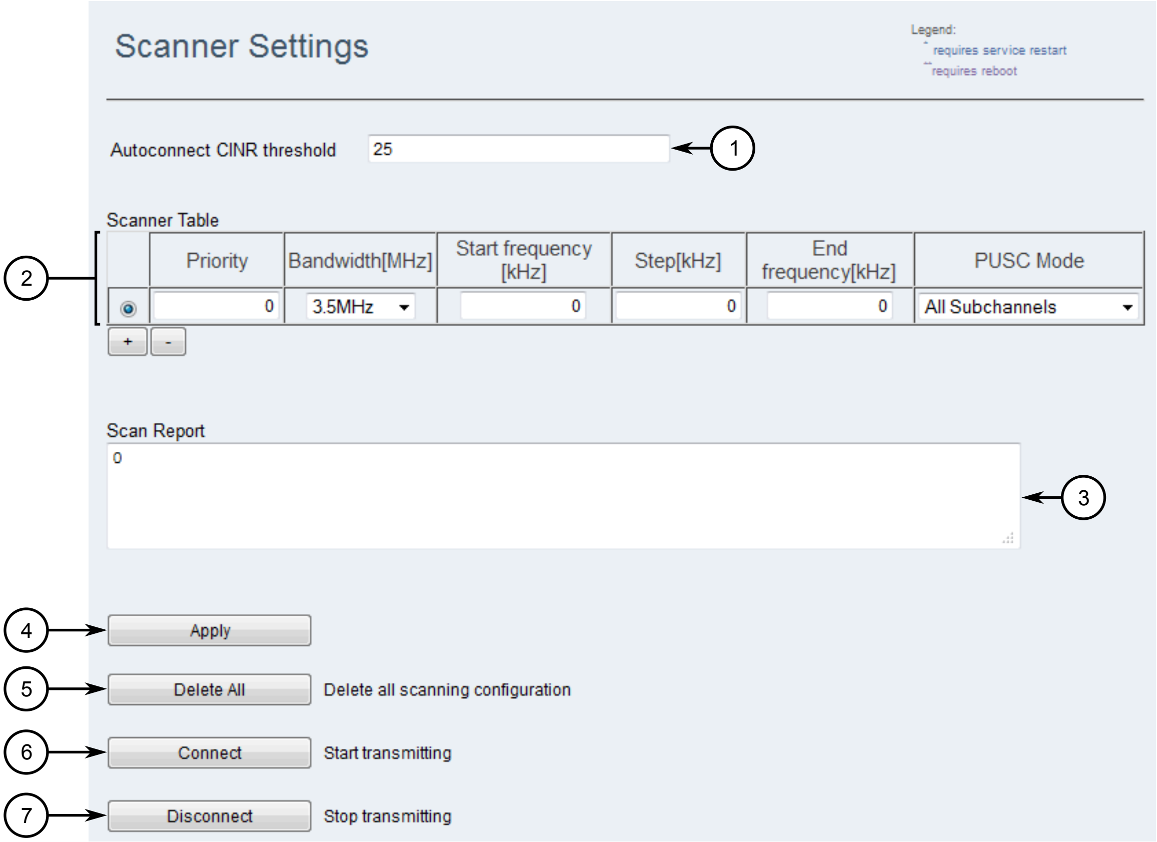
     For more information, refer to Section 8.3.5, "Locking the Scanner on Specific Base Stations".

Section 8.3.3

Setting the Minimum CINR Threshold

To set the minimum CINR threshold for the scanner, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Scanner Settings***. The **Scanner Settings** screen appears.



Scanner Settings

Legend:
* requires service restart
** requires reboot

Autoconnect CINR threshold: 25

Scanner Table

	Priority	Bandwidth[MHz]	Start frequency [kHz]	Step[kHz]	End frequency[kHz]	PUSC Mode
●	0	3.5MHz	0	0	0	All Subchannels

Scan Report
0

Delete All: Delete all scanning configuration
Connect: Start transmitting
Disconnect: Stop transmitting

Figure 50: Scanner Settings Screen

1. Autocorrect CINR Threshold Box **2.** Frequencies **3.** Scan Report **4.** Apply Button **5.** Delete All Button **6.** Connect Button **7.** Disconnect Button

2. If the subscriber station is already connected to a base station, click **Disconnect**.
3. Under **Autoconnect CINR Threshold**, enter the desired minimum CINR threshold.
4. Click **Apply**.

Section 8.3.4

Configuring Target Frequencies

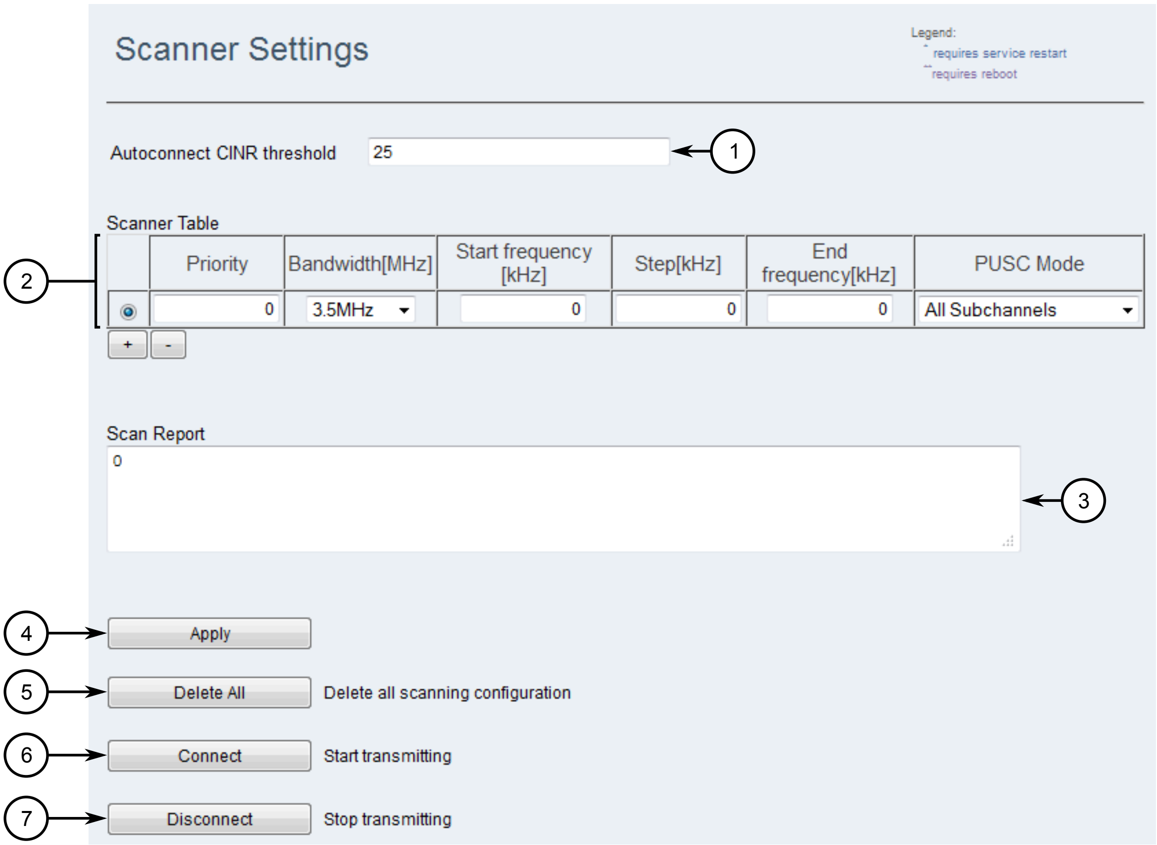
The scanner resorts to scanning for base stations operating on specific frequencies when none are discovered with a CINR higher than the minimum CINR threshold.

Up to 32 target frequencies can be defined. For more information about configuring the frequencies, refer to Section 8.3.1.2, “Single Frequencies and Frequency Ranges”.

Adding/Updating Target Frequencies

To add or update a target frequency, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Scanner Settings***. The **Scanner Settings** screen appears.



Scanner Settings

Legend:
* requires service restart
** requires reboot

Autoconnect CINR threshold 25

Scanner Table

	Priority	Bandwidth[MHz]	Start frequency [kHz]	Step[kHz]	End frequency[kHz]	PUSC Mode
●	0	3.5MHz	0	0	0	All Subchannels

Scan Report

0

Figure 51: Scanner Settings Screen

1. Autocorrect CINR Threshold Box **2.** Frequencies **3.** Scan Report **4.** Apply Button **5.** Delete All Button **6.** Connect Button **7.** Disconnect Button

CAUTION!

*Configuration hazard – risk of losing the connection with current base station. Do not click **Disconnect** if using the RF Interface. The subscriber station will stop transmitting and lose its connection to the serving base station. A hard reset (shutting down and then powering up) or a site visit will be required to reboot the device.*

2. If connecting to the subscriber station directly or if the subscriber station is in scanning mode, click **Disconnect**.
3. Update the configuration for a frequency already defined or click + to add a new frequency.
4. Configure the following parameters:

Parameter	Description
Priority	**Synopsis:** An integer The priority for the scanning table entry. Priority is ranked in numeric order.
Bandwidth	**Synopsis:** { 3.5MHz, 5MHz, 7MHz, 10MHz } The desired bandwidth in megahertz (MHz).

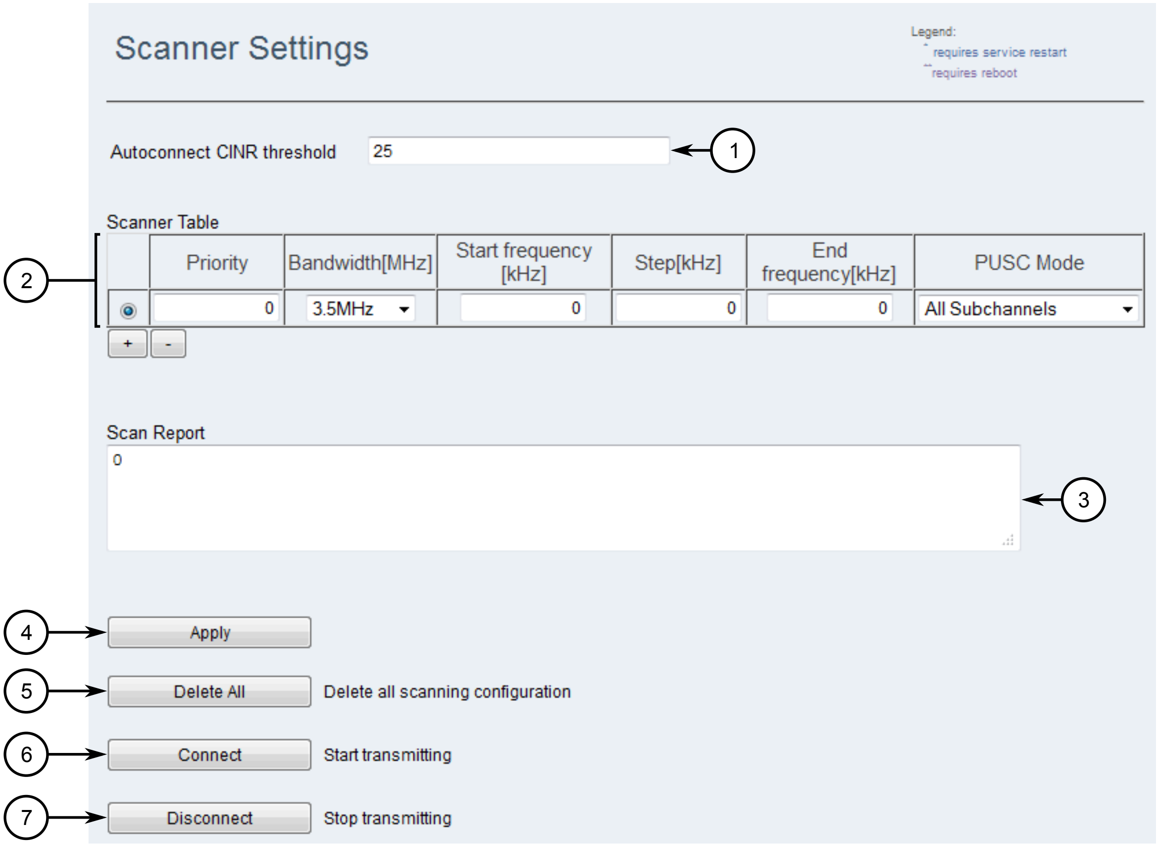
Parameter	Description
Start frequency	The start of the scanning range as a frequency in kilohertz (kHz).
Step	The scanning increment in the scanning range in kilohertz (kHz).
End frequency	The end of the scanning range as a frequency in kilohertz (kHz).
PUSC Mode	**Synopsis:** { PUSC3, PUSC2, PUSC1, All Subchannels } The desired PUSC (Partial Usage of the Sub Channel) mode. For more information, refer to Section 8.3.1.3, “PUSC Mode”.

5. Click **Apply**.

Deleting a Target Frequency

To delete a target frequency, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Scanner Settings***. The **Scanner Settings** screen appears.



Scanner Settings

Legend:
* requires service restart
** requires reboot

Autoconnect CINR threshold 25

Scanner Table

	Priority	Bandwidth[MHz]	Start frequency [kHz]	Step[kHz]	End frequency[kHz]	PUSC Mode
●	0	3.5MHz	0	0	0	All Subchannels

Scan Report
0

Delete All — Delete all scanning configuration

Connect — Start transmitting

Disconnect — Stop transmitting

Figure 52: Scanner Settings Screen

1. Autocorrect CINR Threshold Box **2.** Frequencies **3.** Scan Report **4.** Apply Button **5.** Delete All Button **6.** Connect Button **7.** Disconnect Button

2. Either click **Delete All** to delete all scanner configurations, or delete specific configurations by doing the following:

  a. Select one more rows.
  b. Click **Delete**.

3. Click **Apply**.

Section 8.3.5

Locking the Scanner on Specific Base Stations

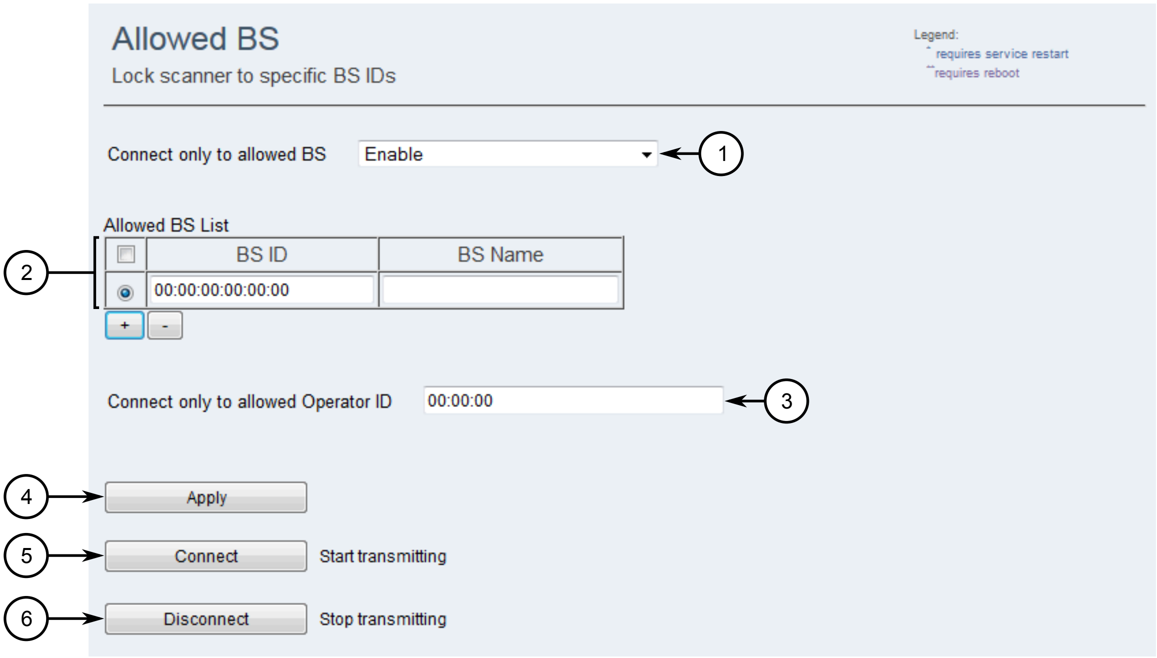
To accelerate scanning time, the subscriber station can be made to scan only base stations in the *Allowed BS* list. This user-defined list details the ID and name for one or more base stations. If the subscriber station needs to disconnect from its serving base station, it can only connect to base stations in the *Allowed BS* list.

If required, the scanner can be further restricted to only scan base stations in the list that use a specific Network Access Provider.

For information about populating the *Allowed BS* list, refer to Section 8.3.6, "Defining Allowed Base Stations".

To configure the subscriber station to only scan and connect to base stations on the *Allowed BS* list, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Allowed BS***. The **Allowed BS** screen appears.



Allowed BS

Lock scanner to specific BS IDs

Legend:
* requires service restart
** requires reboot

Connect only to allowed BS: Enable

Allowed BS List

□	BS ID	BS Name
●	00:00:00:00:00:00	

Connect only to allowed Operator ID: 00:00:00

Figure 53: Allowed BS Screen

1. Connect Only to Allowed BS List **2.** Allowed BS List Table **3.** Connect Only to Allowed Operator ID Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button

2. Under **Connect Only to Allowed BS**, select **Enable**.
3. [Optional] Under **Connect Only to Allowed Operator ID**, enter an operator ID. This represents a specific Network Access Provider. If the subscriber station needs to disconnect from the serving base station, it can only connect to the other base stations in the *Allowed BS* list that use the specified Network Access Provider.

IDs for Network Access Providers are unique to each operator and managed by the IEEE Standards Association. For more information, refer to https://standards.ieee.org/develop/regauth/bopid/.

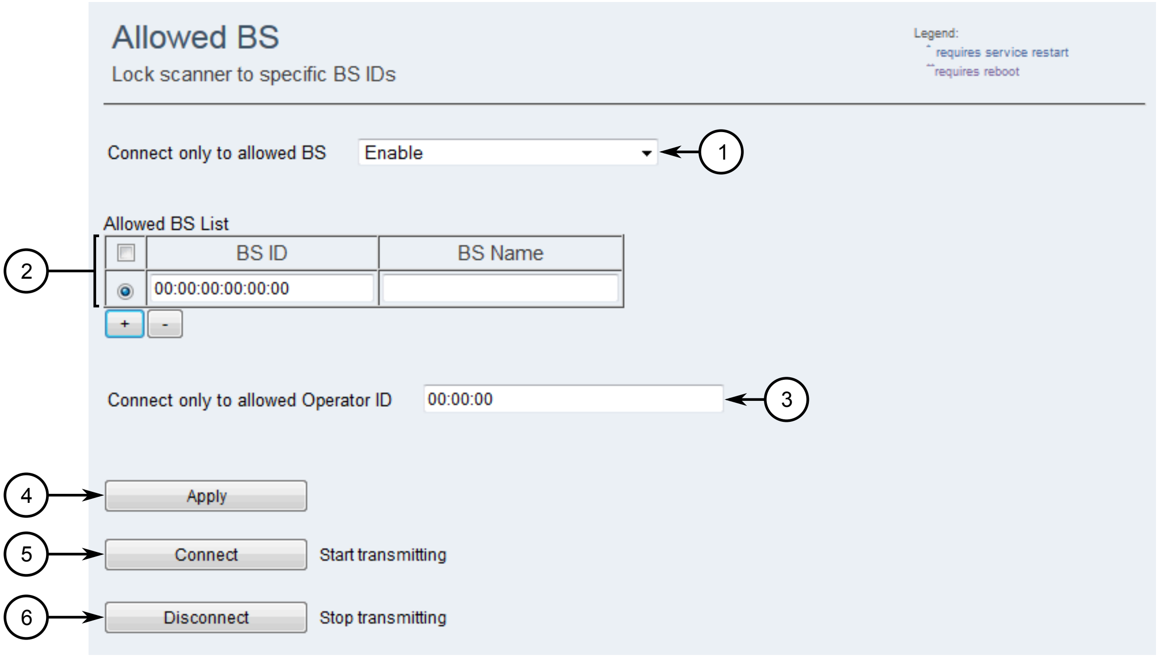
4. Add one or more base stations to the **Allowed BS List** table. For more information, refer to Section 8.3.6, “Defining Allowed Base Stations”.

Section 8.3.6

Defining Allowed Base Stations

To define an allowed base station, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Allowed BS***. The **Allowed BS** screen appears.



Allowed BS

Lock scanner to specific BS IDs

Legend:
* requires service restart
** requires reboot

Connect only to allowed BS: Enable

Allowed BS List

□	BS ID	BS Name
●	00:00:00:00:00:00	

Connect only to allowed Operator ID: 00:00:00

Figure 54: Allowed BS Screen

1. Connect Only to Allowed BS List **2.** Allowed BS List Table **3.** Connect Only to Allowed Operator ID Box **4.** Apply Button **5.** Connect Button **6.** Disconnect Button

IMPORTANT!
*Do not make changes to the **Allowed BS List** table if the subscriber station is in scanning mode. Click **Disconnect** before adding base stations.*

CAUTION!
*Configuration hazard – risk of losing the connection with current base station. Do not click **Disconnect** if using the RF Interface. The subscriber station will stop transmitting and lose its connection to the serving base station. A hard reset (shutting down and then powering up) or a site visit will be required to reboot the device.*

2. If connecting to the subscriber station directly or if the subscriber station is in scanning mode, click **Disconnect**.
3. Click +. A new row appears in the **Allowed BS List** table.
4. Configure the following parameters for the new base station:

Parameter	Description
BS ID	**Synopsis:** A 24-bit number **Default:** 00:00:00 The ID for the base station.
BS Name	**Synopsis:** A string The name assigned to the base station name.

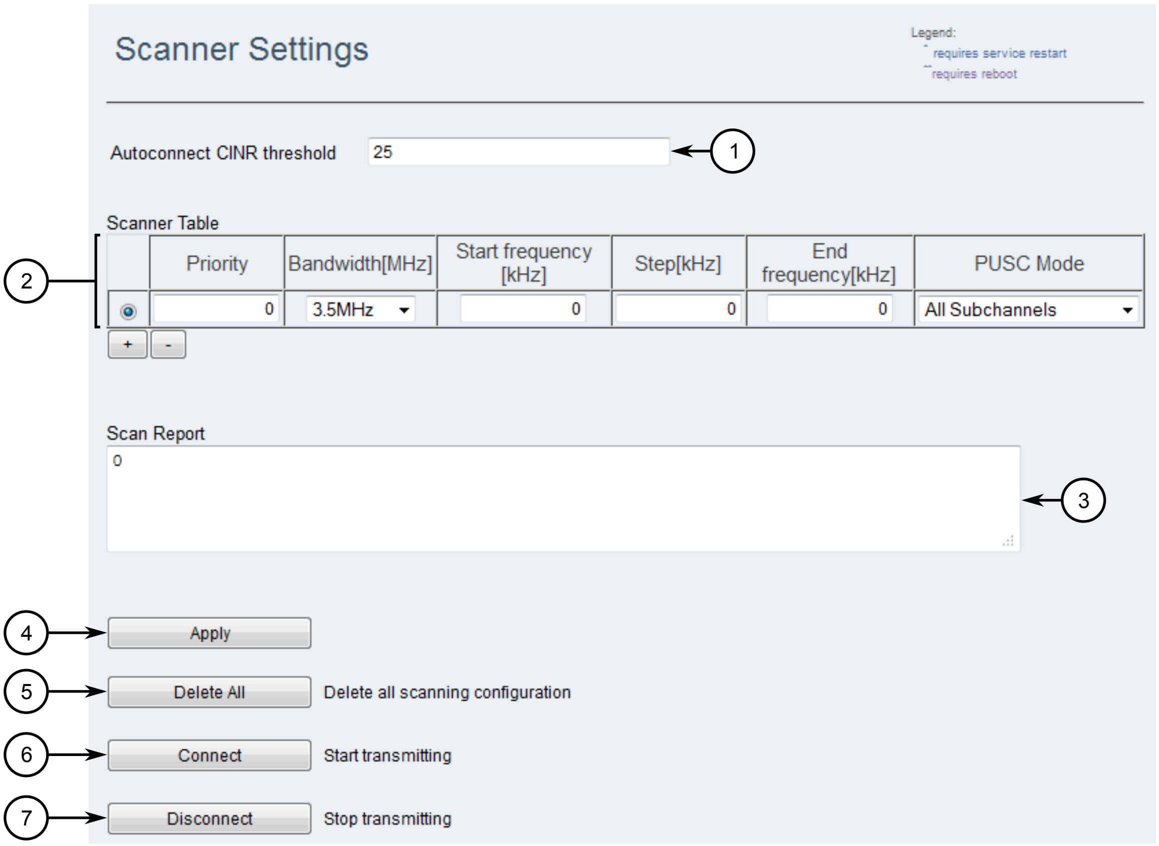
5. Click **Apply**.

Section 8.3.7

Initiating the Scan

To initiate the scanning process, do the following:

1. Navigate to ***WiMAX » Scanner Settings » Scanner Settings***. The **Scanner Settings** screen appears.



Scanner Settings

Legend:
* requires service restart
** requires reboot

Autoconnect CINR threshold: 25

Scanner Table

	Priority	Bandwidth[MHz]	Start frequency [kHz]	Step[kHz]	End frequency[kHz]	PUSC Mode
◉	0	3.5MHz	0	0	0	All Subchannels

Scan Report
0

Apply

Delete All — Delete all scanning configuration

Connect — Start transmitting

Disconnect — Stop transmitting

Figure 55: Scanner Settings Screen

1. Autocorrect CINR Threshold Box **2.** Frequencies **3.** Scan Report **4.** Apply Button **5.** Delete All Button **6.** Connect Button **7.** Disconnect Button

> **CAUTION!**
> *Configuration hazard – risk of losing the connection with current base station. Do not click **Disconnect** if using the RF Interface. The subscriber station will stop transmitting and lose its connection to the serving base station. A hard reset (shutting down and then powering up) or a site visit will be required to reboot the device.*

2. If the subscriber station is already connected to a base station, click **Disconnect**.
3. Click **Connect**. The subscriber station begins scanning for base stations that match the defined criteria.

   When the scan is complete, the following information is displayed under **Scan Report** for each base station found:

   - `BS ID` – The base station identifier
   - `Freq` – The frequency measured in kilohertz (kHz) on which the base station is operating
   - `Band` – The bandwidth measured in megahertz (MHz) on which the base station is operating
   - `Preamble` – The preamble index advertised by the base station
   - `CINR R1` – The base station's downlink CINR (Carrier to Interference and Noise Ratio) in decibels (dB)
   - `RSSI` – The base station's downlink RSSI (Received Signal Strength Indication)

Section 8.4

Managing Handover

This section describes how to configure the subscriber station to participate in the automatic handover process. If the serving base station advertises a list of neighboring base stations, the subscriber station will automatically connect to one of them when it needs to disconnect from its current base station.

NOTE
*If experiencing problems migrating the subscriber station to a target base station, contact Siemens Customer Support to discuss troubleshooting steps, such as enabling **Fast Network Entry**.*

CONTENTS

Section 8.4.1

Understanding Handover

Handover is a technique for making sure each subscriber station is served by the base station with the best signal strength and quality. It makes sure that when a subscriber station needs to transition from its current Serving Base Station (SBS) to a Target Base Station (TBS) it is able to do so with as little disruption to the wireless service as possible.

Handover is necessary when the signal strength (RSSI) is weak, the signal quality (CINR) is poor, or the time between respones (RTD) is too long. Specific thresholds for each can be defined using Downlink Channel Descriptor (DCD) triggers, which can initiate the handover process automatically. Specific subscriber stations can also be handed over manually when needed to another base station, referred to as a *neighboring* base station.

There are different handover techniques:

- **Controlled Handover**
  Consists of an action phase and prepration phase.
- **Uncontrolled Handover**
  Consists of an action phase and a limited prepration phase.
- **Unpredictive Handover**
  Consists of an action phase only.

RUGGEDCOM WIN allows for handover to take place between base stations with different central frequencies (referred to as *Inter-Frequncy Handover*) using the Unpredictive Handover technique.

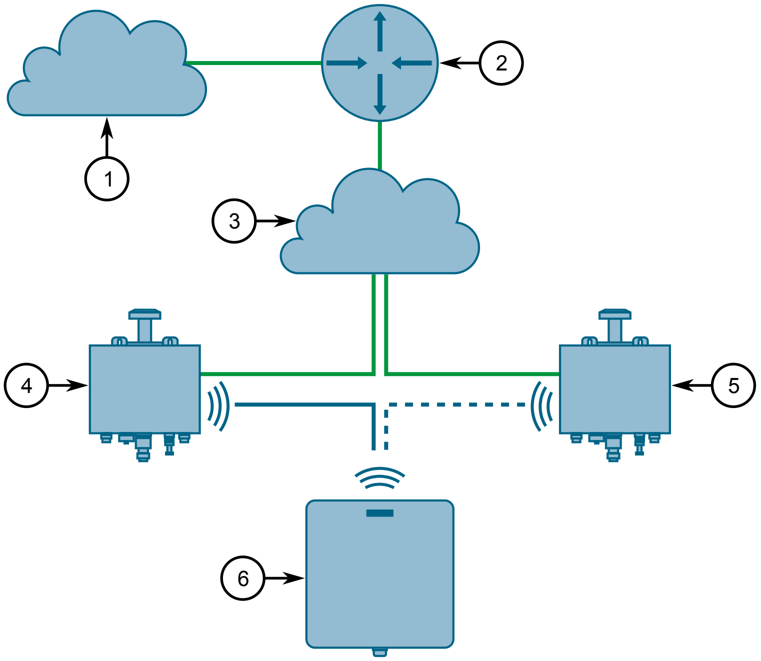


Figure 56: Inter-Frequency Handover Using the Unpredictive Handover Technique

1. Internet **2.** ASN Gateway **3.** R6/R8 Network **4.** Serving Base Station (Current) **5.** Target Base Station (Neighbor) **6.** Subscriber Station

Section 8.4.2

Configuring Handover

To configure the handover feature, do the following:

1. Enable **Failover BS Support**. For more information, refer to Section 8.4.3, "Configuring Failover BS Support".
2. Enable **Allow NBR Scanning**. For more information, refer to Section 8.4.4, "Enabling Neighbor Scanning".
3. [Optional] Set the scan duration. For more information, refer to Section 8.4.5, "Configuring Scan Duration".

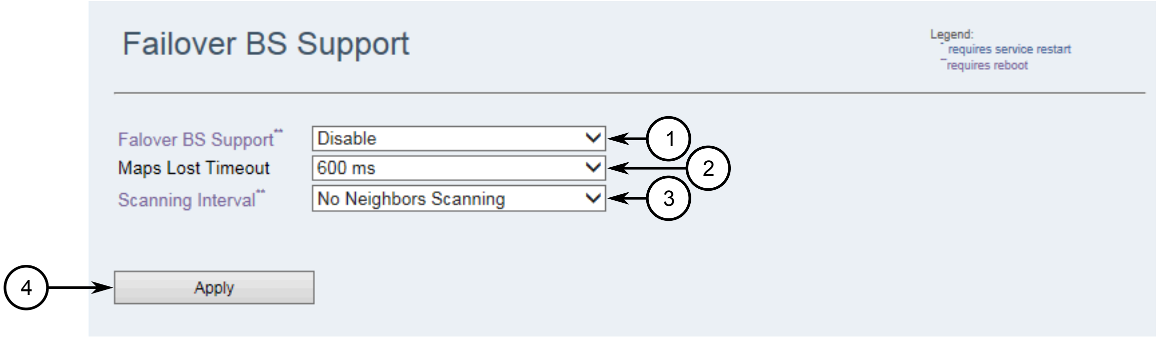
Section 8.4.3

Configuring Failover BS Support

Failover BS Support is the underlying feature that allows the subscriber station to participate in the handover process. It makes sure the subscriber station is aware of neighboring base stations available to it in case it needs to disconnect from the serving base station.

To enable and configure *Failover BS Support*, do the following:

1. Navigate to ***WiMAX » Mobility » Failover BS Support***. The **Failover BS Support** screen appears.



Failover BS Support

Legend:
* requires service restart
** requires reboot

Falover BS Support** Disable

Maps Lost Timeout 600 ms

Scanning Interval** No Neighbors Scanning

Figure 57: Failover BS Support Screen

1. Failover BS Support **2.** Maps Lost Timeout **3.** Scanning Interval **4.** Apply Button

2. Under **Failover BS Support**, select `Enable`.
3. Configure the following parameters:

Parameter	Description
Maps Lost Timeout	**Synopsis:** { 100, 600, 5000 } The time in milliseconds (ms) to wait after losing the WiMAX map before connecting to one of the neighboring base stations previously scanned from the *Neighbor BS* table.
Scanning Interval	**Synopsis:** { 1, 5, 60 } The time in minutes (min) to wait after de-registering from the serving base station before scanning for a new base station.

4. Click **Apply**.

Section 8.4.4

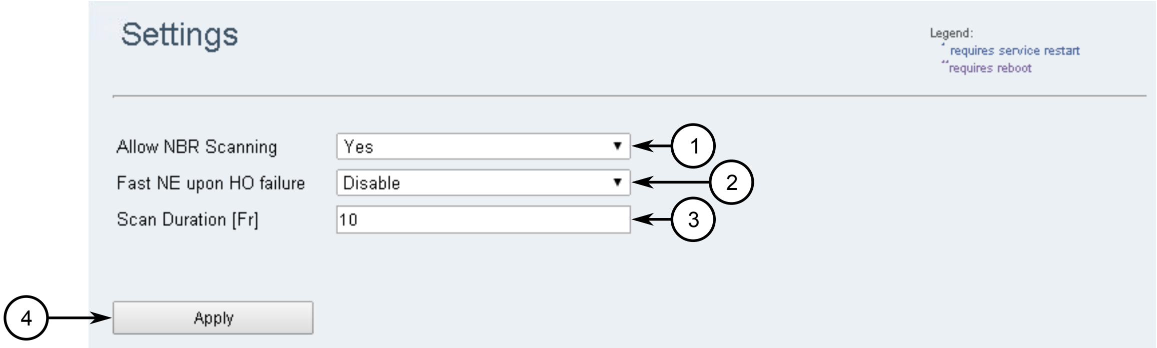
Enabling Neighbor Scanning

For the subscriber station to participate in the handover process, **Allow NBR Scanning** must be enabled. This setting enables the subscriber station to utilize the list of neighboring base stations broadcast by the serving base station. If the subscriber station needs to connect to another base station, it will scan only the neighboring base stations listed.

If **Allow NBR Scanning** is disabled, the subscriber station will not participate in the handover process. It will not scan for other base stations and stay connected to only the current serving base station.

To configure neighbor scanning, do the following:

1. Navigate to ***WiMAX » Mobility » Settings***. The **Settings** screen appears.



Settings

Legend:
* requires service restart
** requires reboot

Allow NBR Scanning: Yes
Fast NE upon HO failure: Disable
Scan Duration [Fr]: 10

Figure 58: Settings Screen

1. Allow NBR Scanning List **2.** Fast NE Upon HO Failure List **3.** Scan Duration Box **4.** Apply Button

2. Under **Allow NBR Scanning**, select one of the following options:
   - `Yes` – The subscriber station will scan the serving base station's neighbors when needed
   - `No` – The subscriber station will not scan the serving base station's neighbors when needed
3. Click **Apply**.

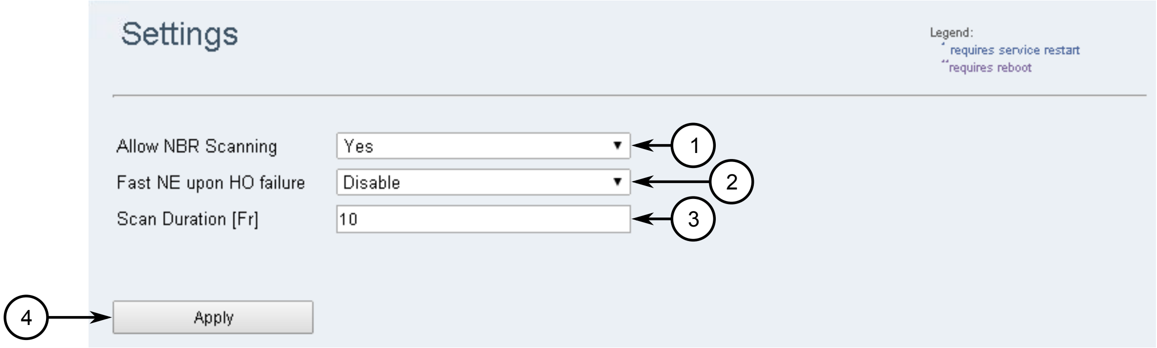
Section 8.4.5

Configuring Scan Duration

The scan duration determines how much time the subscriber station takes to find a suitable base station from the list of neighboring base stations broadcast by the serving base station. Increasing the scan duration allows the subscriber station to scan more candidates. This can be useful in multi-neighbor setups when handovers are often unsuccssful.

To configure the scan duration, do the following:

1. Navigate to ***WiMAX » Mobility » Settings***. The **Settings** screen appears.



Settings

Legend:
* requires service restart
** requires reboot

Allow NBR Scanning: Yes
Fast NE upon HO failure: Disable
Scan Duration [Fr]: 10

Figure 59: Settings Screen

1. Allow NBR Scanning List **2.** Fast NE Upon HO Failure List **3.** Scan Duration Box **4.** Apply Button

NOTE
Values less than 10 are for debugging purposes only. For more information, contact Siemens Customer Support.

2. Under **Scan Duration**, enter the desired scan duration. The duration can be between 3 and 255 milliseconds (ms). The default is 10 milliseconds.
3. Click **Apply**.

Section 8.4.6

Enabling/Disabling Fast Network Entry for Successive Handover Failures

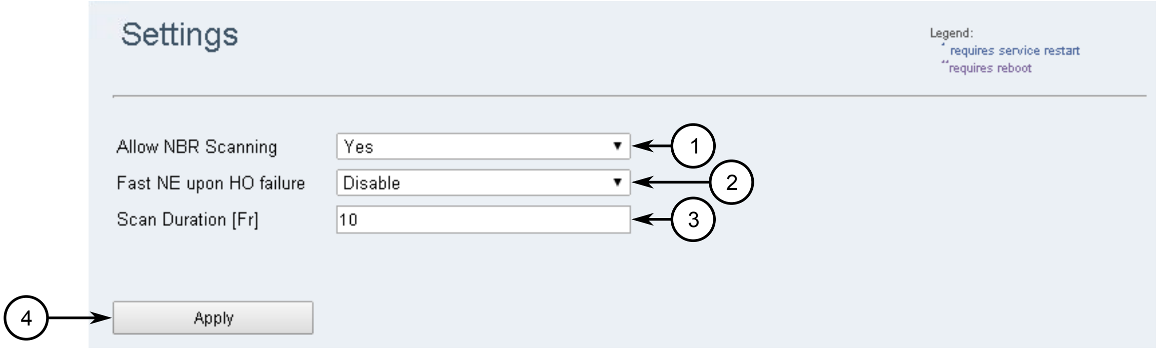
Following consecutive handover failures, consider enabling *Fast Network Entry*. This feature forces the subscriber station to connect with its target base station and fully enter the network.

IMPORTANT!
This feature is for debugging purposes only.

CAUTION!
Data Loss Hazard – risk of packet loss. Only enable ***Fast Network Entry*** *when specifically instructed to by Siemens Customer Support.*

To enable or disable *Fast Network Entry*, do the following:

1. Navigate to ***WiMAX » Mobility » Settings***. The **Settings** screen appears.



Settings

Legend:
* requires service restart
** requires reboot

Allow NBR Scanning: Yes
Fast NE upon HO failure: Disable
Scan Duration [Fr]: 10

Figure 60: Settings Screen

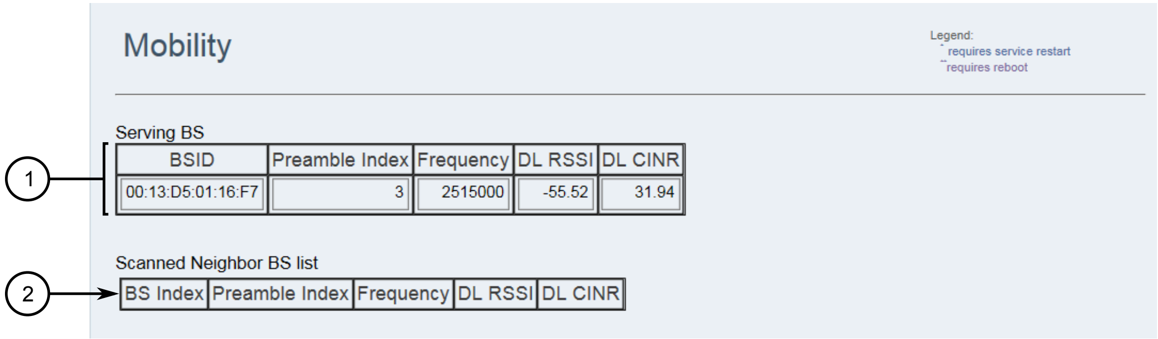
1. Allow NBR Scanning List **2.** Fast NE Upon HO Failure List **3.** Scan Duration Box **4.** Apply Button

2. In the **Fast NE upon HO failure** list, select **Enable** or **Disable**.
3. Click **Apply**.

Section 8.5

Viewing Base Station Information

To view information about the base station serving the subscriber station and its neighboring base stations, navigate to ***WiMAX » Mobility » Mobility***. The **Mobility** screen appears.



Mobility

Legend:
* requires service restart
** requires reboot

Serving BS

BSID	Preamble Index	Frequency	DL RSSI	DL CINR
00:13:D5:01:16:F7	3	2515000	-55.52	31.94

Scanned Neighbor BS list

BS Index	Preamble Index	Frequency	DL RSSI	DL CINR

Figure 61: Mobility Screen

1. Serving Base Station **2.** Neighboring Base Stations

The **Serving BS** table provides information about the serving base station, while the **Scanned Neighbor BS List** table provides the information broadcast by the serving base station about its neighboring base stations. Both tables provide the following information:

Column	Description
BSID	The MAC address of the base station.
Preamble Index	The base station’s preamble index.
Frequency	The frequency in hertz (Hz) on which the base station operates.
DL RSSI	The downlink RSSI (Received Signal Strength Indication).
DL CINR	The downlink CINR (Carrier to Interference and Noise Ratio) in decibels (dB).

9 Traffic Control

This chapter describes how to configure and manage features that control incoming and outgoing traffic.

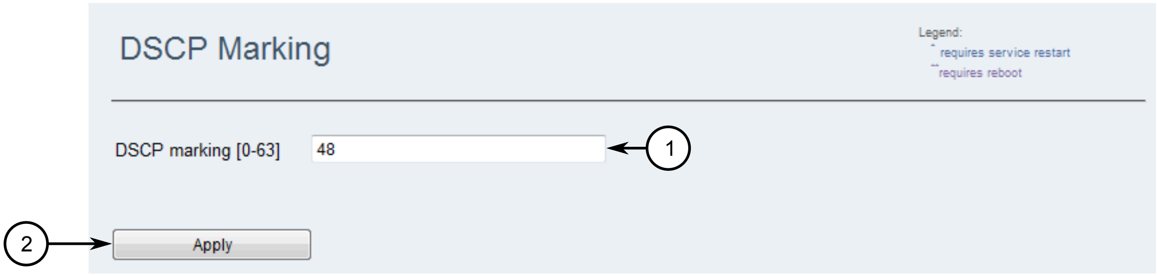
CONTENTS

Section 9.1

Configuring DSCP Marking

To configure Differentiated Services Code Point (DSCP) marking (identified outgoing management traffic), do the following:

1. Navigate to ***Management » Remote Management » DSCP Marking***. The **DSCP Marking** screen appears.



DSCP Marking

Legend:
* requires service restart
** requires reboot

DSCP marking [0-63] 48

Figure 62: DSCP Marking Screen

1. DSCP Marking Box **2.** Apply Button

2. Under **DSCP marking [0-63]**, enter a number between 0 and 63. The default value is 48.
3. Click **Apply**.

Section 9.2

Managing VLANs

This section describes how to configure and manage Virtual Local Area Networks (VLANs).

CONTENTS

- Section 9.2.2, "Configuring VLAN Tagging"

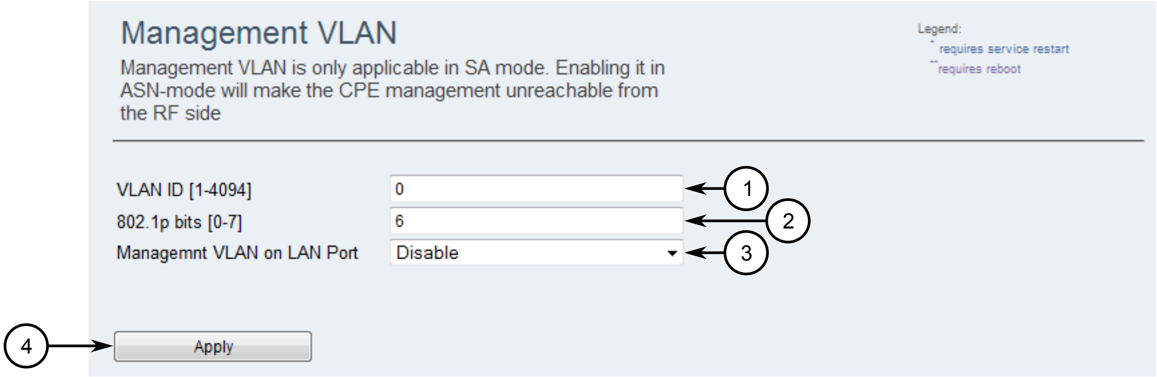
Section 9.2.1

Configuring the Management VLAN

The Management VLAN acts as a channel between the serving base station and its registered subscriber stations, allowing for the exchange of management frames. When configured, outgoing management frames are tagged with an ID and IEEE 802.1p priority value. Incoming management frames must be tagged with the same values or they are dropped by the subscriber station.

To configure the management VLAN, do the following:

1. Navigate to ***Management » Remote Management » Management VLAN***. The **Management VLAN** screen appears.



Management VLAN

Management VLAN is only applicable in SA mode. Enabling it in ASN-mode will make the CPE management unreachable from the RF side

Legend:
* requires service restart
** requires reboot

VLAN ID [1-4094]: 0
802.1p bits [0-7]: 6
Managemnt VLAN on LAN Port: Disable

Figure 63: Management VLAN Screen

1. VLAN ID Box **2.** 802.1p Bits Box **3.** Management VLAN on LAN Port List **4.** Apply Button

2. Configure the following parameters:

Parameter	Description
VLAN ID	**Synopsis:** An integer between 1 and 4094 **Default:** 0 The VLAN ID tagged assigned to incoming and outgoing management frames.
802.1p bits	**Synopsis:** An integer between 0 and 7 **Default:** 6 The 802.1p priority tag assigned to incoming and outgoing management frames.
Management VLAN on LAN Port	**Synopsis:** { Enable, Disable } **Default:** Disable Enables or disables the Management VLAN on the LAN port.

3. Click **Apply**.

Section 9.2.2

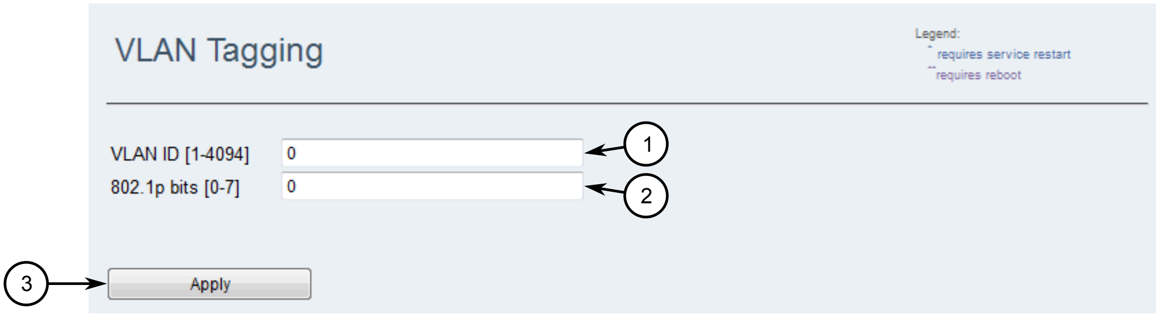
Configuring VLAN Tagging

Configure VLAN tagging to assign a VLAN ID and IEEE 802.1p priority to all outgoing data packets. The same tagging will be used to authenticate incoming data packets. Incoming data packets that do not have the same ID and priority tags are dropped.

> **NOTE**
> *The subscriber station is able to tag or untag data packets with a VLAN ID when there is no switch behind the device to carryout this function. This is only viable when there is only on VLAN. If there is more than one VLAN, connect a switch to the subscriber station to tag and untag data packets.*

To configure VLAN tagging, do the following:

1. Navigate to ***Network » Ethernet Settings***. The **VLAN Tagging** screen appears.



VLAN Tagging

VLAN ID [1-4094] 0

802.1p bits [0-7] 0

Figure 64: VLAN Tagging Screen

1. VLAN ID **2.** 802.1p Bits Box **3.** Apply Button

2. Configure the following parameter(s) as required:

Parameter	Description
VLAN ID	**Synopsis:** An integer between 1 and 4094 **Default:** 0 The VLAN ID tagged assigned to incoming and outgoing data packets.
802.1p bits	**Synopsis:** An integer between 0 and 7 **Default:** 6 The 802.1p priority tag assigned to incoming and outgoing data packets.

3. Click **Apply**.

10 Network Discovery and Management

This section describes how to configure and manage network discovery features.

CONTENTS

Section 10.1

Managing SNMP

The Simple Network Management Protocol (SNMP) is used by network management systems and the devices they manage. It is used to report alarm conditions and other events that occur on the devices it manages.

RUGGEDCOM WIN supports SNMPv2 and SNMPv3, which offer the following features:

- Provides the ability to send a notification of an event via *traps*. Traps are unacknowledged UDP messages and may be lost in transit.
- Provides the ability to notify via *informs*. Informs simply add acknowledgment to the trap process, resending the trap if it is not acknowledged in a timely fashion.
- Encrypts all data transmitted by scrambling the contents of each packet to prevent it from being seen by an unauthorized source. The AES CFB 128 and DES3 encryption protocols are supported.
- Authenticates all messages to verify they are from a valid source.
- Verifies the integrity of each message by making sure each packet has not been tampered with in-transit.

SNMPv3 also provides security models and security levels. A security model is an authentication strategy that is set up for a user and the group in which the user resides. A security level is a permitted level of security within a security model. A combination of a security model and security level will determine which security mechanism is employed when handling an SNMP packet.

Before configuring SNMP, note the following:

- Each user belongs to a group
- A group defines the access policy for a set of users
- An access policy defines what SNMP objects can be accessed for: reading, writing and creating notifications
- A group determines the list of notifications its users can receive
- A group defines the security model and security level for its users

CONTENTS

Section 10.1.1

Configuring SNMP

To configure SNMP, do the following:

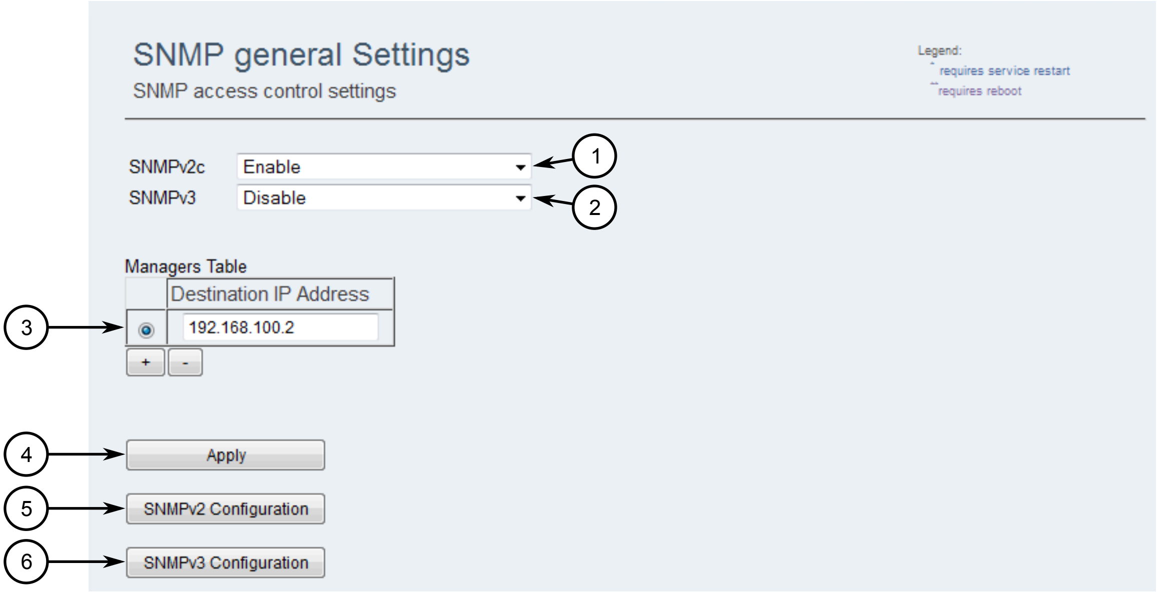
1. Enable and configure either SNMPv2 or SNMPv3. For more information, refer to either Section 10.1.2, “Configuring SNMPv2” or Section 10.1.3, “Configuring SNMPv3”.
2. Enable the required SNMP traps. For more information, refer to Section 10.1.4.1, “Enabling/Disabling SNMP Traps”.
3. Configure one or more trap destinations (up to a maximum of five). For more Information, refer to Section 10.1.4.3, “Configuring SNMP Trap Destinations”.
4. Configure the system contact and location information for the subscriber station. For more Information, refer to Section 10.1.6, “Configuring the SNMP System Group”.

Section 10.1.2

Configuring SNMPv2

To configure the SNMPv2c parameters, do the following:

1. Navigate to ***Management » SNMP***. The **SNMP General Settings** screen appears.



SNMP general Settings

SNMP access control settings

SNMPv2c: Enable

SNMPv3: Disable

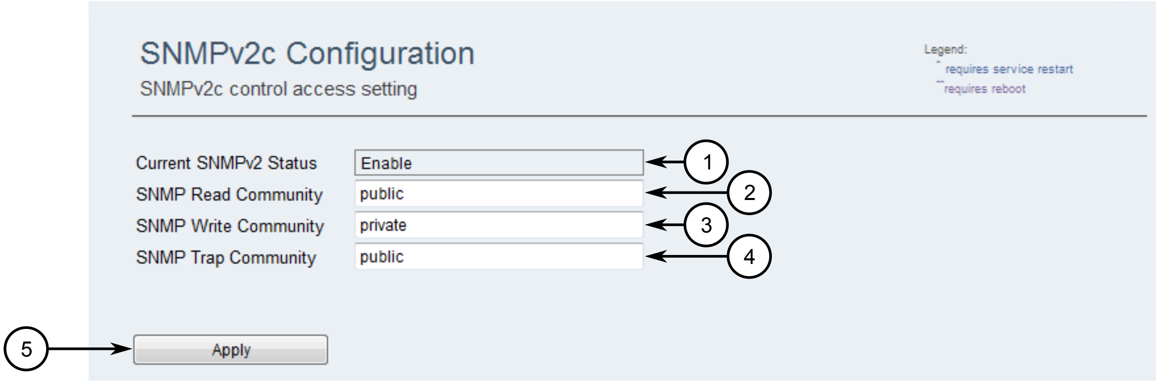
Managers Table

	Destination IP Address
●	192.168.100.2

Figure 65: SNMP General Settings Screen

1. SNMPv2c List **2.** SNMPv3 List **3.** Trap Destinations **4.** Apply Button **5.** SNMPv2 Configuration Button **6.** SNMPv3 Configuration Button

2. Under **SNMPv2c**, select `Enable`.
3. Click **SNMPv2 Configuration**. The **SNMPv2c Configuration** screen appears.



SNMPv2c Configuration

SNMPv2c control access setting

Current SNMPv2 Status: Enable

SNMP Read Community: public

SNMP Write Community: private

SNMP Trap Community: public

Figure 66: SNMPv2c Configuration Screen

1. Current SNMPv2c Status **2.** SNMP Read Community **3.** SNMP Write Community **4.** SNMP Trap Community **5.** Apply Button

4. Configure the following parameters:

> **IMPORTANT!**
> *The **SNMP Read Community** and **SNMP Write Community** values must be unique.*

Parameter	Description
SNMP Read Community	**Synopsis:** A string **Default:** public The SNMP community name for read access. This name can be used as a password for secure information retrieval.
SNMP Write Community	**Synopsis:** A string **Default:** private The SNMP community name for write access. This name can be used as a password for secure set commands.
SNMP Trap Community	**Synopsis:** A string **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.

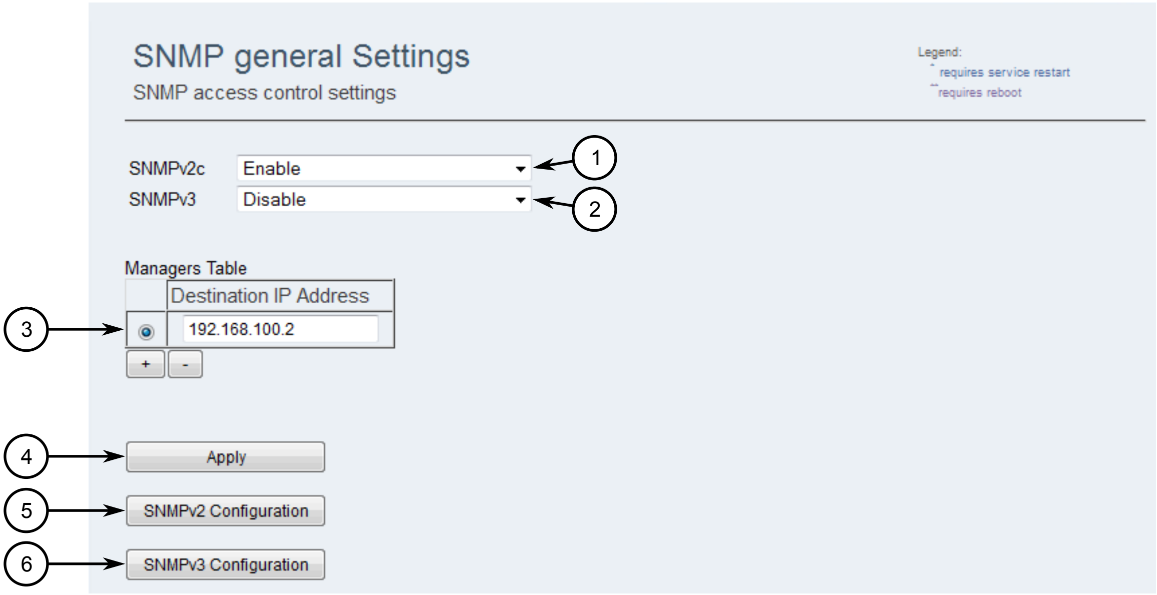
5. Click **Apply**.

Section 10.1.3

Configuring SNMPv3

To configure the SNMPv3 parameters, do the following:

1. Navigate to ***Management » SNMP***. The **SNMP General Settings** screen appears.



SNMP general Settings
SNMP access control settings

Legend:
* requires service restart
** requires reboot

SNMPv2c: Enable
SNMPv3: Disable

Managers Table

	Destination IP Address
●	192.168.100.2

Figure 67: SNMP General Settings Screen

1. SNMPv2c List **2.** SNMPv3 List **3.** Trap Destinations **4.** Apply Button **5.** SNMPv2 Configuration Button **6.** SNMPv3 Configuration Button

2. Under **SNMPv3**, select `Enable`.

3. Configure one or more SNMP users. For more information, refer to Section 10.1.5, “Configuring Users for SNMPv3”.
4. Click **Apply**.

Section 10.1.4

Managing SNMP Traps

This section describes how to configure and manage SNMP Traps.

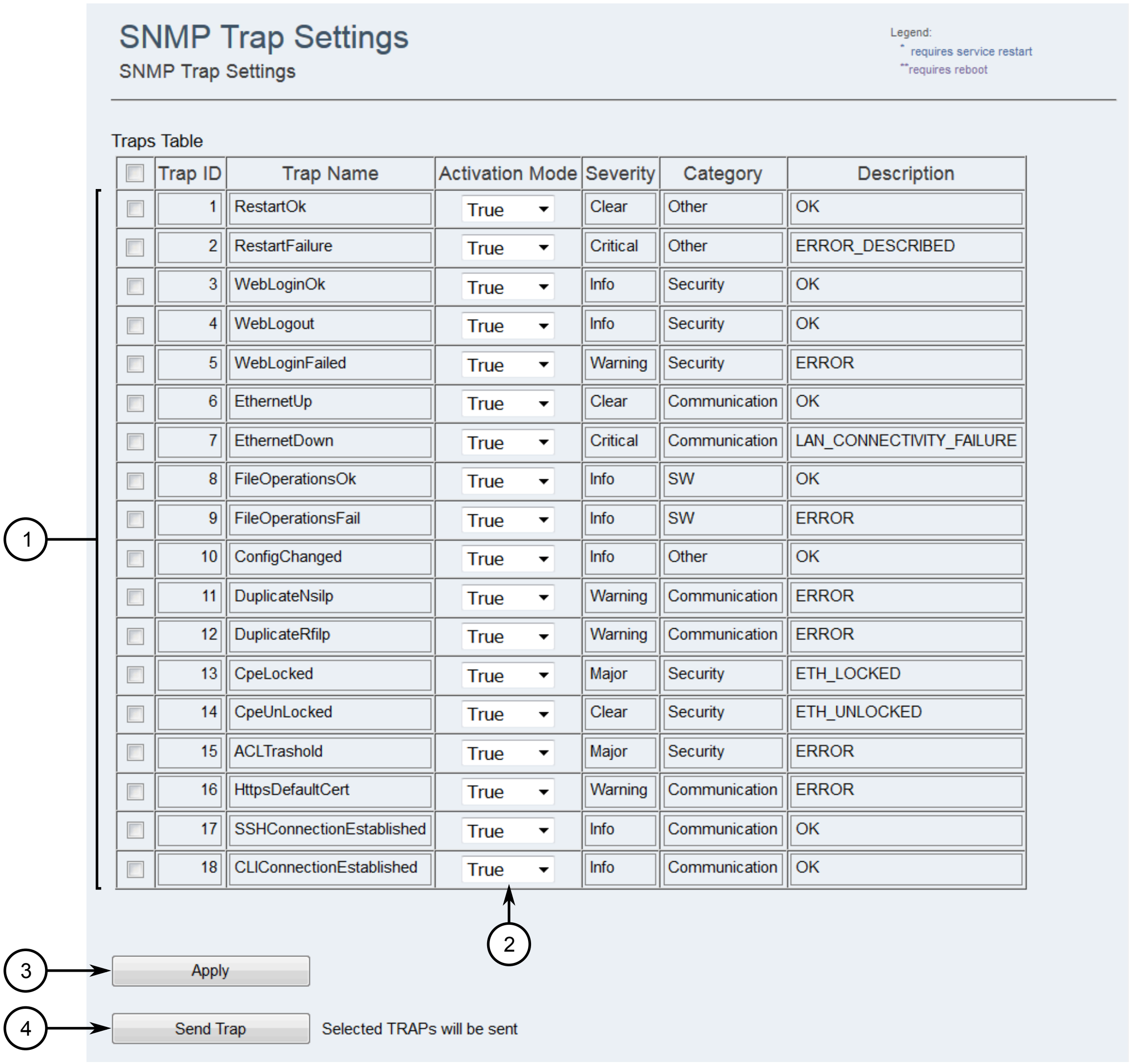
CONTENTS

Section 10.1.4.1

Enabling/Disabling SNMP Traps

To enable or disable an SNMP trap, do the following:

1. Navigate to ***Management » Alarms and Traps » Traps***. The **SNMP Trap Settings** screen appears.



SNMP Trap Settings

SNMP Trap Settings

Legend:
* requires service restart
** requires reboot

Traps Table

☐	Trap ID	Trap Name	Activation Mode	Severity	Category	Description
☐	1	RestartOk	True	Clear	Other	OK
☐	2	RestartFailure	True	Critical	Other	ERROR_DESCRIBED
☐	3	WebLoginOk	True	Info	Security	OK
☐	4	WebLogout	True	Info	Security	OK
☐	5	WebLoginFailed	True	Warning	Security	ERROR
☐	6	EthernetUp	True	Clear	Communication	OK
☐	7	EthernetDown	True	Critical	Communication	LAN_CONNECTIVITY_FAILURE
☐	8	FileOperationsOk	True	Info	SW	OK
☐	9	FileOperationsFail	True	Info	SW	ERROR
☐	10	ConfigChanged	True	Info	Other	OK
☐	11	DuplicateNsilp	True	Warning	Communication	ERROR
☐	12	DuplicateRfilp	True	Warning	Communication	ERROR
☐	13	CpeLocked	True	Major	Security	ETH_LOCKED
☐	14	CpeUnLocked	True	Clear	Security	ETH_UNLOCKED
☐	15	ACLTrashold	True	Major	Security	ERROR
☐	16	HttpsDefaultCert	True	Warning	Communication	ERROR
☐	17	SSHConnectionEstablished	True	Info	Communication	OK
☐	18	CLIConnectionEstablished	True	Info	Communication	OK

Selected TRAPs will be sent

Figure 68: SNMP Trap Settings

1. Available SNMP Traps **2.** Activation Mode List **3.** Apply Button **4.** Send Trap Button

2. Under **Activation Mode** for the selected SNMP trap, select `True` to enable the trap or `False` to disable the trap.
3. Click **Apply**.

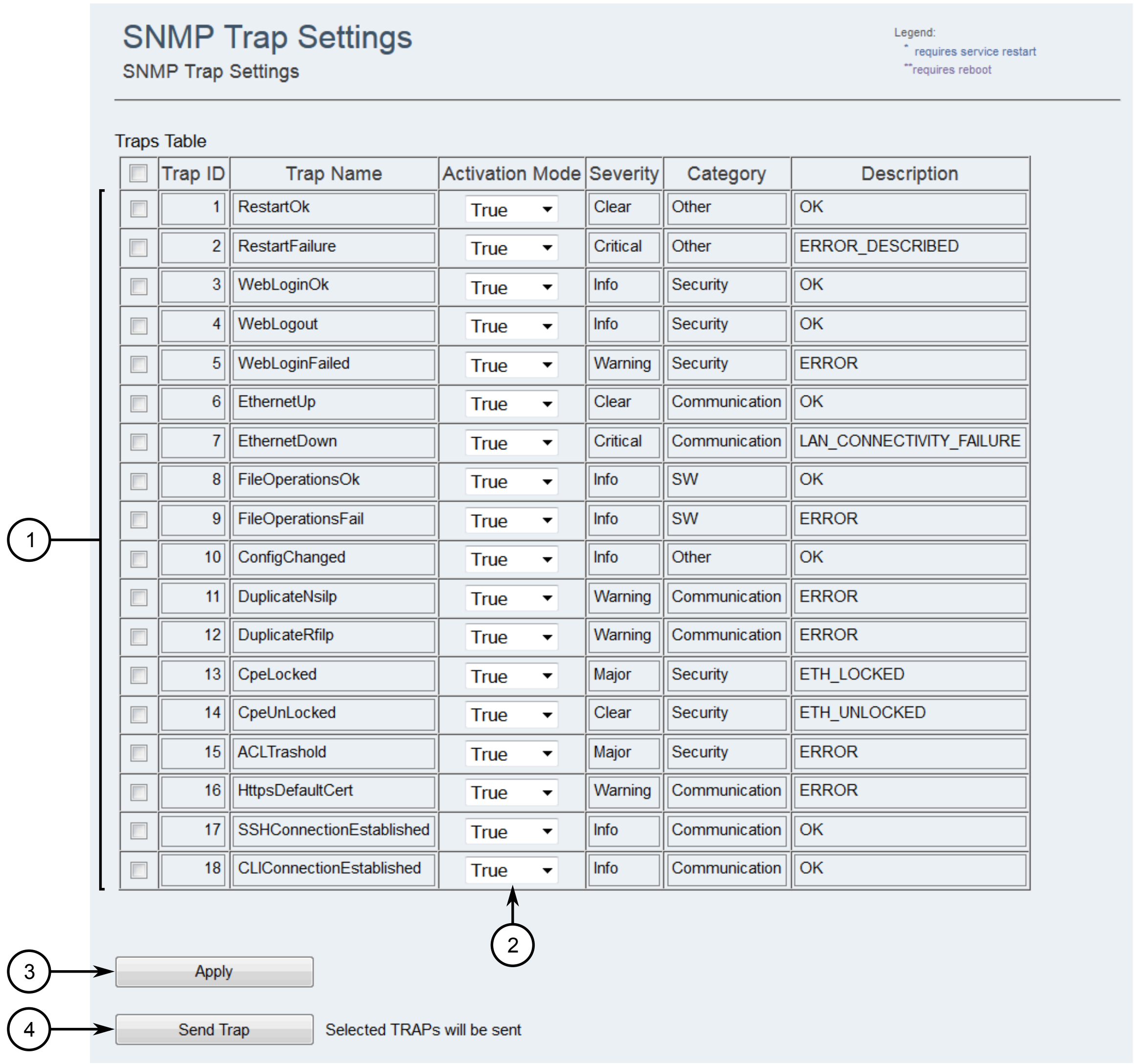
Section 10.1.4.2

Sending SNMP Traps

For testing purposes, selected SNMP traps can be sent on demand.

To send SNMP traps, do the following:

1. Navigate to ***Management » Alarms and Traps » Traps***. The **SNMP Trap Settings** screen appears.



SNMP Trap Settings

SNMP Trap Settings

Legend:
* requires service restart
**requires reboot

Traps Table

☐	Trap ID	Trap Name	Activation Mode	Severity	Category	Description
☐	1	RestartOk	True	Clear	Other	OK
☐	2	RestartFailure	True	Critical	Other	ERROR_DESCRIBED
☐	3	WebLoginOk	True	Info	Security	OK
☐	4	WebLogout	True	Info	Security	OK
☐	5	WebLoginFailed	True	Warning	Security	ERROR
☐	6	EthernetUp	True	Clear	Communication	OK
☐	7	EthernetDown	True	Critical	Communication	LAN_CONNECTIVITY_FAILURE
☐	8	FileOperationsOk	True	Info	SW	OK
☐	9	FileOperationsFail	True	Info	SW	ERROR
☐	10	ConfigChanged	True	Info	Other	OK
☐	11	DuplicateNsilp	True	Warning	Communication	ERROR
☐	12	DuplicateRfilp	True	Warning	Communication	ERROR
☐	13	CpeLocked	True	Major	Security	ETH_LOCKED
☐	14	CpeUnLocked	True	Clear	Security	ETH_UNLOCKED
☐	15	ACLTrashold	True	Major	Security	ERROR
☐	16	HttpsDefaultCert	True	Warning	Communication	ERROR
☐	17	SSHConnectionEstablished	True	Info	Communication	OK
☐	18	CLIConnectionEstablished	True	Info	Communication	OK

Selected TRAPs will be sent

Figure 69: SNMP Trap Settings Screen

1. Available SNMP Traps **2.** Activation Mode List **3.** Apply Button **4.** Send Trap Button

> **IMPORTANT!**
> *Only SNMP traps that have been enabled can be sent on demand.*

2. Select one or more SNMP traps.
3. Click **Send Trap**.

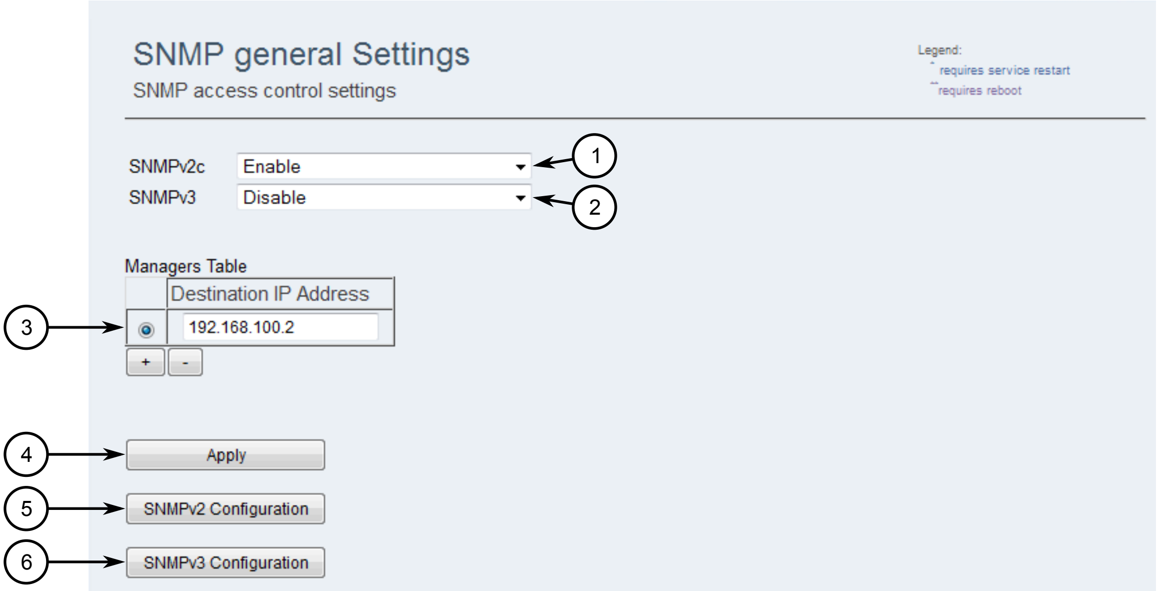
Section 10.1.4.3

Configuring SNMP Trap Destinations

Trap destinations represent SNMP trap receivers configured to receive SNMP traps and inform messages from a device. RUGGEDCOM WIN supports up to five trap destinations.

To configure a destination for SNMP traps, do the following:

1. Navigate to ***Management » SNMP***. The **SNMP General Settings** screen appears.



SNMP general Settings

SNMP access control settings

Legend:
* requires service restart
** requires reboot

SNMPv2c: Enable

SNMPv3: Disable

Managers Table

	Destination IP Address
●	192.168.100.2

Figure 70: SNMP General Settings Screen

1. SNMPv2c List **2.** SNMPv3 List **3.** Trap Destinations **4.** Apply Button **5.** SNMPv2 Configuration Button **6.** SNMPv3 Configuration Button

2. Under the **Managers Table**, click the **+** button. A new row is added to the table.
3. In the **Destination IP Address** column, enter the IP address of an SNMP server.
4. Click **Apply**.

Section 10.1.5

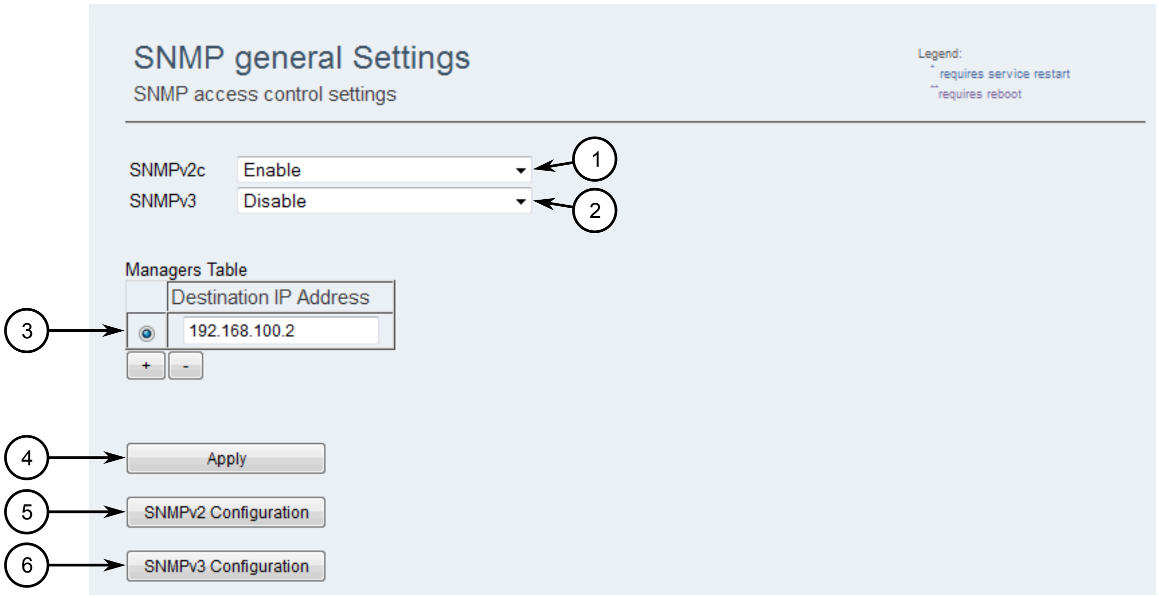
Configuring Users for SNMPv3

A user profile is required for each remote SNMP manager. The profile defines a unique user name, authentication and privacy information, and the associated SNMP access group. Once defined, all traps and inform message to and from the SNMP manager can be authenticated, encrypted and decrypted.

RUGGEDCOM WIN supports up to five user profies for SNMPv3.

To configure a user profile for SNMPv3, do the following:

1. Navigate to ***Management » SNMP***. The **SNMP General Settings** screen appears.



SNMP general Settings

SNMP access control settings

SNMPv2c: Enable

SNMPv3: Disable

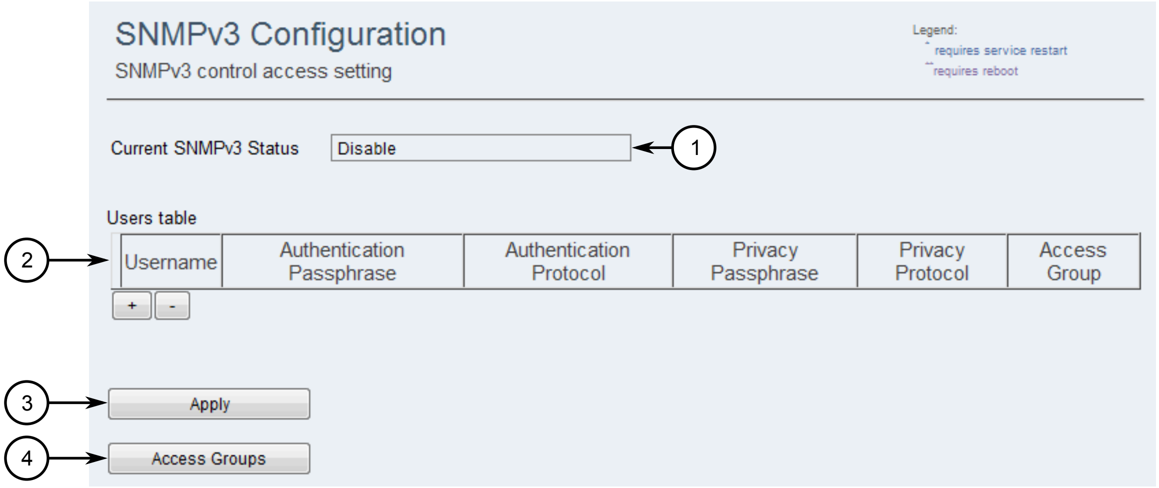
Managers Table

	Destination IP Address
●	192.168.100.2

Figure 71: SNMP General Settings Screen

1. SNMPv2c List **2.** SNMPv3 List **3.** Trap Destinations **4.** Apply Button **5.** SNMPv2 Configuration Button **6.** SNMPv3 Configuration Button

2. Click **SNMPv3 Configuration**. The **SNMPv3 Configuration** screen appears.



SNMPv3 Configuration

SNMPv3 control access setting

Current SNMPv3 Status: Disable

Users table

Username	Authentication Passphrase	Authentication Protocol	Privacy Passphrase	Privacy Protocol	Access Group

Figure 72: SNMPv3 Configuration Screen

1. Current SNMPv3 Status **2.** Users **3.** Apply Button **4.** Access Groups Button

3. Under the **Users Table**, click the **+** button. A new row is added to the table.
4. Configure the following parameters:

NOTE

It is recommended to use strong passphrases that meet the following criteria:

- *One lower case character*
- *One upper case character*
- *One number*
- *One special character (i.e. !@#$%^&*()_+-={}[];:',<>/?\|`~)*

Parameter	Description
Username	The user name.
Authentication Passphrase	The passphrase used to authenticate the user name.
Authentication Protocol	**Synopsis:** HMAC-SHA1 The authentication protocol used to authenticate the user name.
Privacy Passphrase	The passphrase used to decrypt communications with the SNMP trap receiver.
Privacy Protocol	**Synopsis:** CBC-DES The protocol used to encrypt/decrypt communications with the SNMP trap receiver.
Access Group	The SNMPv3 access group associated with the user name. For more information about available access groups, refer to Section 10.1.7, “Viewing SNMPv3 Access Groups”.

5. Click **Apply**.
6. Verify the new user by generating and sending a trap. For more information about sending a trap manually, refer to Section 10.1.4.2, “Sending SNMP Traps”.

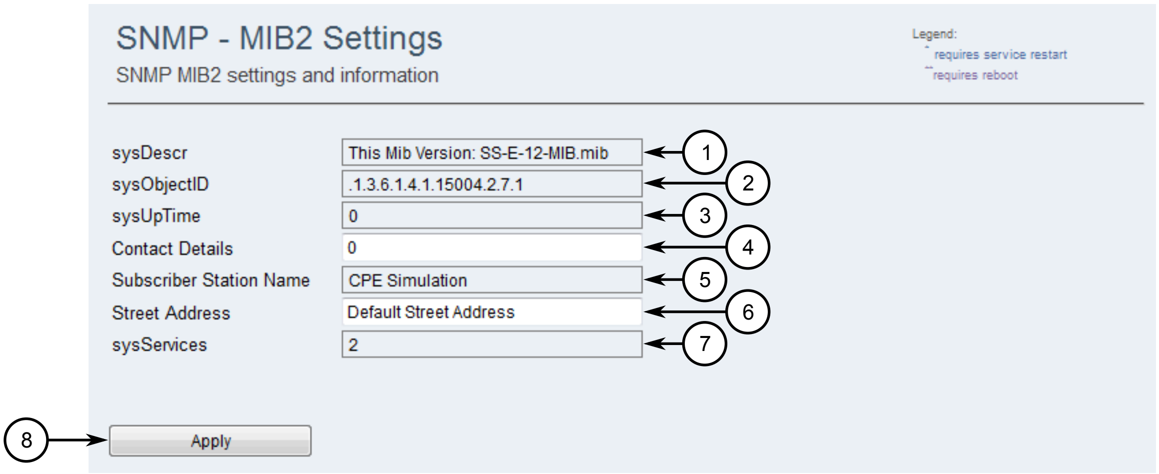
Section 10.1.6

Configuring the SNMP System Group

The SNMP system group provides information about the subscriber station's owner, identity and location. These details are added to the SNMP configuration file and can be accessed by SNMP trap receivers.

To configure the SNMP system group, do the following:

1. Navigate to ***Management » SNMP » MIB2 System***. The **SNMP - MIB2 Settings** screen appears.



SNMP - MIB2 Settings

SNMP MIB2 settings and information

Legend:
* requires service restart
** requires reboot

sysDescr: This Mib Version: SS-E-12-MIB.mib

sysObjectID: .1.3.6.1.4.1.15004.2.7.1

sysUpTime: 0

Contact Details: 0

Subscriber Station Name: CPE Simulation

Street Address: Default Street Address

sysServices: 2

Figure 73: SNMP - MIB2 Settings Screen

1. sysDescr **2.** sysObjectID **3.** sysUpTime **4.** Contact Details Box **5.** Subscriber Station Name **6.** Street Address Box **7.** sysServices **8.** Apply Button

2. Configure the following parameters:

Parameter	Description
Contact Details	**Synopsis:** A string 4 to 255 characters long The contact information including name and contact details.
Subscriber Station Name	**Synopsis:** A string 4 to 255 characters long The name assigned to the subscriber station.
Street Address	**Synopsis:** A string 4 to 255 characters long The street address where the subscriber station is located.

3. Click **Apply**.

Section 10.1.7

Viewing SNMPv3 Access Groups

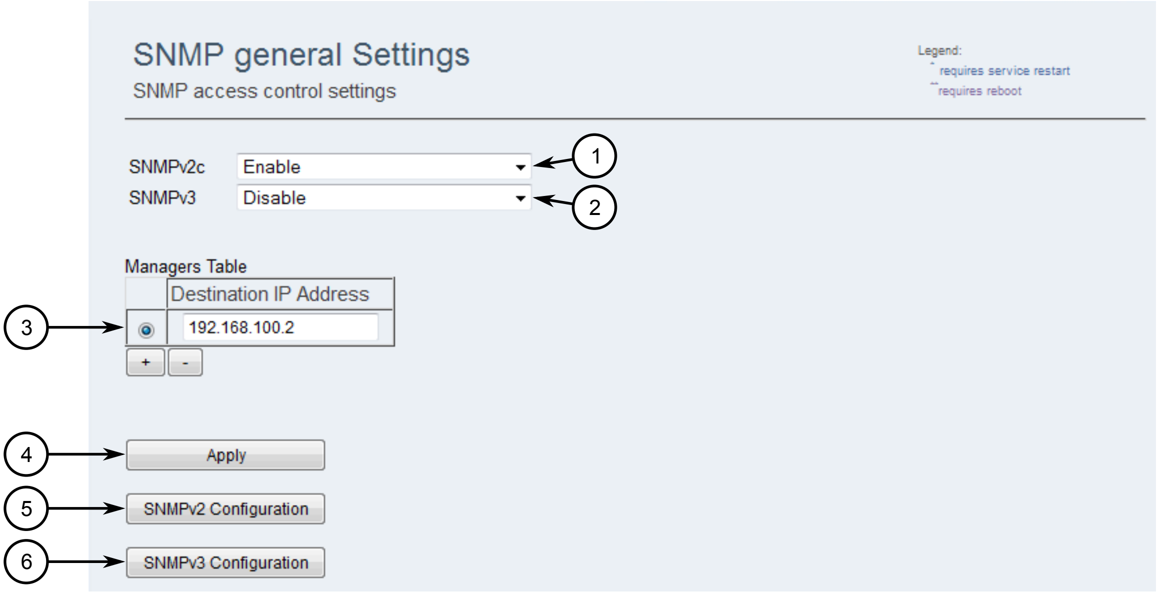
SNMPv3 access groups define authorization and access privileges for associated users. The following access groups are defined in RUGGEDCOM WIN:

Access Group	Read View	Write View	Notification View
NMS Access Group	Users can view and read all MIBs	User can create, modify and delete MIBs	Users can view and read all notification MIBs
Traps Only	Users cannot view or read MIBs	User cannot create, modify or delete MIBs	Users can view and read all notification MIBs

For convenience, these access group definitions are included in the user interface.

To view the available SNMPv3 access groups, do the following:

1. Navigate to ***Management » SNMP***. The **SNMP General Settings** screen appears.



SNMP general Settings

SNMP access control settings

SNMPv2c: Enable

SNMPv3: Disable

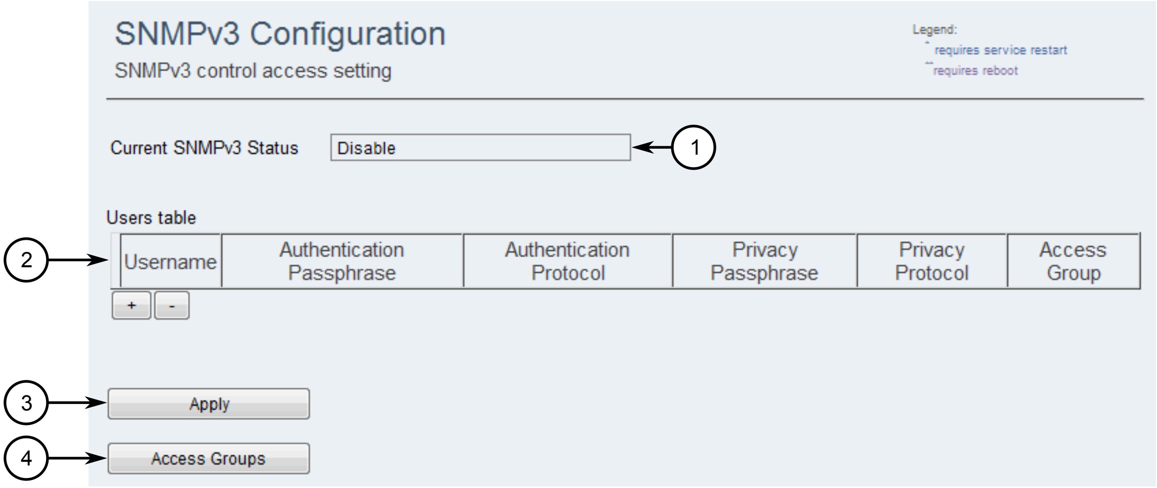
Managers Table

	Destination IP Address
●	192.168.100.2

Figure 74: SNMP General Settings Screen

1. SNMPv2c List **2.** SNMPv3 List **3.** Trap Destinations **4.** Apply Button **5.** SNMPv2 Configuration Button **6.** SNMPv3 Configuration Button

2. Click **SNMPv3 Configuration**. The **SNMPv3 Configuration** screen appears.



SNMPv3 Configuration

SNMPv3 control access setting

Current SNMPv3 Status: Disable

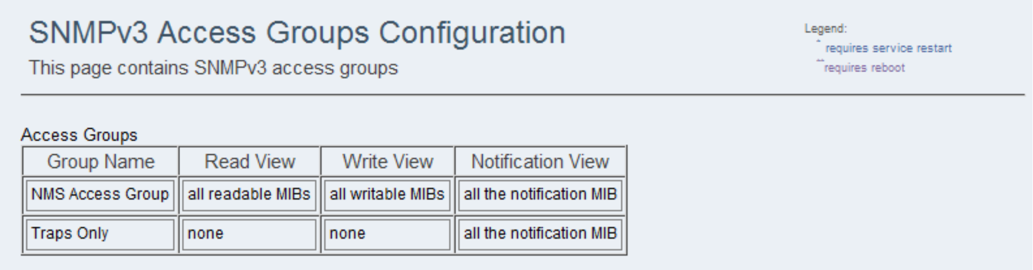
Users table

Username	Authentication Passphrase	Authentication Protocol	Privacy Passphrase	Privacy Protocol	Access Group

Figure 75: SNMPv3 Configuration Screen

1. Current SNMPv3 Status **2.** Users **3.** Apply Button **4.** Access Groups Button

3. Click **Access Groups**. The **SNMPv3 Access Groups Configuration** screen appears.



SNMPv3 Access Groups Configuration

This page contains SNMPv3 access groups

Legend:
* requires service restart
** requires reboot

Access Groups

Group Name	Read View	Write View	Notification View
NMS Access Group	all readable MIBs	all writable MIBs	all the notification MIB
Traps Only	none	none	all the notification MIB

Figure 76: SNMPv3 Access Groups Configuration Screen

Section 10.2

Managing MAC Addresses

This section describes how to configure and manage MAC addresses.

CONTENTS

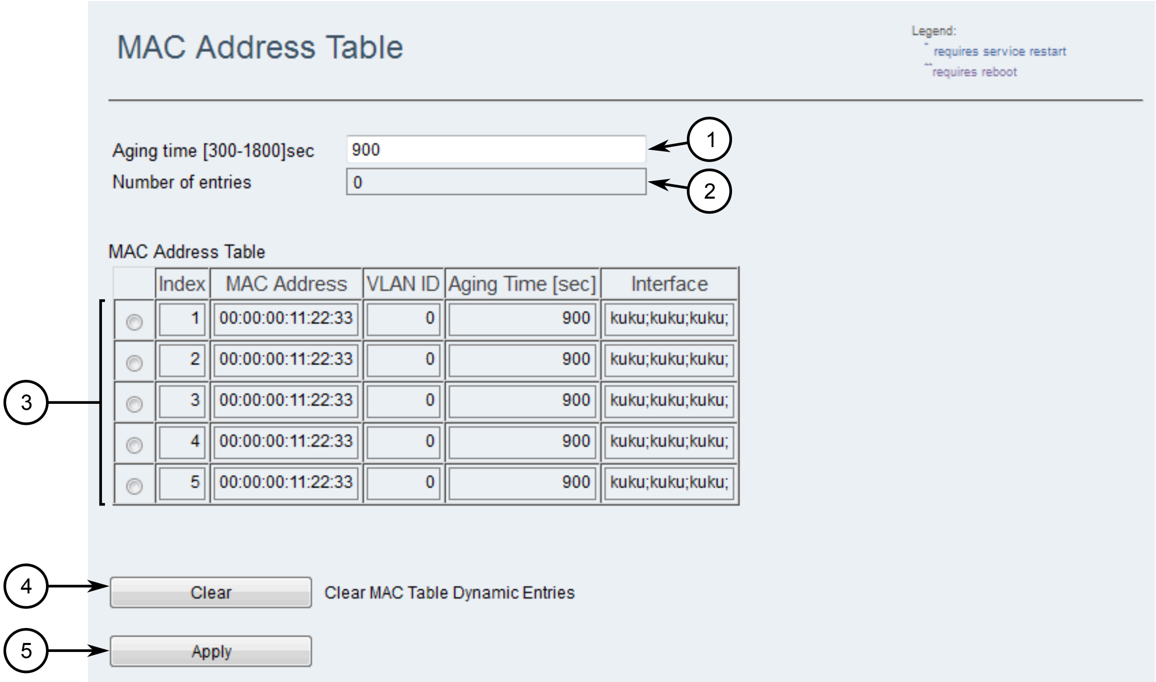
Section 10.2.1

Viewing/Clearing the MAC Address Table

The MAC Address Table displays the MAC addresses learned by the subscriber station.

›› Viewing the MAC Address Table

To view the MAC Address Table, navigate to ***Network » Ethernet Settings » MAC Address Table***. The **MAC Address Table** screen appears.



MAC Address Table

Legend:
* requires service restart
** requires reboot

Aging time [300-1800]sec: 900

Number of entries: 0

MAC Address Table

	Index	MAC Address	VLAN ID	Aging Time [sec]	Interface
○	1	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	2	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	3	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	4	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	5	00:00:00:11:22:33	0	900	kuku;kuku;kuku;

Clear MAC Table Dynamic Entries

Figure 77: MAC Address Table Screen

1. Aging Time Box **2.** Number of Entries **3.** MAC Addresses **4.** Clear Button **5.** Apply Button

The table provides the following information:

Column	Description
Index	Displays a unique identifier for the table entry.
MAC Address	Displays the MAC address of a local or remote node.
VLAN ID	Displays the identifier for the Virtual LAN on which the node is active.
Aging Time	Displays the time (in seconds) until the entry will be removed from the table.
Interface	Displays the interface from which the subscriber station learned the MAC address. Possible values 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

Clearing the MAC Address Table

MAC addresses are removed automatically from the MAC Address Table when the associated device does not transmit traffic before the *age out* period expires. Individual MAC addresses can also be removed manually when needed.

To clear the MAC address table, do the following:

1. Select on or more entries in the MAC address table.
2. click **Clear**. The seclected entries are removed.

Section 10.2.2

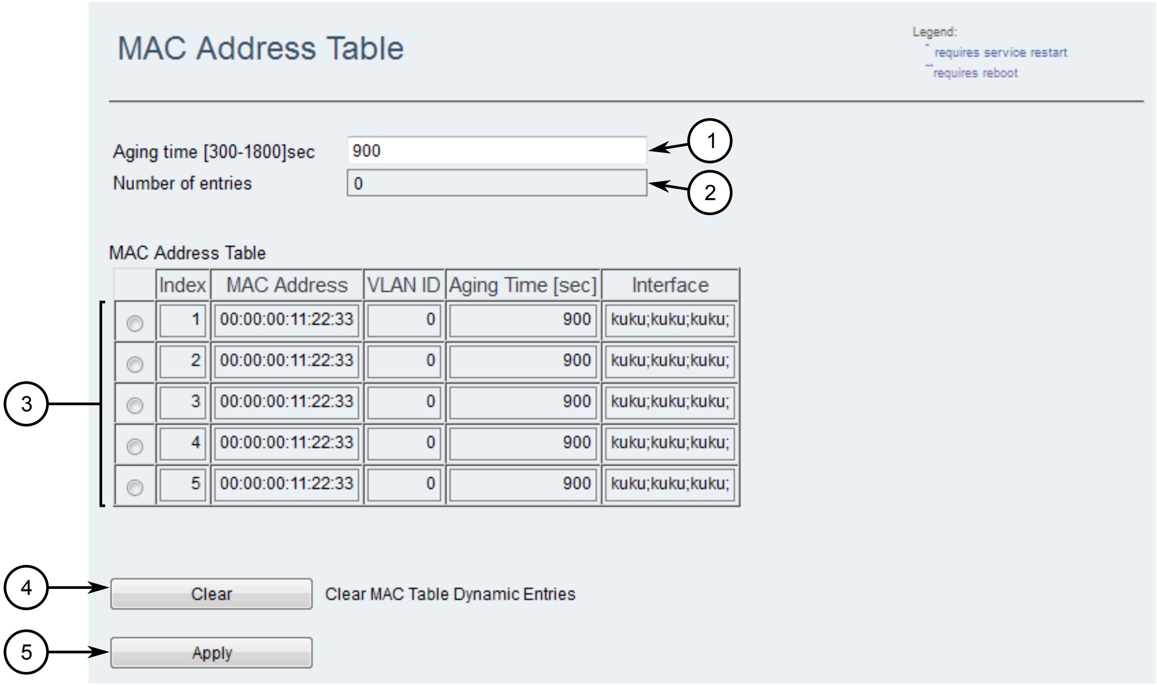
Configuring the Age Out Period for MAC Addresses

RUGGEDCOM WIN defines an *age out* period for all MAC Address Table entries to make sure the table only lists MAC addresses for active devices on the network. For each new MAC address added to the table, a timestamp is assigned to make when the address was learned. When the associated device sends traffic, the timestamp is updated. However, if the timestamp is not updated before the *age out* period expires, the MAC address is removed from the list.

To configure the *age out* period for MAC addresses, do the following:

MAC addresses are automatically removed from the MAC Address Table once their age out period expires. Age out defines the time in seconds each MAC Address Table entry is retained.

1. Navigate to ***Network » Ethernet Settings » MAC Address Table***. The **MAC Address Table** screen appears.



MAC Address Table

Legend:
* requires service restart
** requires reboot

Aging time [300-1800]sec	900
Number of entries	0

MAC Address Table

	Index	MAC Address	VLAN ID	Aging Time [sec]	Interface
○	1	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	2	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	3	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	4	00:00:00:11:22:33	0	900	kuku;kuku;kuku;
○	5	00:00:00:11:22:33	0	900	kuku;kuku;kuku;

Clear MAC Table Dynamic Entries

Figure 78: MAC Address Table Screen

1. Aging Time Box **2.** Number of Entries **3.** MAC Addresses **4.** Clear Button **5.** Apply Button

2. Under **Aging Time**, enter the *age out* period in seconds. The value can between 300 and 1800 seconds. The default value is 900 seconds.
3. Click **Apply**.

Section 10.2.3

Managing the Access List

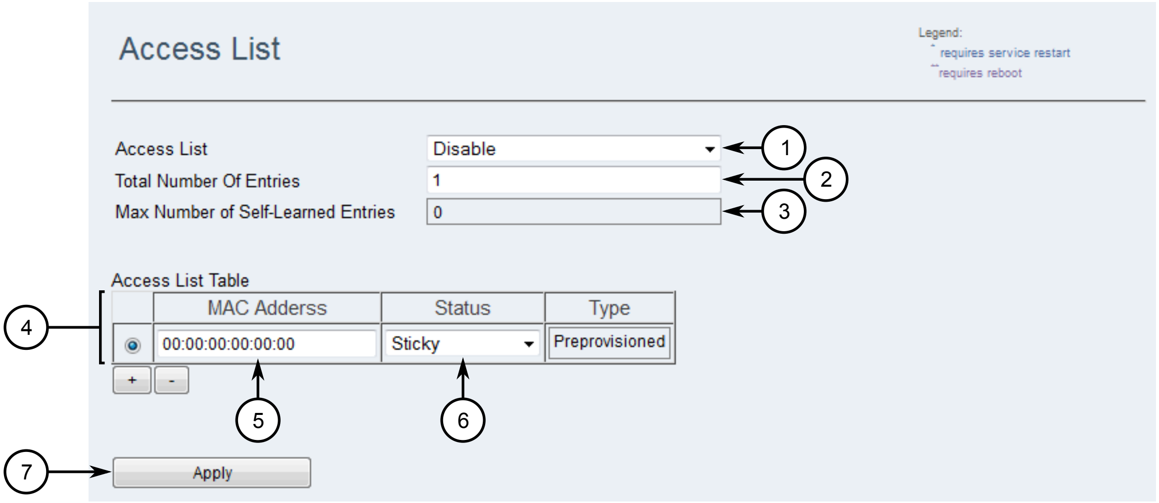
The Access List controls which devices linked to the subscriber station can communicate with the base station. When the list is enabled, the MAC address of any device that sends traffic to the subscriber station is added to the list automatically. Specific MAC addresses can also be added. These are referred to respectively as *self-learned* and *pre-provisioned* addresses.

Section 10.2.3.1

Configuring the Access List

To configure the Access List, do the following:

1. Navigate to ***Network » Access List***. The **Access List** screen appears.



Access List

Legend:
* requires service restart
** requires reboot

Access List: Disable
Total Number Of Entries: 1
Max Number of Self-Learned Entries: 0

Access List Table

	MAC Adderss	Status	Type
●	00:00:00:00:00:00	Sticky	Preprovisioned

Figure 79: Access List Screen

1. Access List List **2.** Total Number of Entries **3.** Max Number of Self-Learned Entries **4.** Access List **5.** MAC Address Box **6.** Status List **7.** Apply Button

2. Configure the following parameter(s) as required:

Parameter	Description
Access List	**Synopsis:** { Enable, Disable } **Default:** Disable a group defines the Access List. When disabled, all traffic traverses the subscriber station freely.
Total Number of Entries	**Synopsis:** An integer between 1 and 16 **Default:** 1 The total number of entries that can be added to the Access List, including self-learned and pre-provisioned entries. For example, if the list is limited to only five entries and one of which is pre-provisioned, the remaining four are open for self-learned entries. It is recommended the total number of entries be equal to the number of physical devices connected to the subscriber station.

Parameter	Description
	NOTE *If a new device attempts to send traffic through the subscriber station, its MAC address is added automatically to the Access List. However, if the list is at capacity, the device's address cannot be added and its traffic is dropped. If the* ***ACLThreshold*** *trap is enabled, RUGGEDCOM WIN will also trigger an SNMP trap to notify administrators.*

3. Click **Apply**.
4. [Optional] Add devices to the Access List. For more information, refer to Section 10.2.3.2, “Adding Devices to the Access List”.

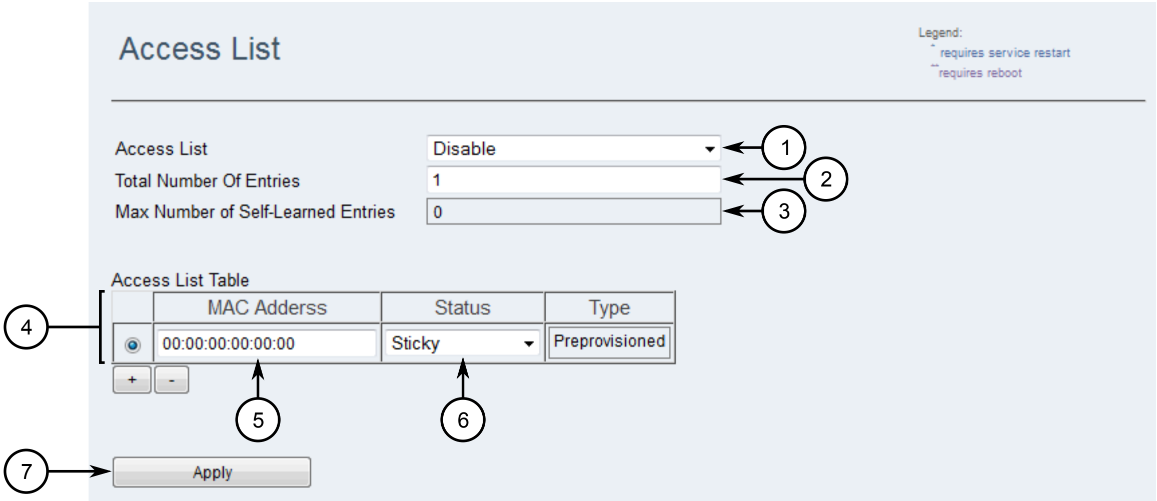
Section 10.2.3.2

Adding Devices to the Access List

Devices added to the Access List are referred to as *pre-provisioned* entries.

To add a device to the Access List, do the following:

1. Navigate to ***Network » Access List***. The **Access List** screen appears.



Access List

Legend:
* requires service restart
** requires reboot

Access List	Disable
Total Number Of Entries	1
Max Number of Self-Learned Entries	0

Access List Table

	MAC Adderss	Status	Type
●	00:00:00:00:00:00	Sticky	Preprovisioned

Figure 80: Access List Screen

1. Access List List **2.** Total Number of Entries **3.** Max Number of Self-Learned Entries **4.** Access List **5.** MAC Address Box **6.** Status List **7.** Apply Button

2. If needed, remove an existing entry to open a row for the new entry. For more information, refer to Section 10.2.3.3, “Removing Devices from the Access List”.
3. Click +. A new row appears in the **Access List Table**.
4. In the new row, configure the following paramters:

Parameter	Description
MAC Address	The MAC address for the device.

Parameter	Description
Status	**Synopsis:** { Sticky, Non-Sticky } Controls whether or not the MAC address is retained following a reboot. Options include: • `Sticky` – Sticky MAC addresses are retained following a reboot • `Non-Sticky` – Non-sticky MAC addresses are cleared from the list following a reboot **NOTE** *The status of a MAC address entry cannot be changed from **sticky** to **non-sticky**. To change status of these entries, remove the entry and allow the subscriber station to discover the device on its own.* *For information about removing entries from the Access List, refer to Section 10.2.3.3, "Removing Devices from the Access List".* **NOTE** *The default status is **non-sticky** for self-learned MAC addresses and **sticky** for pre-provisioned MAC addresses.*

5. Click **Apply**.

Section 10.2.3.3

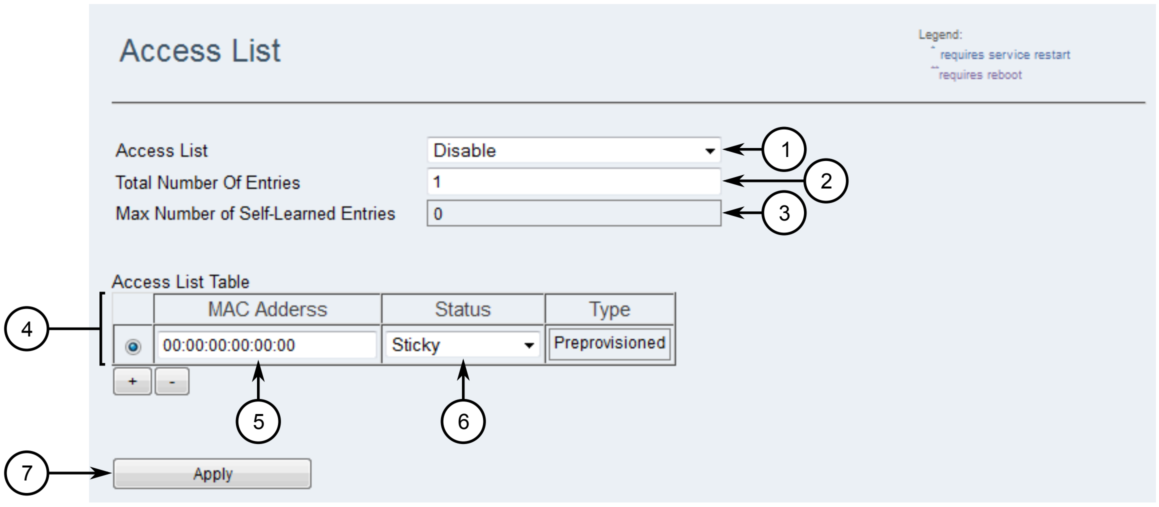
Removing Devices from the Access List

Entries can be removed from the Access List as needed to make room for a pre-provisioned entry or to change the status of an entry from *sticky* to *non-sticky*.

NOTE
MAC addresses removed from the Access List will be added automatically the next time the associate device sends traffic to the subscribe station, unless the Access List is at capacity.

To remove a device from the Access List, do the following:

1. Navigate to ***Network » Access List***. The **Access List** screen appears.



Access List

Legend:
* requires service restart
** requires reboot

Access List	Disable
Total Number Of Entries	1
Max Number of Self-Learned Entries	0

Access List Table

	MAC Adderss	Status	Type
●	00:00:00:00:00:00	Sticky	Preprovisioned

Figure 81: Access List Screen

1. Access List List **2.** Total Number of Entries **3.** Max Number of Self-Learned Entries **4.** Access List **5.** MAC Address Box **6.** Status List **7.** Apply Button

2. Select an entry and then click -. The selected entry is removed from the Access List.
3. Click **Apply**.

11 Remote Management

This section describes how to configure the subscriber station to be managed by a remote host.

CONTENTS

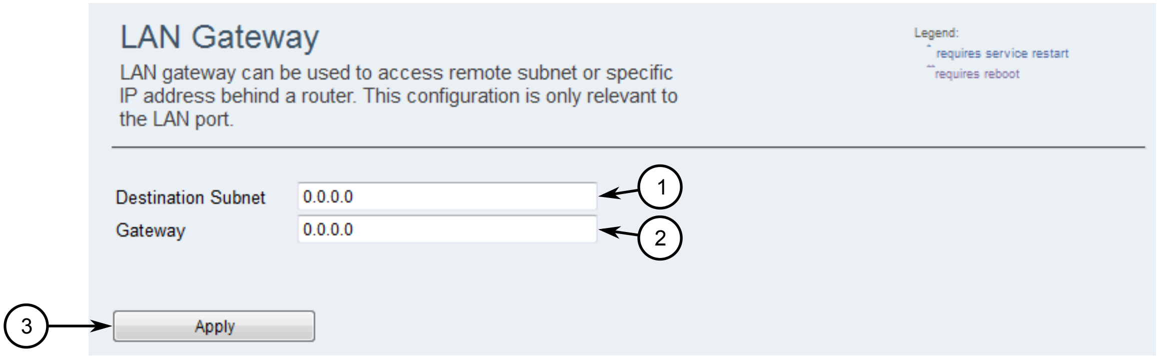
Section 11.1

Configuring the LAN Gateway

The LAN gateway allows the subscriber station to access a remote subnet or a specific IP address behind a router.

To configure the LAN gateway, do the following:

1. Navigate to ***Network » IP Settings » LAN Gateway***. The **LAN Gateway** screen appears.



LAN Gateway

LAN gateway can be used to access remote subnet or specific IP address behind a router. This configuration is only relevant to the LAN port.

Legend:
* requires service restart
** requires reboot

Destination Subnet: 0.0.0.0
Gateway: 0.0.0.0

Figure 82: LAN Gateway Screen

1. Destination Subnet Box **2.** Gateway **3.** Apply Button

2. Configure the following parameters:

Parameter	Description
Destination Subnet	The IPv4 address for the destination subnet.
Gateway	The IPv4 address for the gateway.

3. Click **Apply**.
4. [Optional] Allow or block management frames on the LAN port. For more information, refer to Section 9.2.1, “Configuring the Management VLAN”.

Section 11.2

Managing the Network Interface Protocol (NIP)

This section describes how to enable queries from NIP-enabled management systems.

Section 11.2.1

Understanding NIP

The Network Interface Protocol (NIP) allows third party applications, such as management and control systems, to query the subscriber station. It is similar to other management protocols, such as SNMP and HTTPS. However, NIP is UPD-based and UPD packets do not feature any form of authentication, identification or encryption. Therefore, NIP does not require acknowlege messages, timers or retransmissions. It is a faster and more efficient management protocol in this sense.

Use NIP for management systems that require fast, high volume queries.

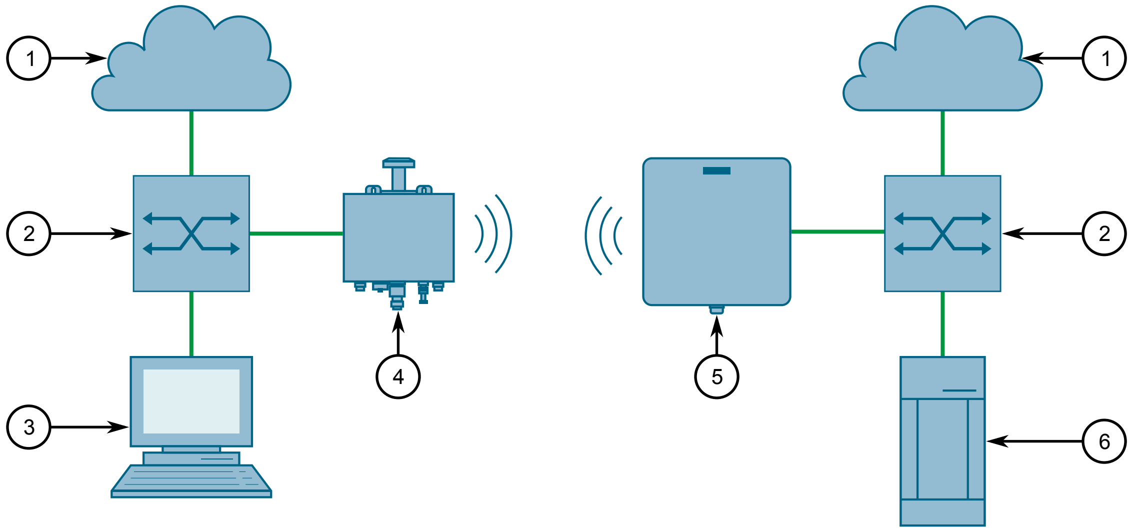


Figure 83: Network Interface Protocol Topology (Example)

1. Network **2.** Switch **3.** NIP-Enabled Management System **4.** Base Station **5.** Subscriber Station **6.** AAA/NMS/DHCP Server

NOTE

NIP does not offer a write option and may only read a specific information from the subscriber station.

NOTE
NIP is a UDP-based protocol. Retransmissions and lost packet recognition (if required) should be handled by the query application.

CONTENTS

Section 11.2.1.1

Request/Response Architecture

NIP is based on a request/response architecture. It never sends information unless it receives a specific request. NIP will also never answer requests from multicast IP addresses.

Dependent on the request, NIP will provide a compound response that includes several pieces of information. This is done to improve efficiency and prevent consecutive requests.

Section 11.2.1.2

Using NIP to Interface With Subscriber Station

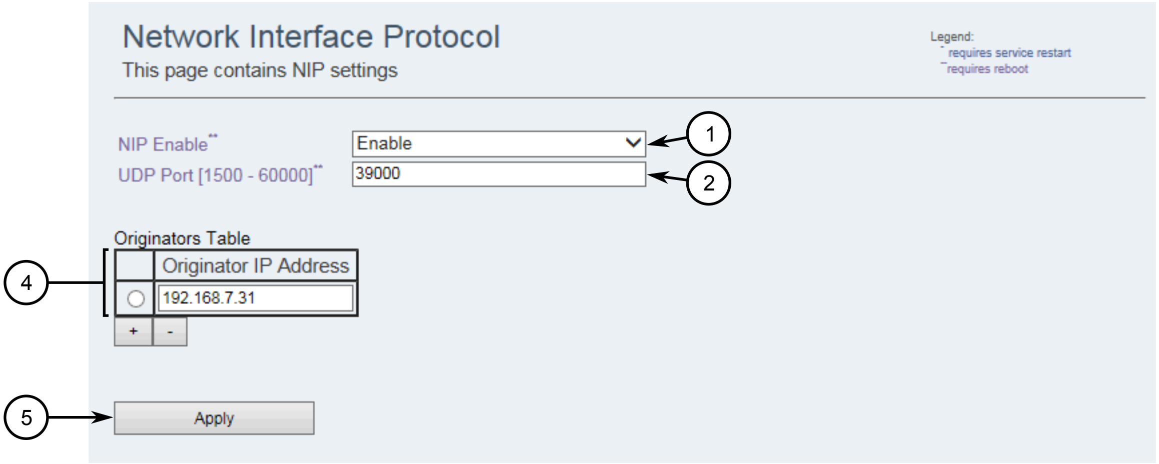
For more information about how to interface with the subscriber station using NIP, refer to the *FAQ: RUGGEDCOM WIN Network Interface Protocol API [https://support.industry.siemens.com/cs/ww/en/view/109741871]*.

Section 11.2.2

Enabling NIP

To enable the subscriber station to be queried by a Network Interface Protocol (NIP) enabled management system, do the following:

1. Navigate to ***Management » System Functions » NIP***. The **Network Interface Protocol** screen appears.



Network Interface Protocol

This page contains NIP settings

Legend:
* requires service restart
** requires reboot

NIP Enable** Enable

UDP Port [1500 - 60000]** 39000

Originators Table

	Originator IP Address
○	192.168.7.31

Figure 84: Network Interface Protocol Screen

1. NIP Enable List **2.** UDP Port Box **3.** Originators **4.** Apply Button

2. Under **NIP Enable**, select **Enable**.
3. [Optional] Under **UDP Port**, enter a port number between 1500 and 60000. The default port is 3900.

> **NOTE**
> *Up to 10 NIP-enabled management systems are supported.*

4. Add the IP address for each NIP-enabled mangement system that will be quering the subscriber station.
   a. Click +. A new row appears in the **Access List Table**.
   b. Under **Originator IP Address** enter the IP address for the management system.
5. Click **Apply**.
6. Reboot the device. For more information, refer to Section 4.1, “Rebooting the Device”.

12 Wireless

This section describes how to configure and manage the subscriber station's wireless features.

CONTENTS

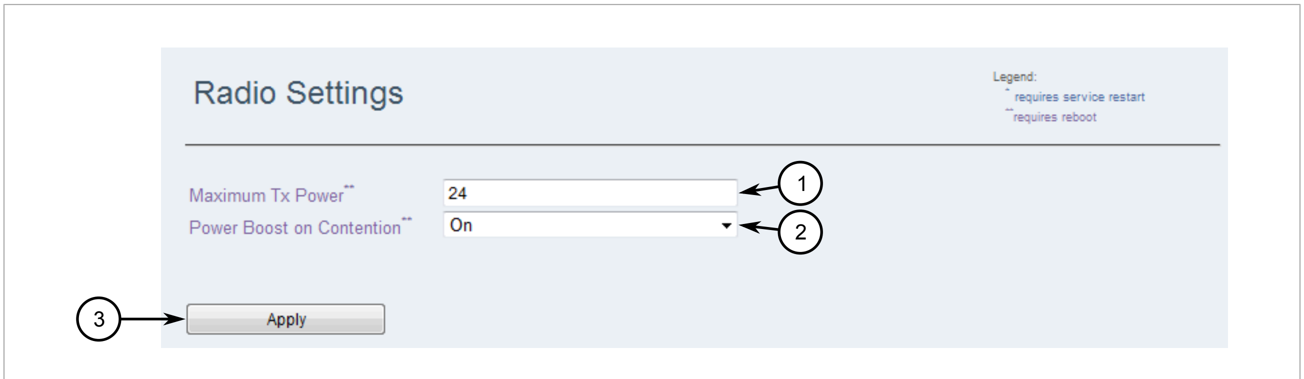
Section 12.1

Configuring the WiMAX Radio

To configure the WiMAX radio, do the following:

> **IMPORTANT!**
> *In accordance with FCC regulations, the WiMAX radio is disabled automatically for all subscriber stations that operate in the 2.3 GHz WCS (Wireless Communication Service) spectrum.*

1. Navigate to ***WiMAX » Radio » Radio Settings***. The **Radio Settings** screen appears.



Radio Settings

Legend:
* requires service restart
** requires reboot

Maximum Tx Power** 24
Power Boost on Contention** On

Figure 85: Radio Settings Screen

1. Maximum Tx Power Box **2.** Power Boost on Contention List **3.** Apply Button

2. Configure the following parameter(s) as required:

Parameter	Description
Maximum Tx Power	**Synopsis:** An integer **Default:** 24 The maximum power in dBm that can be transmitted by the device. Any value can be configured. However, the device will not exceed the following limits based on frequency band and modulation.

<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th rowspan="2">Band</th><th colspan="2">Modulation</th></tr>
<tr><th>BPSK, QPSK, QAM16</th><th>QAM64</th></tr>
<tr><td>1.4 GHz</td><td>27 dBm</td><td>24 dBm</td></tr>
<tr><td>1.8 GHz</td><td>27 dBm</td><td>24 dBm</td></tr>
<tr><td>2.3 GHz</td><td>27 dBm</td><td>24 dBm</td></tr>
<tr><td>2.5 GHz</td><td>27 dBm</td><td>24 dBm</td></tr>
<tr><td>3.5 GHz</td><td>27 dBm</td><td>24 dBm</td></tr>
<tr><td>4.9 GHz</td><td>24 dBm</td><td>21 dBm</td></tr>
<tr><td>5.1 GHz</td><td>24 dBm</td><td>21 dBm</td></tr>
<tr><td>5.8 GHz</td><td>21 dBm</td><td>21 dBm</td></tr>
</table>
</td></tr>
<tr><td>Power Boost on Contention</td><td><b>Synopsis:</b> { On, Off }
<b>Default:</b> On
Determines if the transmission power is boosted on CDMA (Code Division Multiple Accessbase) contention. Options include:
• <code>On</code> – The transmission power is boosted when another station competes for the same bandwidth
• <code>Off</code> – The transmission power is not boosted when the subscriber station detects contention</td></tr>
</table>

3. Click **Apply**.
4. Reboot the device. For more information, refer to Section 4.1, “Rebooting the Device”.

Section 12.2

Managing WiMAX Authentication

This section describes how to configure and manage WiMAX authentication. RUGGEDCOM WIN supports EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) and EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) authentication.

CONTENTS

Section 12.2.1

Viewing the Current Authentication Settings

To view the current authentication settings for the subscriber station, do the following:

1. Navigate to ***WiMAX » Authentication***. The **Authentication Method** screen appears.

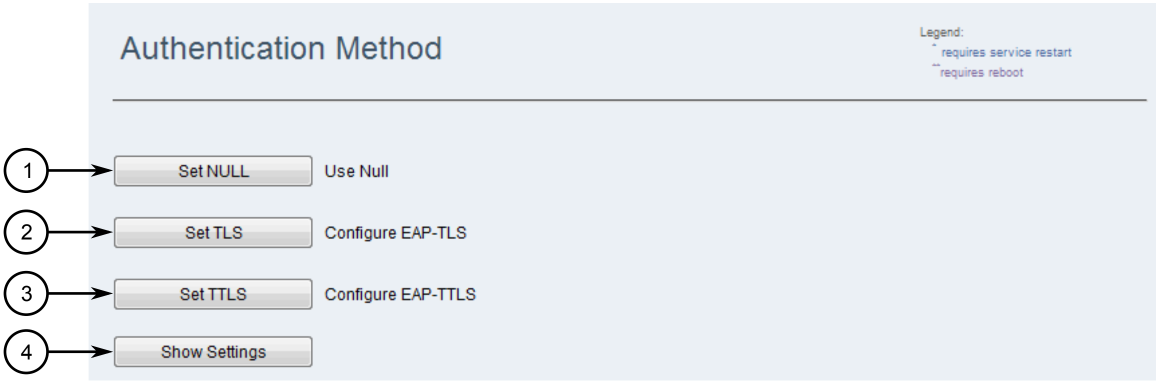
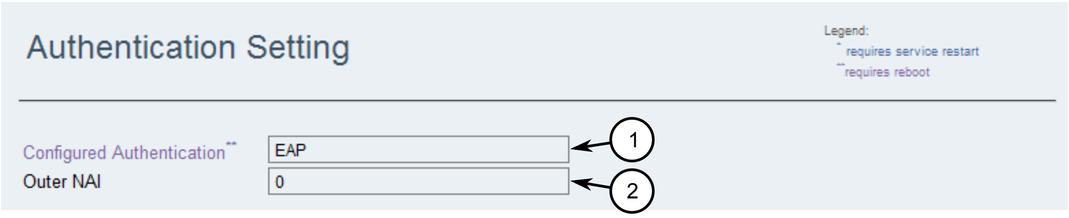


Figure 86: Authentication Method Screen

1. Set Null Button **2.** Set TLS Button **3.** Set TTLS Button **4.** Show Settings Button

2. Click **Show Settings**. The **Authentication Setting** screen appears.



Configured Authentication** EAP
Outer NAI 0

Figure 87: Authentication Setting Screen

1. Configured Authentication **2.** Outer NAI

The following information is displayed:

Setting	Description
Configured Authentication	The current configuration setting. Possible values: `Null` or `EAP`.
Outer NAI	The outer Network Access Identifier (NAI).

Section 12.2.2

Configuring EAP-TLS Authentication

To configure wireless authentication using the EAP-TLS (Extensible Authentication Protocol - Transport Layer Security), do the following:

1. Navigate to ***WiMAX » Authentication***. The **Authentication Method** screen appears.

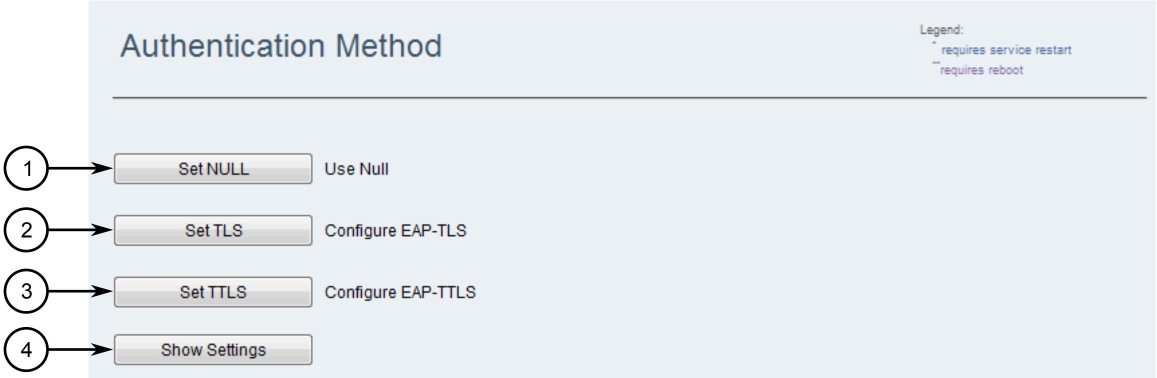
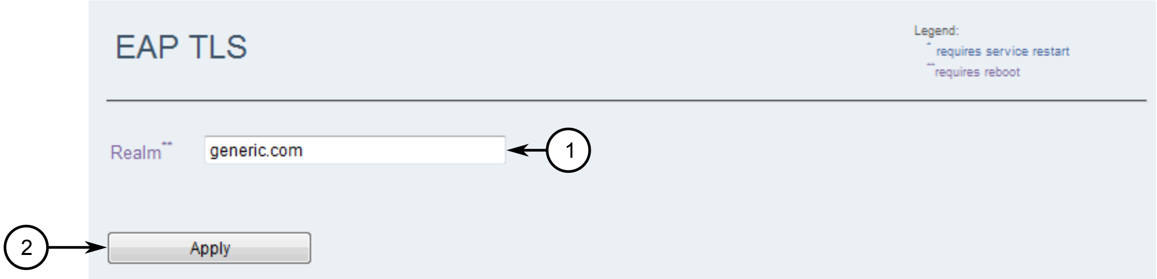


Figure 88: Authentication Method Screen

1. Set Null Button **2.** Set TLS Button **3.** Set TTLS Button **4.** Show Settings Button

2. Click **Set TLS**. The **EAP TLS** screen appears.



generic.com

Figure 89: EAP TLS Screen

1. Realm Box **2.** Apply Button

3. Under **Realm**, enter the EAP-TLS authentication realm (e.g. generic.com).
4. Click **Apply**.
5. Reboot the subscriber station. For more information, refer to Section 4.1, “Rebooting the Device”.

Section 12.2.3

Configuring EAP-TTLS Authentication

To configure wireless authentication using the EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security), do the following:

1. Navigate to ***WiMAX » Authentication***. The **Authentication Method** screen appears.

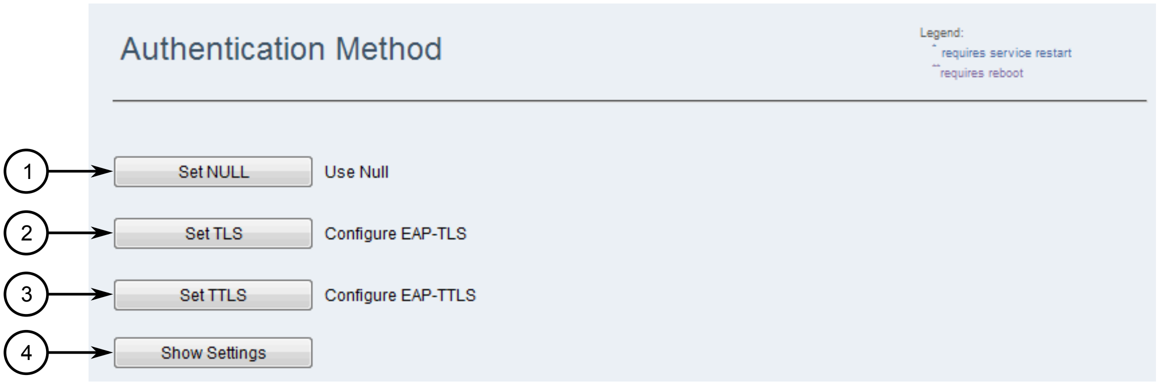
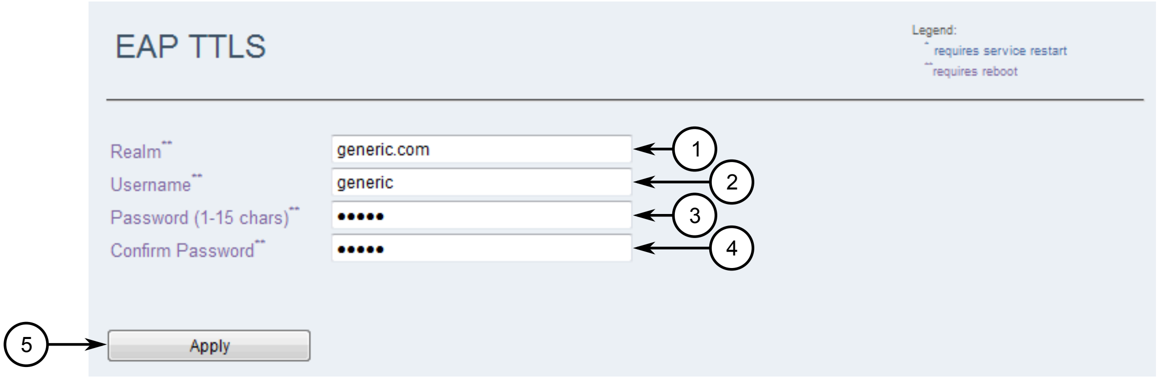


Figure 90: Authentication Method Screen

1. Set Null Button **2.** Set TLS Button **3.** Set TTLS Button **4.** Show Settings Button

2. Click **Set TTLS**. The **EAP TTLS** screen appears.



Realm** generic.com

Username** generic

Password (1-15 chars)** •••••

Confirm Password** •••••

Figure 91: EAP TTLS Screen

1. Realm Box **2.** Username Box **3.** Passowrd Box **4.** Confirm Password Box **5.** Apply Button

3. Configure the following parameter(s) as required:

Parameter	Description
Realm	The EAP-TTLS authentication realm (e.g. generic.com).
Username	The EAP-TTLS user name.
Password/Confirm Password	The password for the EAP-TTLS user.

4. Click **Apply**.
5. Reboot the device. For more information, refer to Section 4.1, “Rebooting the Device”.

Section 12.2.4

Disabling WiMAX Authentication

To disable WiMAX authentication, do the following:

1. Navigate to ***WiMAX » Authentication » Authentication Method***. The **Authentication Method** screen appears.

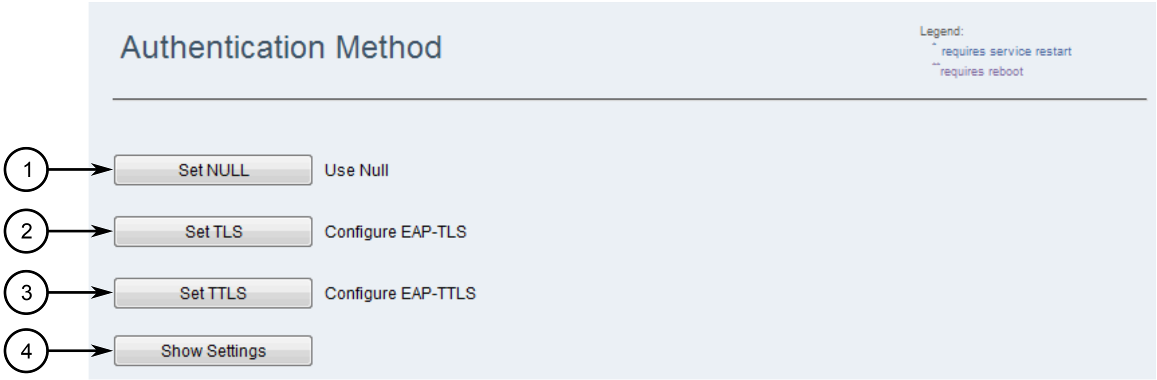


Figure 92: Authentication Method screen

1. Set NULL Button **2.** Set TLS Button **3.** Set TTLS Button **4.** Show Settings Button

2. Click **Set NULL**.

Section 12.2.5

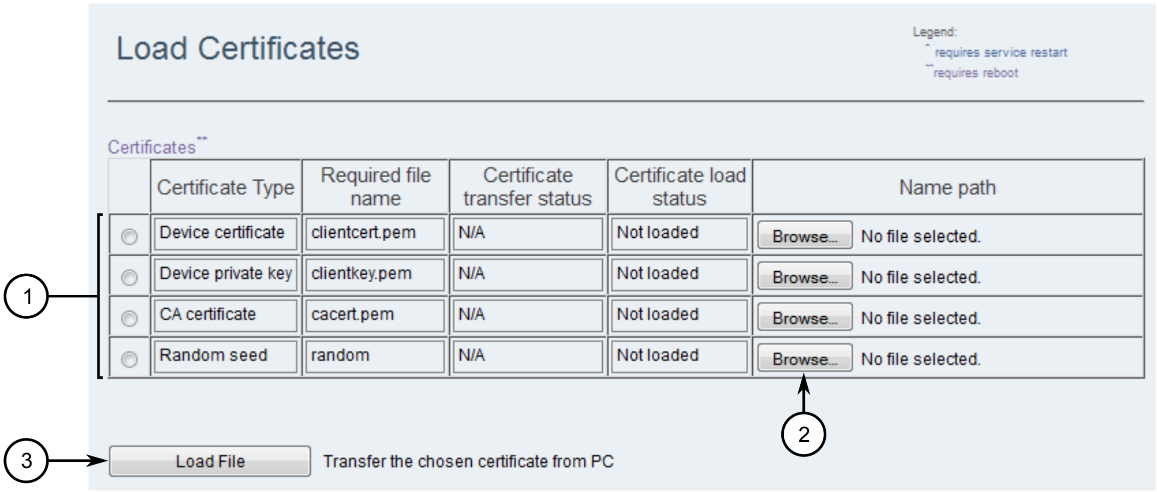
Loading Authentication Certificates

The following types of authentication certificates can be uploaded to the subscriber station:

- Device Certificate
- Device Private Key
- CA Certificate
- Random Seed

To load authentication certificates, do the following:

1. Navigate to ***WiMAX » Authentication » Load Certificates***. The **Load Certificates** screen appears.



Load Certificates

Legend:
* requires service restart
** requires reboot

Certificates**

	Certificate Type	Required file name	Certificate transfer status	Certificate load status	Name path
○	Device certificate	clientcert.pem	N/A	Not loaded	Browse... No file selected.
○	Device private key	clientkey.pem	N/A	Not loaded	Browse... No file selected.
○	CA certificate	cacert.pem	N/A	Not loaded	Browse... No file selected.
○	Random seed	random	N/A	Not loaded	Browse... No file selected.

Load File — Transfer the chosen certificate from PC

Figure 93: Load Certificates Screen

1. Certificates **2.** Browse Button **3.** Load File Button

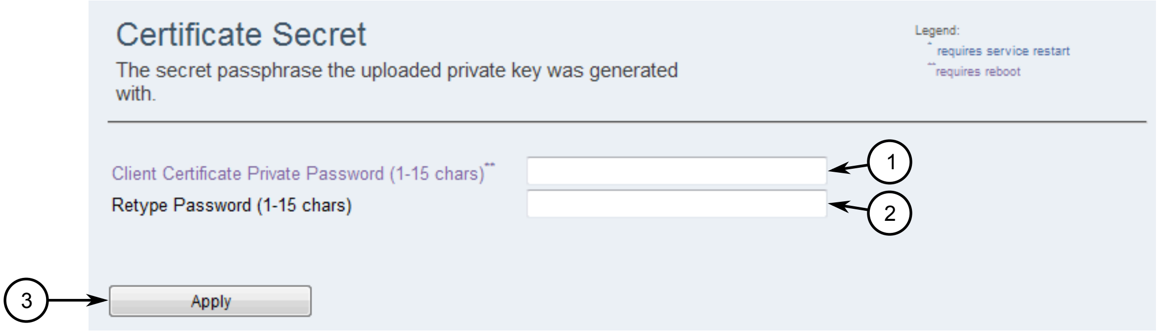
2. Select one or more certificate types.
3. For each selected certificate type, specify the associated file to be uploaded using one of the following methods:
   - Click **Browse** and select the file
   - Under **Name Path**, enter the full path to the file
4. Click **Load File**.
5. Reboot the subscriber station. For more information, refer to Section 4.1, “Rebooting the Device”.

Section 12.2.6

Changing the Private Password for the Client Certificate

To change the private password for the Client Certificate, do the following:

1. Navigate to ***WiMAX » Authentication » Certificate Secret***. The **Certificate Secret** screen appears.



Certificate Secret

The secret passphrase the uploaded private key was generated with.

Legend:
* requires service restart
** requires reboot

Client Certificate Private Password (1-15 chars)**
Retype Password (1-15 chars)
Apply
1
2
3

Figure 94: Certificate Secret Screen

1. Client Certificate Private Password Box **2.** Retype Password Box **3.** Apply Button

2. Under **Client Certificate Private Password**, enter the new password.

   It is recommended to use a strong password that meets the following criteria:

   - One lower case character
   - One upper case character
   - One number
   - One special character (i.e. !@#$%^&*()_+-={}[];:',<>/?\|`~)

3. Under **Retype Password**, enter the password again.
4. Click **Apply**.
5. Reboot the device. For more information, refer to Section 4.1, “Rebooting the Device”.

13 Troubleshooting

This chapter describes troubleshooting steps for common issues that may be encountered when using RUGGEDCOM WIN.

CONTENTS

Section 13.1

Troubleshooting Resources

This section describes the various troubleshooting resources available within RUGGEDCOM WIN.

CONTENTS

Section 13.1.1

Accessing Developer Mode

Developer mode provides additional options for configuring and debugging the device. It is intended primarily for use by Siemens Customer Support.

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 a password, contact Siemens Customer Support.

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

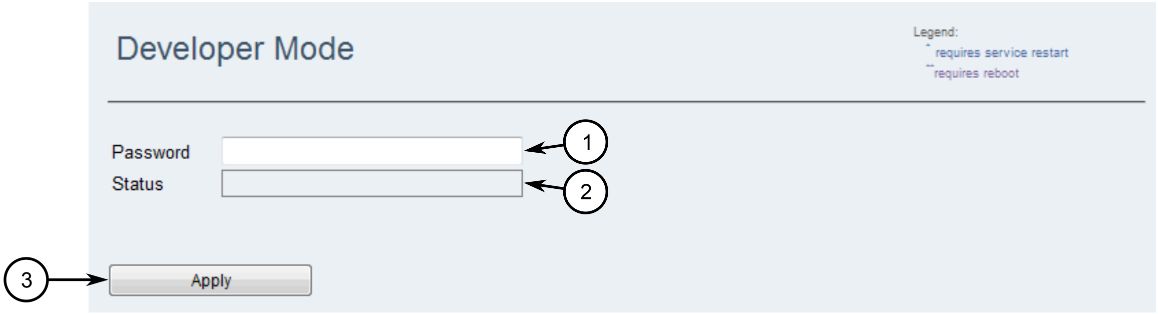


Figure 95: Developer Mode Screen

1. Password Box **2.** Status **3.** Apply Button

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 13.2

Frequently Asked Questions

The following are common questions and answers. If a question is not answered in this section, refer to the many FAQs available on Siemens Industry Online Support [https://support.industry.siemens.com] or contact Siemens Customer Support for assistance.

Q: Why is there no connectivity between the subscriber station and RUGGEDCOM NMS?

A: The subscriber station is either powered down, not connected to the network, or using a different RF IP address than what is configured in RUGGEDCOM NMS. Do the following to identify the problem:

1. First, make sure the workstation running RUGGEDCOM NMS is setup as an SNMP trap destination. For more information, refer to Section 10.1.4.3, “Configuring SNMP Trap Destinations”.
2. If the workstation is an SNMP trap destination, ping the subscriber station at its RF IP address from the workstation running RUGGEDCOM NMS.
3. If there is no response, make sure the subscriber station is powered and connected to the network.
4. If the subscriber station is powered and connected, verify the RF IP address assigned to the device. This can be done via the RUGGEDCOM WIN management interface for the serving base station. For more information, refer to the *RUGGEDCOM WIN User Guide* for the base station.
5. From the workstation running RUGGEDCOM NMS, ping the IP address assigned to the subscriber station.
6. If there is still no response from the subscriber station, contact Siemens Customer Support.