

**RUGGEDCOM**<sup>®</sup>  
**INDUSTRIAL STRENGTH NETWORKS**<sup>™</sup>

# RuggedMAX<sup>™</sup>

**WiN5100 / WiN5200**  
**Installation and User Guide**



**RUGGED** **MAX**<sup>™</sup>

Version 4.2.1 - November 28, 2011

## RuggedMAX™: WiN5100 / WiN5200 Installation and User Guide

Copyright © 2011 RuggedCom Inc.

### All Rights Reserved

Dissemination or reproduction of this document, or evaluation and communication of its contents, is not authorized except where expressly permitted. Violations are liable for damages. All rights are reserved, particularly for the purposes of patent application or trademark registration.

This document contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of RuggedCom Inc.

### Disclaimer Of Liability

We have checked the contents of this manual against the hardware and software described. However, deviations from the description cannot be completely ruled out.

RuggedCom 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

ROX™, RuggedRated™, eRSTP™, RuggedBackbone™, and RuggedMAX™ are trademarks of RuggedCom Inc. RuggedRouter® is a registered trademark of RuggedCom Inc. Other designations in this manual might be trademarks whose use by third parties for their own purposes would infringe the rights of the owner.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

The registered trademark Linux® is used pursuant to a sublicense from LMI, the exclusive licensee of Linus Torvalds, owner of the mark on a world-wide basis.

### Warranty

Five (5) years from date of purchase, return to factory. For warranty details, visit [www.RuggedCom.com](http://www.RuggedCom.com) or contact your customer service representative.

### Contacting RuggedCom

Corporate Headquarters	US Headquarters	Europe Headquarters
RuggedCom Inc. 300 Applewood Crescent, Concord, Ontario Canada, L4K 5C7 Tel: +1 905 856 5288 Fax: +1 905 856 1995 Toll-free: 1 888 264 0006	RuggedCom 1930 Harrison Street, Suite 209 Hollywood, Florida USA, 33020 Tel: +1 954 922 7938 ext.103 Fax: +1 954 922 7984 Toll-free: 1 888 264 0006	RuggedCom Unit 41, Aztec Centre, Aztec West, Almondsbury, Bristol United Kingdom BS32 4TD Tel: +44 1454 203 404 Fax: +44 1454 203 403
Email: <a href="mailto:RuggedSales@RuggedCom.com">RuggedSales@RuggedCom.com</a>		

Technical Support
Toll Free (North America): 1 866 922 7975 International: +1 905 856 5288 Email: <a href="mailto:Support@RuggedCom.com">Support@RuggedCom.com</a>

Web: [www.RuggedCom.com](http://www.RuggedCom.com)

---

# Table of Contents

FCC Statement And Cautions .....	8
1. Introduction .....	9
1.1. WiN5100 Package Components and Unpacking .....	9
1.2. WiN5200 Package Components and Unpacking .....	9
1.3. Safety Information .....	10
1.3.1. RF Exposure .....	10
1.3.2. Lightning Protection .....	10
1.3.3. Power Cord Protection .....	10
1.3.4. Servicing .....	10
1.3.5. Outdoor Grounding System .....	10
2. Product Description .....	11
2.1. IEEE 802.16e Mobile WiMAX Compliance .....	11
2.2. Block Diagram .....	11
2.3. Features .....	13
2.3.1. Mobile WiMAX Wave 2 MIMO Features .....	13
2.3.2. Deployment Models .....	17
2.3.3. Service Flows .....	18
2.3.4. Physical Description .....	20
2.3.5. Connectors and LED Indicators .....	21
2.3.6. LED Indicators .....	23
3. Mounting .....	24
3.1. Site Survey .....	24
3.1.1. Recommended Site Requirements .....	24
3.1.2. Pole Mounting .....	24
3.1.3. Wall Mounting .....	24
4. Installation Procedure .....	25
4.1. Safety Hazards .....	25
4.2. Required Installation Tools .....	25
4.3. Required Cables .....	25
4.4. Pole Mount Installation .....	26
4.5. Wall Mount Installation .....	27
4.6. Aligning the CPE Antenna .....	28
4.7. Cable Connections .....	29
4.7.1. Weatherproofing .....	29
4.7.2. Assembling the RJ45 Connector .....	31
4.7.3. Installing the WiN1010 Data Adaptor .....	34
5. Equipment Configuration and Monitoring .....	36
5.1. Connecting to and Logging In to the CPE .....	36
5.2. Configuring the CPE .....	38
6. CPE Management Interface .....	42
6.1. Using the CPE Management Interface .....	42
6.1.1. Configuration Buttons .....	43
6.2. System Management .....	44
6.2.1. Managing System Functions .....	44
6.2.2. Changing the CPE Management Interface Password .....	45
6.2.3. Remote Management Parameters .....	46

- 6.2.4. Software Version Management ..... 48
- 6.2.5. SNMP Administration ..... 55
- 6.2.6. Alarms & Traps ..... 57
- 6.3. CPE Network Configuration ..... 61
  - 6.3.1. Network IP Settings ..... 61
  - 6.3.2. Ethernet Settings ..... 62
- 6.4. CPE Statistics ..... 65
  - 6.4.1. General Statistics ..... 65
  - 6.4.2. RF Statistics ..... 66
  - 6.4.3. Network Statistics ..... 67
  - 6.4.4. Service Flow Statistics ..... 68
- 6.5. WiMAX Settings ..... 70
  - 6.5.1. Scanner Settings ..... 70
  - 6.5.2. WiMAX Authentication ..... 72
  - 6.5.3. Viewing Base Station Information ..... 76
  - 6.5.4. Configuring WiMAX Radio Parameters ..... 77
- A. WiN5100 / WiN5200 Specifications ..... 78
- B. List of Acronyms ..... 80
- C. RuggedMAX CPE Warranty ..... 83

## List of Figures

2.1. WiN5100 CPE Block Diagram: External Antennas .....	12
2.2. WiN5200 CPE Block Diagram: Integrated Antenna .....	12
2.3. MIMO Antenna System .....	13
2.4. WiN5100: General View .....	20
2.5. WiN5200: Top View .....	20
2.6. WiN5100 Connectors: AC Version .....	21
2.7. WiN5100 Connectors: DC Version .....	22
2.8. WiN5200 Connectors .....	23
4.1. Pole Mounting .....	26
4.2. WiN5200 Pole Mounted .....	26
4.3. Wall Mount Rear View .....	27
4.4. Wall Mount Front View .....	27
4.5. Wrapping the Connector with Rubber-splicing or Self-amalgamating Tape .....	30
4.6. Wrapping the Cable with Rubber-splicing or Self-amalgamating Tape .....	30
4.7. Wrapping the Connector with Electrical Tape .....	30
4.8. Sealing Gaps with Putty .....	31
4.9. RJ45 Connector Components and Cable .....	31
4.10. Preparing the CPE Cable .....	32
4.11. CPE Cable Sheathing .....	32
4.12. Ethernet Port Pinout .....	32
4.13. Modular Plug Assembly .....	33
4.14. Crimping the Connector .....	33
4.15. Assembly of Connector Components .....	34
4.16. Connecting the Cable to the CPE .....	34
4.17. Power over Ethernet Connection Schematic .....	35
5.1. Windows Local Area Connection Properties dialog .....	36
5.2. Windows TCP/IP Properties dialog .....	37
5.3. CPE General Statistics pane .....	37
5.4. Scanner Settings pane .....	38
5.5. IP Settings pane .....	39
5.6. General Statistics pane .....	40
5.7. Service Flow pane .....	41
6.1. CPE Management Interface Controls .....	42
6.2. CPE Configuration Buttons .....	43
6.3. System Functions pane .....	44
6.4. Change Password for User Admin pane .....	45
6.5. Management Settings pane .....	46
6.6. Management VLAN pane .....	47
6.7. DSCP Marking pane .....	48
6.8. SW Properties pane .....	49
6.9. SW Download pane .....	50
6.10. Primary Bank Components pane .....	52
6.11. Secondary Bank Components pane .....	53
6.12. File Transfer Status pane .....	54
6.13. SNMPv2c Access Settings pane .....	56
6.14. SNMP MIB2 Settings pane .....	57

6.15. System Alarms pane .....	58
6.16. SNMP Trap Settings .....	59
6.17. IP Settings pane .....	61
6.18. VLAN Tagging pane .....	62
6.19. MAC Address Table pane .....	63
6.20. MTU pane .....	64
6.21. General Statistics pane .....	65
6.22. RF pane .....	66
6.23. Network pane .....	67
6.24. Network pane .....	68
6.25. Scanner Settings pane .....	70
6.26. Authentication Setting pane .....	72
6.27. EAP TLS pane .....	73
6.28. EAP TTLS pane .....	74
6.29. View Certificates pane .....	75
6.30. Mobility pane .....	76
6.31. Radio Settings pane .....	77

## List of Tables

2.1. WiN5100 Connectors: AC Version .....	21
2.2. WiN5100 Connectors: DC Version .....	22
2.3. WiN5200 Connectors .....	23
2.4. CPE LED Indicators .....	23
4.1. Wall Mount Parts List .....	27
4.2. Ethernet Port Pinout .....	32
4.3. WiN1010 Data Adaptor LED Indications .....	35
5.1. Scanner Table fields .....	39
5.2. IP Settings fields .....	40
6.1. Configuration Buttons and Options Pane Links .....	43
6.2. Management VLAN Fields .....	47
6.3. SW Properties .....	49
6.4. Download Parameters .....	50
6.5. Primary Components Table .....	52
6.6. Secondary Components Table .....	53
6.7. File Transfer Operation Status table .....	55
6.8. SNMPv2c Configuration table .....	56
6.9. MIB2 System Table .....	57
6.10. System Alarms .....	58
6.11. Alarms Table .....	58
6.12. Traps Table .....	59
6.13. SNMP Traps List .....	60
6.14. IP Settings fields .....	61
6.15. IP Settings fields .....	62
6.16. IP Settings fields .....	63
6.17. General Statistics fields .....	65
6.18. RF Statistics fields .....	66
6.19. Network Statistics fields .....	67
6.20. SS Statistic Table .....	68
6.21. Service flow statistics Table .....	68
6.22. Scanner Table fields .....	71
6.23. EAP-TTLS Authentication fields .....	74
6.24. Serving BS table .....	76
6.25. Radio Settings fields .....	77
B.1. List of Acronyms .....	80

## FCC Statement And Cautions

### Federal Communications Commission Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.



**Caution: Service**

*This product contains no user-serviceable parts. Attempted service by unauthorized personnel shall render all warranties null and void.*

*Changes or modifications not expressly approved by could invalidate specifications, test results, and agency approvals, and void the user's authority to operate the equipment.*



**Caution: Physical Access**

*This product should be installed in a restricted access location where access can only be gained by service personnel or users who have been instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken; and access is through the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.*



## 1. Introduction

This guide describes how to install and configure the RuggedMAX™ WiN5100-series and WiN5200-series Out Door Unit (ODU) Customer Premises Equipment (CPE) units. The WiN5100-series and WiN5200-series ODU CPEs are members of the RuggedMAX™ family, a line of WiMAX broadband wireless access systems based on the 802.16e mobile WiMAX standard.

This guide is intended for installers and network operators. This manual assumes that users have some experience with WiMAX technologies and procedures.



*While some safety precautions are reviewed here, this guide assumes that installers are trained in safe installation practices. Users who are new to WiMAX technologies and service procedures should not rely on this guide for comprehensive guidance.*

### 1.1. WiN5100 Package Components and Unpacking

- 1 × WiN5100-series ODU CPE with external antenna connectors
- RF cables - 5m (approximately 16')
- Power cable - 5m (approximately 16')
- Mounting kit

### 1.2. WiN5200 Package Components and Unpacking

- 1 × WiN5200-series ODU CPE with integrated directional dual slant antenna
- 1 × commercial grade power supply

### 1.3. Safety Information

#### 1.3.1. RF Exposure


The WiN5100/WiN5200 CPE is compliant with the requirements set forth in CFR 47, section 1.1307, addressing Radio Frequency (RF) exposure from radio frequency devices as defined in OET Bulletin 65. The emitted radiation should be as little as possible. To achieve minimum RF exposure, install the CPE when it is configured not to transmit and set it to operational mode remotely, rather than enabling transmission by the installer on-site. For maintenance of the CPE, or other operations which require RF exposure, the exposure should be minimized in time and according to the regulations set by the FCC or the regulations relevant to the country of installation.  
Install antenna always at distance at least 0.39 m from the people and public area.

#### 1.3.2. Lightning Protection

When the ODU CPE is installed in an outdoor location, all indoor components (Ethernet connections and power supply) should be connected through a lightning protector. Lightning protection is intended to protect people and equipment located indoors from lightning that might strike the ODU CPE or its outdoor cables. The lightning protection device should be installed indoors, as close as possible to the point where the cables enter the building.

#### 1.3.3. Power Cord Protection

The ODU CPE should always be connected to a supported Power over Ethernet (PoE) injector.

 The WiN5100-series and WiN5200-series ODU CPEs are non-standard PoE devices. Do not attempt to use third-party PoE injectors. The use of any other type of connection or application of the ODU CPE and/or WiN1010 data adaptor is not permitted.

Route all power supply cords so that people cannot walk on them or place objects on or against them, which can damage the cords.

#### 1.3.4. Servicing

Do not open the ODU CPE cover to perform corrective actions unless instructed to do so in the operating instructions.

#### 1.3.5. Outdoor Grounding System



*For the WiN5200, the antenna is an integral part of the CPE.*

Verify that the antenna or cable system is grounded. The CPE antenna installation must be as per Article 810 of the NEC. Of particular note is the requirement that the grounding conductor be not less than 10 AWG (Cu). The grounding scheme should either be in accordance with UL 96 and 96A Lightning Protection Components and Installation Requirements for Lightning Protection Systems, or tested in accordance with UL 50 and UL 497.



*To reduce the risk of fire, use only 26 AWG or larger telecommunication line cord between indoor and outdoor units.*

#### 1.3.6. Allowed antenna types

**For WCS CPE 2.3GHz, to comply with FCC regulations & restrictions, use only outdoor antennas with gain of 16dBi!**

## 2. Product Description

The WiN5100-series and WiN5200-series Out Door Unit (ODU) Customer Premises Equipment (CPE) units are IEEE 802.16-2005 compliant wireless devices for the deployment of point-to-multipoint (PMP) and point-to-point (PTP) network architectures.

The ODU CPEs are WiMAX Forum 802.16e Wave 2 (MIMO) certified subscribers. Each subscriber registers and establishes a bi-directional data link with the base station.

### 2.1. IEEE 802.16e Mobile WiMAX Compliance

The IEEE 802.16-2005 specifications describe a PMP broadband wireless access standard for systems. This standard includes descriptions for both the Media Access Control (MAC) and the physical (PHY) layers.

The ODU CPE is compliant to IEEE 802.16-2005 WiMAX forum Wave 2 profile.

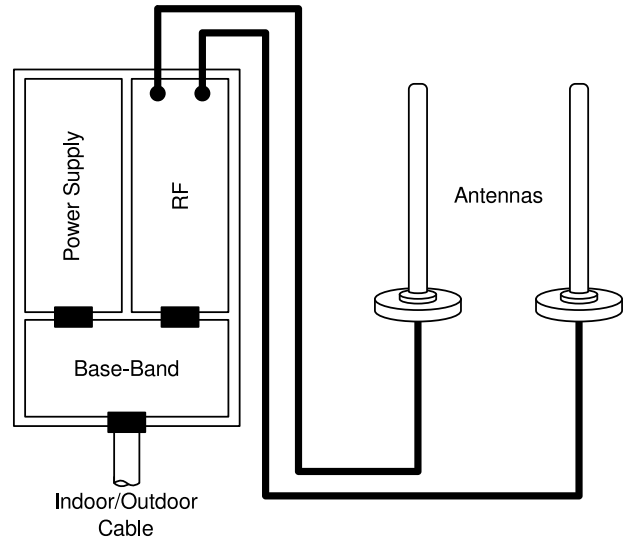


*The 802.16e standards are subject to amendment and the WiN5100 / WiN5200 product family design compliance applies to a specific revision of the standard. The WiN5100 / WiN5200 product family does not support mesh communication (direct subscriber-to-subscriber).*

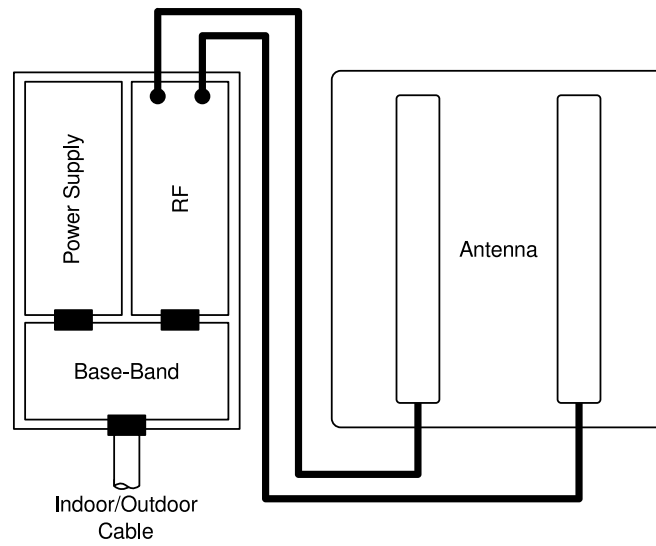
### 2.2. Block Diagram

The CPE consists of the following modules:

1. **Base-Band board:** includes the the WiMAX 16e MIMO Base-Band SoC and runs the 16e MAC + PHY, user interface, and analog front end interface to the RF module.
2. **Power Supply board with DC/DC power supply:** converts 48 VDC input to the voltages feeding the Digital and RF modules.
3. **RF board:** single transmit/dual receive module that modulates the analog WiMAX signal input from the Base-Band modem to the high frequency RF output. Several RF modules exist, each supporting a different frequency band.
4. **Chassis**
5. **Antenna or Antennas:** dual omni or polarization antennas (WiN5100) or integrated dual polarization antenna (WiN5200) supporting MIMO schemes.



**Figure 2.1. WiN5100 CPE Block Diagram: External Antennas**



**Figure 2.2. WiN5200 CPE Block Diagram: Integrated Antenna**

## 2.3. Features

### 2.3.1. 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  $2 \times 2$  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.

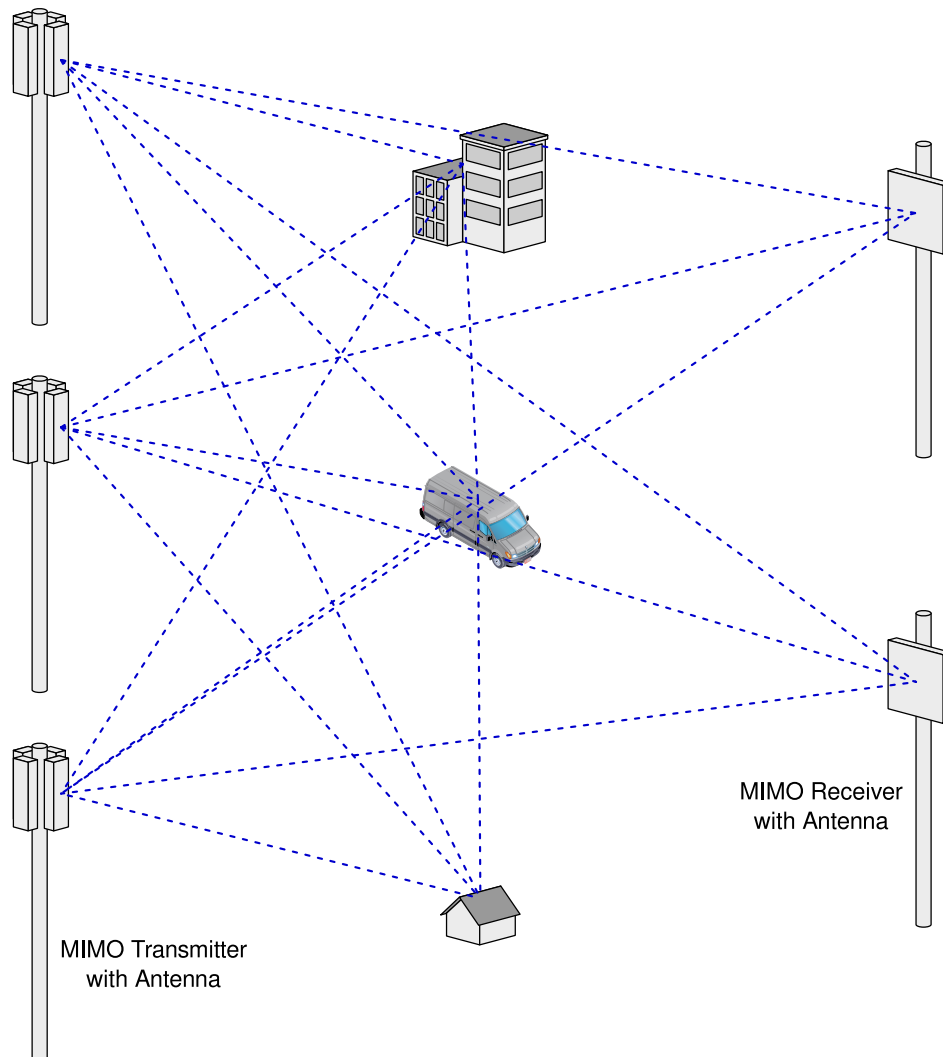


Figure 2.3. MIMO Antenna System

### 2.3.1.1. 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, was published in 1998[4] is incorporated in the WiMAX 16e standard.

### 2.3.1.2. Security

Security was a key failing of older broadband wireless systems of the past: any network that transmits its data across wireless signals rather than wires is inherently more open to interference, intrusion or assault. This does not mean solid broadband wireless security is impossible, just much more difficult.

As broadband wireless networks have matured security features have improved. With the advent of WiMAX, the security toolsets available to broadband wireless service providers have reached high levels of functionality. Today's WiMAX networks can be secured more effectively than ever before.

WiMAX and IEEE 802.16 Security Sublayer provides for privacy, authentication and confidentiality across the broadband wireless network. Defined initially by IEEE 802.16-2004 and then corrected and amended by Corrigendum 1 and IEEE 802.16e-2005 respectively, the Security Sublayer now supports fixed and mobile operation.

There are two major differences between the standards. The first difference is that the IEEE 802.16-2004 security mechanism is based on the DOCSIS standard. In 802.16e-2005, many changes have been made in the security mechanisms. The second difference is in the flexibility of subscriber station connection characteristics with the base station. IEEE 802.16-2004 only supports fixed access. In fixed access, a subscriber station cannot migrate to the air interface of a new base station without re-performing the network entry after a connection termination. IEEE 802.16e-2005 supports mobile access. In mobile access, a subscriber station can move between base station cells while maintaining the connection.

There are five primary aspects of WiMAX security that should be considered when designing a security plan for a WiMAX network:

- mitigation techniques at the physical layer
- improved wireless authentication
- encryption
- intrusion protection
- data transport security

Choices in implementation and security levels can be made at each level. However, options are limited at the physical layer.

### Physical Layer Security

There are two basic types of attacks that can affect the WiMAX physical layer: jamming and packet scrambling. The first is relatively straightforward, and is sometimes the result of interference rather than an attack. Jamming consists of a signal stronger than the WiMAX network signal overwhelming network data feeds, either in intermittent bursts or with sustained carrier waves.

Most WiMAX network services are delivered over licensed bands (currently 3.5 GHz internationally and 2.5 GHz both internationally and in the United States), and this offers spectrum that is relatively quiet from accidental interference. Accidental interference in licensed spectrum cannot always be completely discounted, as there is a possibility of second- and third-harmonic interference waves. For example, such interference might arise from much lower frequency signals that are in close proximity to the WiMAX antenna systems, or if such signals cross the WiMAX signal in close physical proximity and locally overload the WiMAX signal. In practice, however, this is rare.

Packet scrambling is an attack that occurs when control packets in the downlink and uplink subframes are sniffed, scrambled, and returned to the network. This attack is much harder to mount than a jamming attack. Since most WiMAX networks today use time division duplexing (TDD), an attacker can parse this timing sequence to capture control data, preamble, and map. The attacker can scramble this data and send it back with the correct timing to interrupt the legitimate signal, resulting in slowdowns and effectively lowered bandwidth. Intercepted and scrambled packets are also possible with frequency division duplexing (FDD), which transmits the uplink and downlink simultaneously. However, it is harder to exploit this attack than with TDD systems.

While it may seem the physical layer is inherently most vulnerable as the security elements of WiMAX are located at higher layers, the fact is hackers can often find useful exploits higher in the stack. This is because WiMAX supports multiple authentication selections, and sometimes the door can be left open by the selected authentication settings.

### Authentication

Traditionally, the first level of security authentication for older broadband wireless technologies has been MAC authentication. WiMAX supports this, although providers should not settle for this method. MAC authentication allowed service providers to log permitted MAC device addresses and allow only those addresses to access the network. Hackers long ago figured out how to spoof these. If a base station is not set up with adequate authentication measures, an attacker can capture control packets and pose as a legitimate subscriber even with older MAC device authentication enabled.

A second, newer and much better choice, embraced by the WiN5100 / WiN5200 system, is the built-in support for X.509 device certificates embedded in the Extensible Authentication Protocol-Transport Layer Security (EAP-TTLS) method. EAP-TTLS is added with the 802.16e standard and WiMAX Forum.

The EAP-TLTS authentication method allows both the subscriber and the base station to authenticate each other using an X.509 method for both, in addition to a subscriber authentication based on well-known subscriber authentication techniques such as PAP and MS-CHAP. MAC control headers are never encrypted in WiMAX. However, with EAP, carriers can optionally choose to authenticate them. This capability adds an additional layer of authentication confirmation.

### Encryption

The first layer of defense for WiMAX operators is to authenticate a legitimate user on its network. However, WiMAX, with its 802.16e ratification, offers top-line tools for data encryption. Older wireless iterations used the Data Encryption Standard (DES), which relied on a 56-bit key for encryption. This is largely considered obsolete. WiMAX 802.16e supports DES (3DES) and adds support for the Advanced Encryption Standard (AES), supporting 128-bit, 192-bit and 256-bit encryption keys. AES also meets the Federal Information Processing Standard (FIPS) 140-2 specification, which is required by numerous governmental branches. This technology, which requires dedicated processors within base stations, is robust and highly effective.

Traffic encryption may be employed per 802.16 Service Flow and is subject to operator policy.

The relevance of encryption to the network operator deployment is debatable. For example, in the past, many cellular carriers focused on authentication and mostly ignored encryption. Whether that will change as mobile service providers ramp up more broadband applications is an open question.

Authentication and encryption are resource-intensive tasks, requiring processor cycles that may affect system performance. The RuggedMAX™ subscriber stations and base stations offload these heavy computing tasks from the host processor to a specific circuit, avoiding any performance degradation due to such processing.

#### 2.3.1.3. Time Division Duplexing (TDD)

The CPE 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 PTP or 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.

#### 2.3.1.4. Coding Rate

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.

#### 2.3.1.5. Modulation

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

#### 2.3.1.6. 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.



### 2.3.2. Deployment Models

The CPE supports point to point (PTP) and point to multipoint (PMP) deployment scenarios.

#### 2.3.2.1. PTP Deployment

When deployed in a 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.

#### 2.3.2.2. PMP Deployment

When deployed in a 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.

#### 2.3.2.3. Non Line-of-Sight

The WiN5100 / WiN5200 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. In this case, a wireless link can be established only if a reflective path can be established between the base station and subscriber.

#### 2.3.2.4. Channelization

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

The CPE 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.

### 2.3.3. Service Flows

Service flows are a key feature of the 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.

#### 2.3.3.1. 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.

#### 2.3.3.2. 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.

#### 2.3.3.3. Scheduling

The 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 ensures that 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.

- **Real-Time Polling Service (rt-PS)**

The base station schedules a continuous regular series of transmit opportunities for the subscriber to send variable size data packets. The grant size is based on the current data transfer requirement. Typical applications include streaming MPEG video or VOIP with silence suppression. This is efficient for applications that have a real-time component and continuously changing bandwidth requirements.

- **Extended Real-Time Polling Service (ert-PS)**

The base station schedules a continuous series of transmit opportunities for the subscriber to send variable size data packets. This schedule supports real-time applications including VoIP with silence suppression. The dynamically scheduled grants guarantee reserved bandwidth and reduce latency introduced by repetitive grant requests. The service flow will not transmit packets larger than the nominal grant interval.

- **Non-Real-Time Polling Service (nrt-PS)**

The base station schedules regular transmit opportunities for the subscriber to send variable size data packets. Typical applications include high bandwidth FTP. The polling period is typically be one second or less, even during periods of network congestion.

- **Best Effort (BE)**

The base station schedules transmit opportunities for the subscriber to send traffic based on unused bandwidth after all higher level traffic scheduling requirements are serviced. Typical applications include Internet access and email. Best effort service flows can be assigned a priority of 0 to 7.

- **Unsolicited Grant Service (UGS)**

The base station schedules a continuous series of transmit opportunities for the subscriber to send fixed size data packets. This schedule supports real-time applications, including VoIP or TDM transport. The UGS pre-scheduled grants guarantee reserved bandwidth and reduce latency introduced by repetitive grant requests. The service flow will not transmit packets larger than the nominal grant interval.

### 2.3.4. Physical Description

**Dimensions (H × W × D without antenna):** 22cm × 9.2cm × 6cm

**Weight:** <1.5 Kg



Figure 2.4. Win5100: General View



Figure 2.5. Win5200: Top View

### 2.3.5. Connectors and LED Indicators

Connectors and LED indicators are found on the bottom of the CPE casing.

#### 2.3.5.1. WiN5100 Connectors: AC Version



Figure 2.6. WiN5100 Connectors: AC Version


Name	Description	Connector Type
ETH/PWR	Data and power from PoE injector	RJ-45
	Ground	Grounding screw
ANT1	Antenna 1	RF
ANT2	Antenna 2	RF

Table 2.1. WiN5100 Connectors: AC Version

2.3.5.2. WiN5100 Connectors: DC Version



Figure 2.7. WiN5100 Connectors: DC Version


Name	Description	Connector Type
ETH/PWR	Ethernet data connection only	RJ-45
	Ground	Grounding screw
ANT1	Antenna 1	RF
ANT2	Antenna 2	RF
DC	DC input, 10 VDC to 30 VDC	3-pin connector

Table 2.2. WiN5100 Connectors: DC Version

### 2.3.5.3. WiN5200 Connectors

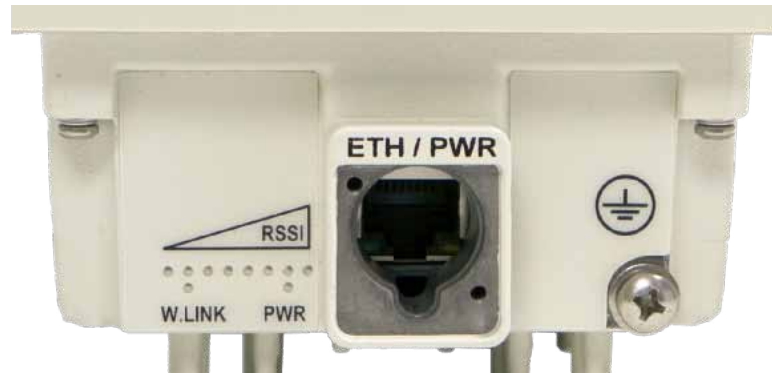


Figure 2.8. WiN5200 Connectors

Name	Description	Connector Type
ETH/PWR	Data and power from PoE injector	RJ-45
	Ground	Grounding screw

Table 2.3. WiN5200 Connectors

### 2.3.6. LED Indicators

The LED indicators at the bottom of the CPE casing display the following information:

- RSSI: displays the RSSI level
- W.LNK: displays the wireless link indication
- PWR: displays the power status

LED	Color	Description
WLNK is ON	Green	CPE is connected with and receives services from the base station; network entry is complete.
WLNK is BLINKING	Green	Link between CPE and base station is down.
PWR is ON	Green	CPE power is good
RSSI: one LED is ON (least significant)		Green 5dB # SNR < 10dB
RSSI: two LEDs are ON		Green 10dB # SNR < 15dB
RSSI: three LEDs are ON		Green 15dB # SNR < 20dB
RSSI: four LEDs are ON		Green 20dB # SNR < 24dB
RSSI: five LEDs are ON		Green SNR # 24dB and RSSI < -75dBm
RSSI: six LEDs are ON		Green SNR # 24dB and RSSI # -75dBm
RSSI: seven LEDs are ON		Green SNR # 24dB and RSSI # -70dBm
RSSI: eight LEDs are ON		LEDs 1-7: Green LED 8: Red SNR # 24dB and RSSI # -61dBm
RSSI: only the last LED is ON (most significant)		Red RSSI # -35dBm (saturation)

Table 2.4. CPE LED Indicators

### 3. Mounting

The WiN5100 / WiN5200 ODU CPE mounting kit allows for pole or wall mounting.

When choosing the mounting location for the unit, consider the available mounting structures and antenna clearance.

#### 3.1. Site Survey

Most wireless networks include many CPEs and BSTs installed in various locations in an overlapping radio-cell pattern. It is important to position each CPE at an optimal location considering the assignment of its radio channels. Therefore, a site survey becomes an essential first step before physically deploying the WiN5100 / WiN5200 solution.

Installation of the CPEs requires a backhaul connection to interface with the corporate network or Internet. The backhaul connection can be an Ethernet-wired connection, a wireless-connection, or a third party solution.

The site survey should include a detailed planning of the WiMAX system deployment. The system deployment plan should include mounting points and the routes for the power and backhaul cables.

##### 3.1.1. Recommended Site Requirements

It is highly recommended that the WiN5100 / WiN5200 CPEs be mounted near the edge of the roof of a tall building. The CPEs should be pointed in the direction of the area to be covered. To provide maximum coverage, multiple CPEs can be installed on the same rooftop. To prevent interference between the units themselves, it is important to leave some distance between each unit. When choosing the ideal location, it is also important to take into consideration the overall area topology.

##### 3.1.2. Pole Mounting

You can attach the WiN5100 and WiN5200 to any pipe or pole with a diameter of 1.75" to 10".

##### 3.1.3. Wall Mounting

You can attach the WiN5100 and WiN5200 to any wall capable of carrying the weight of the unit. An outer wall on a roof or other high location to avoid interference from other buildings or trees is preferred.



## 4. Installation Procedure

### 4.1. Safety Hazards



*Installing the WiN5100 / WiN5200 ODU CPEs can pose a serious hazard. Be sure to take precautions to avoid the following:*

- *Exposure to high voltage lines during installation*
- *Falls when working at heights or with ladders*
- *Injuries from dropping tools*
- *Contact with AC wiring*

Install antenna always at distance at least 0.39m from the people and public area!

Antenna must be in a fixed position!

Antenna position is not allowed to be changed!

### 4.2. Required Installation Tools

- Flat screwdriver
- Wrench or socket set
- Drill
- RJ-45 connector crimping tool

### 4.3. Required Cables

- IDU-to-ODU Category 5e Ethernet cable (maximum 100 m) and two RJ-45 plug connectors
- Ground cable with an appropriate termination

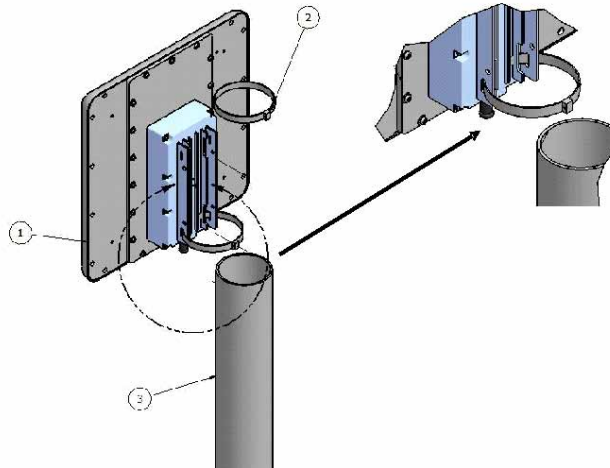
## 4.4. Pole Mount Installation

To pole mount the unit, first attach the pole mount band clamps to the CPE and then mount the CPE to the pole.

The illustrations below show the WiN5200 with integrated antenna. The installation procedure for the WiN5100 is the same.

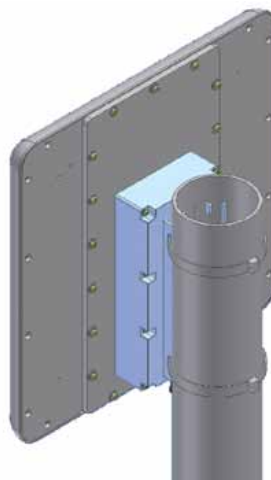
### Procedure 4.1. Pole Mounting the Unit

1. Select a mounting location on the pole.
2. Open the pole mount band clamps and insert the bands into the slots on the back of the CPE casing.



**Figure 4.1. Pole Mounting**

3. Locate the CPE on the pole and loop each band clamp around the pole.
4. Assemble and tighten each band clamp.



**Figure 4.2. WiN5200 Pole Mounted**

## 4.5. Wall Mount Installation

To wall mount the unit, first mount the wall mount bracket to the wall and then mount the CPE to the bracket.

The illustrations below show the WiN5200 with integrated antenna. The installation procedure for the WiN5100 is the same.

Item	Quantity	Description
1	1	SU16e Top Assembly
2	1	SU16e Wall Mount Bracket
3	4	Screw Flathead 100 DEG 6-32 × 3/8"
4	4	Phillips Fastener
5	4	Washer Flat NC 1/4"
6	4	Washer Spring NC 1/4"
7	4	Screw NC 1/4" × 1/2" hex

Table 4.1. Wall Mount Parts List

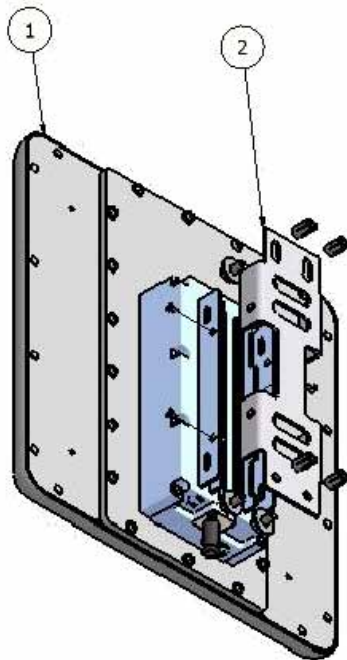


Figure 4.3. Wall Mount Rear View

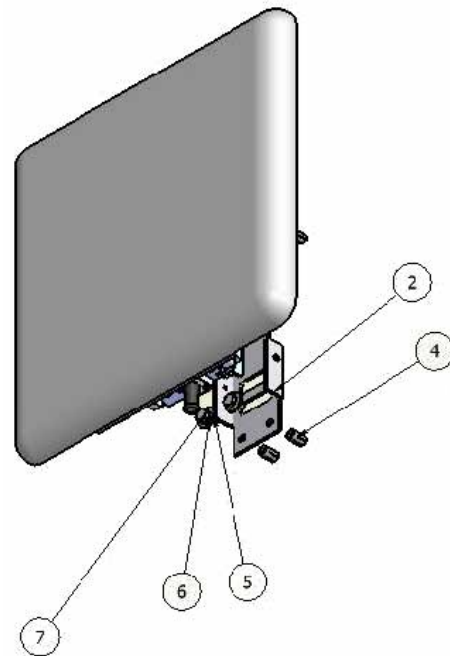


Figure 4.4. Wall Mount Front View

### Procedure 4.2. Wall Mounting

1. Select a mounting location on the wall.
2. Place the wall mounting bracket on the wall and mark 4 mounting holes.
3. Drill 4 holes and insert 4 type NC 1/4" fastening inserts into the holes.
4. Secure the mounting bracket to the wall with 4 type NS 1/4" × 1/2" HEX screws, 4 spring washers, and 4 flat washers.
5. Secure the CPE to the mounting bracket with 4 type NC 1/4" × 1/2" HEX screws, 4 spring washers and 4 flat washers.

## 4.6. Aligning the CPE Antenna



For information on the location of and how to read the RSSI LED indicators, see Section 2.3.6, “LED Indicators”.

### Procedure 4.3. Aligning the CPE Antenna

1. Point the antenna towards the general direction of the base station.
2. Verify that power is applied to the CPE. The PWR LED should be ON.
3. Verify that at least one green RSSI LED is ON, indicating that the CPE is synchronized with the base station. If the CPE is not synchronized with the base station, ensure that all parameters are configured properly. If the CPE is still not synchronized with the base station, improve link quality by changing the direction of the antenna or by placing the CPE at a higher or alternate location.
4. Rotate the CPE until the maximum RSSI link quality reading is achieved. If you encounter prolonged difficulty in achieving the expected link quality, try to improve the reception quality by placing the CPE at a higher point or in an alternate location.



Ensure that the front of the antenna is always facing the base station. In some conditions, such as when the line of sight to the base station is impeded, better reception may be achieved using a reflected signal. In this case, direct the antenna towards the reflecting object, rather than towards the base station.

In some cases, the antenna may need to be tilted to ensure that the level at which the CPE receives transmissions from the base station (and vice versa) is not too high. When only the last RSSI LED is on, this indicates saturation and that the received signal level is too high. This must be avoided, preferably by tilting the antenna upwards. As a rule of thumb, if the CPE is located at a distance of less than 300 meters from the base station, it is recommended to tilt the antenna upwards by approximately 10° to 15°.

## 4.7. Cable Connections

### 4.7.1. Weatherproofing

It is extremely important to weatherproof all outdoor cable connections. Weatherproofing the connections at the outdoor unit and antennas prevents corrosion, prevents water from interfering with the connection, and helps to keep the connection tight. Because cables also carry DC current, the need for proper weatherproofing cannot be overstated.

We recommend the use of sealing tapes designed for outdoor use:

- 3M™ Scotch® Super 88 Electrical Tape
- Heavy-duty weather-, abrasion-, and UV-resistant rubber splicing tape or self-amalgamating tape

Rubber mastic putty or duct sealing putty must also be used to complete the weatherproofing where needed. We do not recommend silicon seal or glue. These materials are difficult to apply accurately and are difficult to remove. Do not use PVC tape.

### Weatherproofing Cable Connections

Most outdoor unit, antenna, or cable problems are caused by coaxial cable connections loosened by vibration, allowing moisture to penetrate the connector interface. We recommend that all outdoor unit-to-cable connections be weatherproofed using a procedure similar to the one described below.

This method of weatherproofing must be completed on *all* external connections. If surge arrestors are used, all the associated connections and arrestors must be completely wrapped with splicing tape or self-amalgamating tape.



*Before waterproofing, ensure all connectors are correctly tightened. Ensure the connector and cables are free of foreign substances such as oil, water, grease, and dirt. Ensure that the cable extends below the connector to which it is attached, providing a path for water to follow away from the connected device.*

### Procedure 4.4. Weatherproofing Cable Connectors

1. Begin to wrap the rubber-splicing or self-amalgamating tape. Start as close to the equipment body as possible. Stretch and wind the tape around the connector housing, ensuring there are no gaps in the tape.



**Figure 4.5. Wrapping the Connector with Rubber-splicing or Self-amalgamating Tape**

2. Tightly wrap the connector and the cable. Overlap the tape, without gaps, all the way along the connector. Continue wrapping the tape 25 mm (1") onto the cable.



**Figure 4.6. Wrapping the Cable with Rubber-splicing or Self-amalgamating Tape**

3. For UV protection of the rubber splicing tape, wrap two layers of electrical tape on top of the rubber splicing tape.



**Figure 4.7. Wrapping the Connector with Electrical Tape**

4. Work mastic putty or duct sealing putty between the connector and the body of the radio or antenna. Ensure the putty fills any gaps not covered by the tape.



Figure 4.8. Sealing Gaps with Putty

### 4.7.2. Assembling the RJ45 Connector

The ODU CPE uses a male, shielded, RJ45 connector to provide the data and Power over Ethernet (PoE) connection to the device. To assemble the RJ45 connector, follow the instructions in this section. Before beginning, you will need the following items:

- CPE RJ45 Connector Kit
- Category 5e cable of suitable length for your application
- Standard cable splicing tools, including a standard crimp tool

#### Procedure 4.5. Assembling the CPE RJ45 Connector

1. Slide the connector parts on to the end of the cable as shown in [Figure 4.9, “RJ45 Connector Components and Cable”](#).

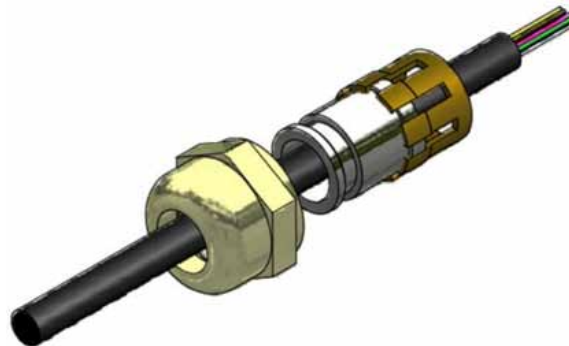


Figure 4.9. RJ45 Connector Components and Cable

2. Refer to [Figure 4.10, “Preparing the CPE Cable”](#).
  - Strip at least 18mm (0.71 inch) of sheathing from the end of the cable.
  - Pull back the cable braiding.
  - Remove the inner jacket and foil, leaving 6mm (0.25 inch) of inner jacket and foil.
  - Fan the pairs into proper color code and trim the conductors, leaving 12mm (0.47 inch) extending from the inner jacket.

## 4. Installation Procedure

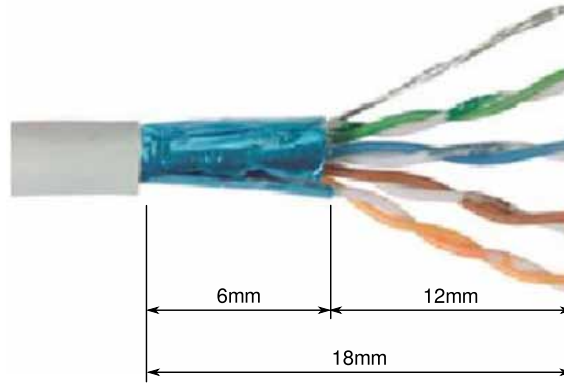


Figure 4.10. Preparing the CPE Cable

3. Form the braiding into two pigtails. The stripped cable should appear as shown in [Figure 4.11, "CPE Cable Sheathing"](#).

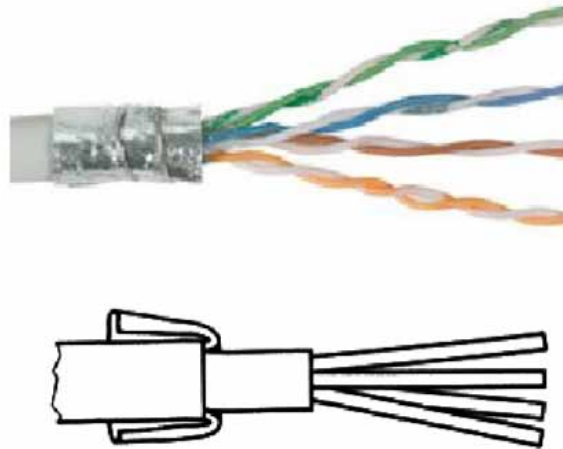


Figure 4.11. CPE Cable Sheathing

4. Place the modular plug over the wire ends, making sure to maintain the pin arrangement shown in [Figure 4.12, "Ethernet Port Pinout"](#) and [Table 4.2, "Ethernet Port Pinout"](#).

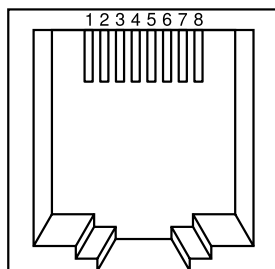
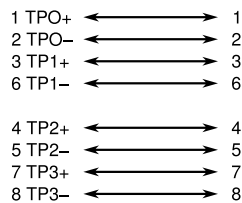


Figure 4.12. Ethernet Port Pinout



Pin Number	Description	
1	ETH Data	TP0+
2	ETH Data	TP0-
3	ETH Data	TP1+
4	+55V	TP2+
5	+55V	TP2-
6	ETH Data	TP1-
7	RTN (-)	TP3+
8	RTN (-)	TP3-

Table 4.2. Ethernet Port Pinout



## 4. Installation Procedure

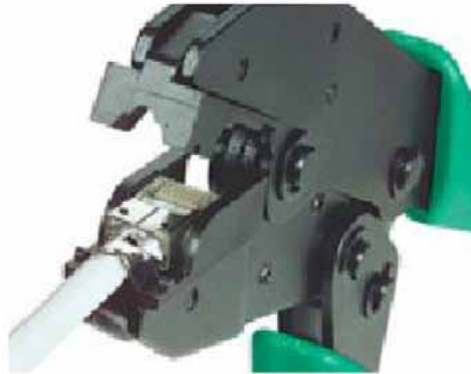
---

5. Refer to [Figure 4.13, “Modular Plug Assembly”](#). Insert the cable all the way into the modular plug case, including the inner jacket and foil. The inner jacket should be directly under the plug's strain relief tab.



**Figure 4.13. Modular Plug Assembly**

6. Refer to [Figure 4.14, “Crimping the Connector”](#). Use a standard crimp tool to secure the modular plug assembly to the cable.



**Figure 4.14. Crimping the Connector**

7. Cut the braid pigtails as close to the back of the plug as possible.
8. Slide the plug housing up the cable and align with the modular plug.
9. Refer to [Figure 4.15, “Assembly of Connector Components”](#).
  - Insert the modular plug into the plug housing.
  - Align the latch with the LATCH slot.
  - Press the modular plug into the plug housing until it bottoms out.

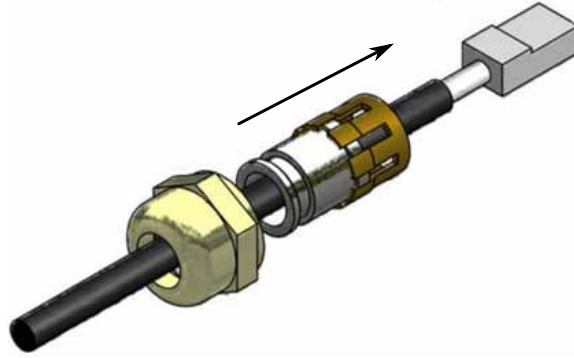


Figure 4.15. Assembly of Connector Components

10. Refer to [Figure 4.16, “Connecting the Cable to the CPE”](#). While maintaining inward pressure on the plug or keeping the dust cover engaged, tighten the compression nut to 0.56Nm (5 In-lbs).



Figure 4.16. Connecting the Cable to the CPE

### 4.7.3. Installing the WiN1010 Data Adaptor

The WiN1010 data adaptor powers the ODU CPE and distributes data. The WiN1010 data adaptor unit provides RJ-45 input connectors that include 10/100Base-T transformers for connection to an IEEE802.3 (10/100Base-T) compatible device. The unit receives power from 100V to 240V AC using an IEC-320-C14 industry standard connector.



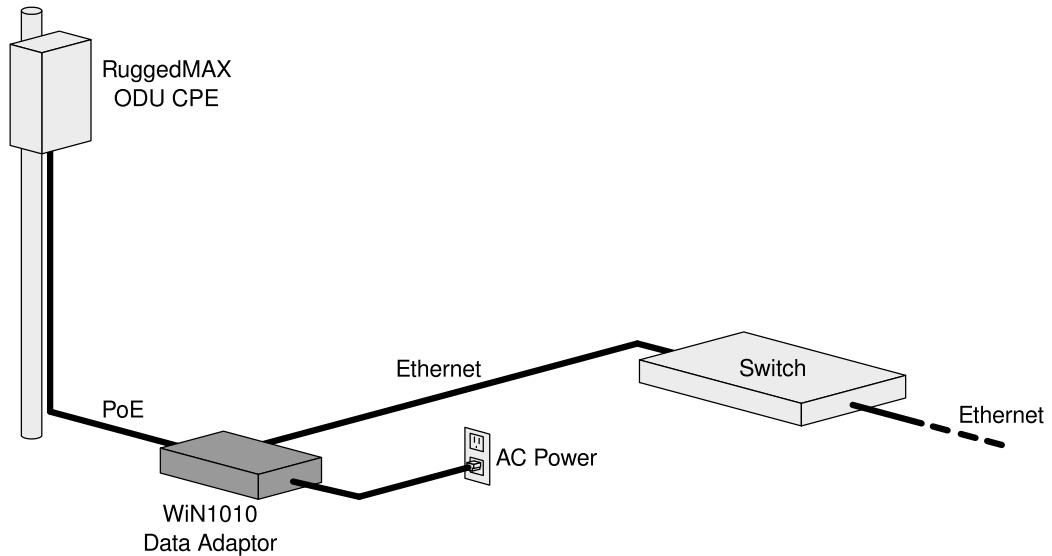
**Important:**

*The power supply AC cord should be 3 wires, 18 AWG minimum, with length less than 4.5 m, and safety certified according to national rules.*

*A single output RJ-45 connector provides 10/100 Base-T data and power to the outdoor unit over a Category 5e cable. This cable provides for the bi-directional transfer of data and signalling as well as a power feed to the outdoor equipment.*



*The Category 5e Ethernet cable is not included. Refer to "Appendix B – IDU to ODU cable specification" for detailed technical specifications.*



**Figure 4.17. Power over Ethernet Connection Schematic**



*Before connecting the WiN1010 data adaptor to the 110 VAC/220 VAC power source, verify that all system components are properly installed. Make sure that all cable connectors are securely positioned in the appropriate ports.*

**Procedure 4.6. Connecting Power to the CPE**

1. Connect a Category 5e cable between the CPE and the WiN1010 data adaptor.
2. Connect a Category 5e cable between the WiN1010 data adaptor and a 10/100 Base-T port of a switch, router, or PC.
3. Connect the WiN1010 data adaptor to the 110 VAC/220 VAC power source using the cable.

**4.7.3.1. WiN1010 Data Adaptor LED Indicators**

LEDs on the WiN1010 data adaptor front panel indicate the status of the WiN1010 power supply.

Name	Color	Description
PWR	Green	Input power is connected
LAN	Green	LAN link/activity display
WLNK	Green	Wireless link/activity display

**Table 4.3. WiN1010 Data Adaptor LED Indications**

## 5. Equipment Configuration and Monitoring

This section describes how to configure basic CPE parameters. You can preconfigure the CPE in the lab, eliminating the need to configure the unit in the field. After installing a preconfigured unit, configure additional parameters remotely through the wireless link.

### 5.1. Connecting to and Logging In to the CPE

This section describes how to set up the network parameters in Microsoft Windows so you can connect a computer to the WIN5100 or WIN5200 . For instructions on how to configure the network parameters for other operating systems, refer to your operating system documentation.

Before beginning, ensure that the CPE is connected to the Power over Ethernet (PoE) power adaptor and that power is applied.

#### Procedure 5.1. Connecting a computer to the CPE

1. Ensure that the PoE adaptor is connected to the base station. Connect the computer's Ethernet port to the PoE adaptor's Ethernet port.
2. On the computer, click **Start** and select **Control Panel**.
3. In the **Control Panel**, select **Network and Internet Connections**.
4. Select **Network Connections** and then double-click **Local Area Connection**. The **Local Area Connections Properties** dialog appears with the **General** tab selected.

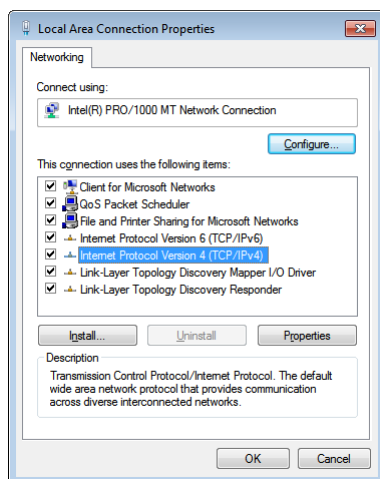


Figure 5.1. Windows Local Area Connection Properties dialog

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

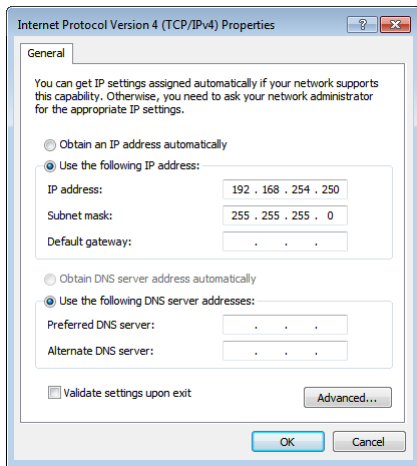


Figure 5.2. Windows TCP/IP Properties dialog

- Assign your computer the IP address **192.168.254.250** and the subnet **255.255.255.0**.
- On the **Internet Protocol (TCP/IP) Properties** dialog, click **OK**. On the **Local Area Connection Properties** dialog, click **Close**.
- Launch your web browser and type `http://192.168.254.251` in the address field. The **Login** window appears. Enter your user name and password and click **Log In**. The RuggedMAX™ WiN5100 / WiN5200 management interface appears.

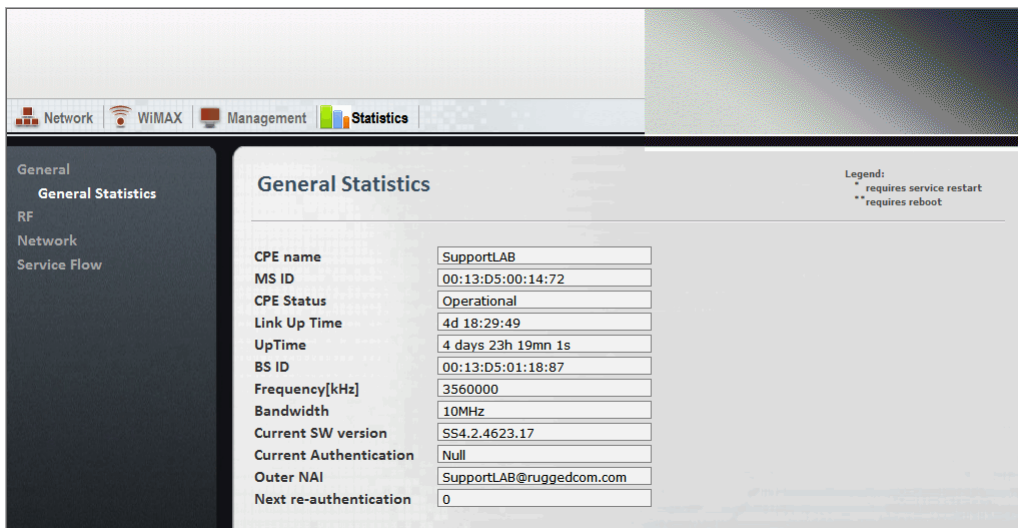


Figure 5.3. CPE General Statistics pane



The default user name is **admin** and the default password is **Axxess**. The user name and password are case sensitive.

## 5.2. Configuring the CPE

This section describes how to configure the initial CPE settings. This section describes just the minimal setting required to connect the CPE to the network. After installing the minimally configured CPE, configure additional parameters remotely through the wireless link.

### Procedure 5.2. Configuring the WiN5100 / WiN5200

1. Connect a computer to the CPE and log in to the CPE management interface. For instructions, see [Section 5.1, “Connecting to and Logging In to the CPE”](#).
2. Click the **WiMAX** button. The **Scanner Settings** pane appears.

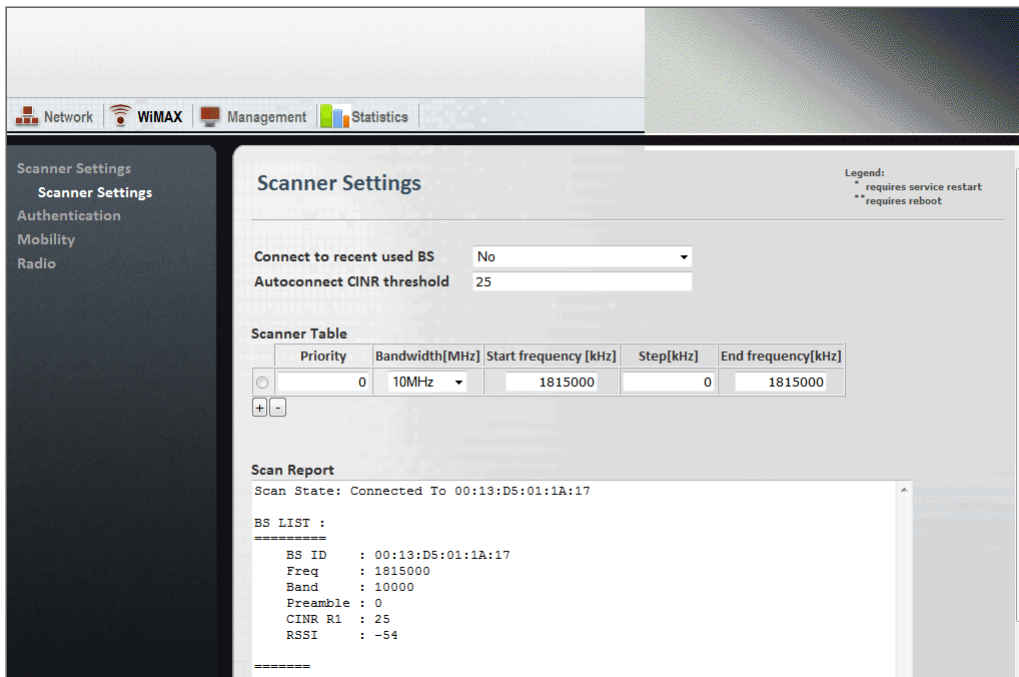


Figure 5.4. Scanner Settings pane


3. Review the entries in the **Scanner Table** and ensure that the CPE is configured to work in the correct frequency.

- To add an entry to the **Scanner Table**, click the **+** button. A new row appears in the table. You can add up to 32 rows to the table.

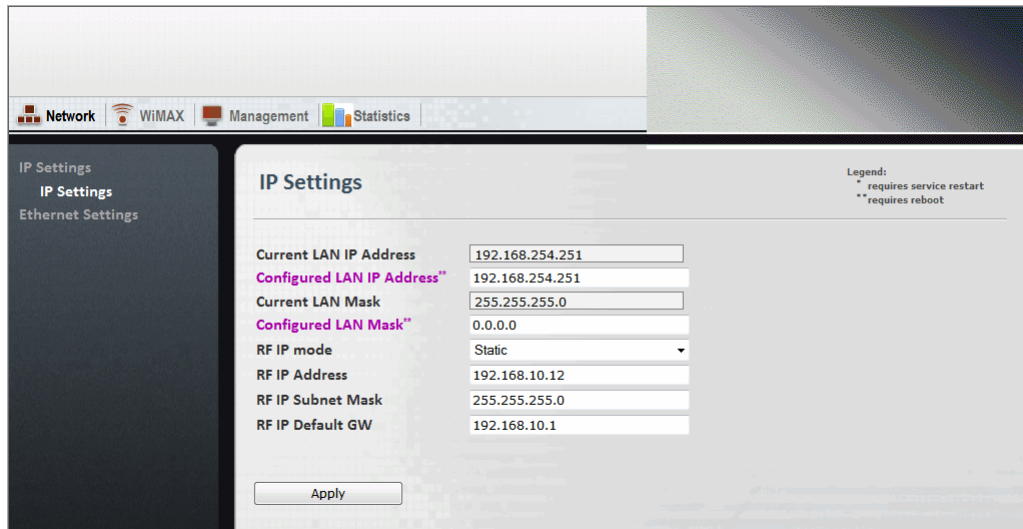
Configure the bandwidth and frequency settings in the following fields:

Field	Description
Priority	Sets the scanning priority.
Bandwidth [MHz]	Sets the scanning bandwidth. Values: 3.5 MHz   5 MHz   10 MHz
Start frequency [kHz]	Sets the start of the scanning range.
Step [kHz]	Sets the scanning step.
End frequency [kHz]	Sets the end of the scanning range.

**Table 5.1. Scanner Table fields**

 *The frequency and bandwidth should match the base station configuration.*

- To remove a row from the table, select the row and click the **-** button. The row is removed from the table.
- After making changes to the **Scanner Settings** table, click the **Apply** button.
- To begin transmitting, click the **Connect** button.
- Click the **Network** button. The **IP Settings** pane appears.



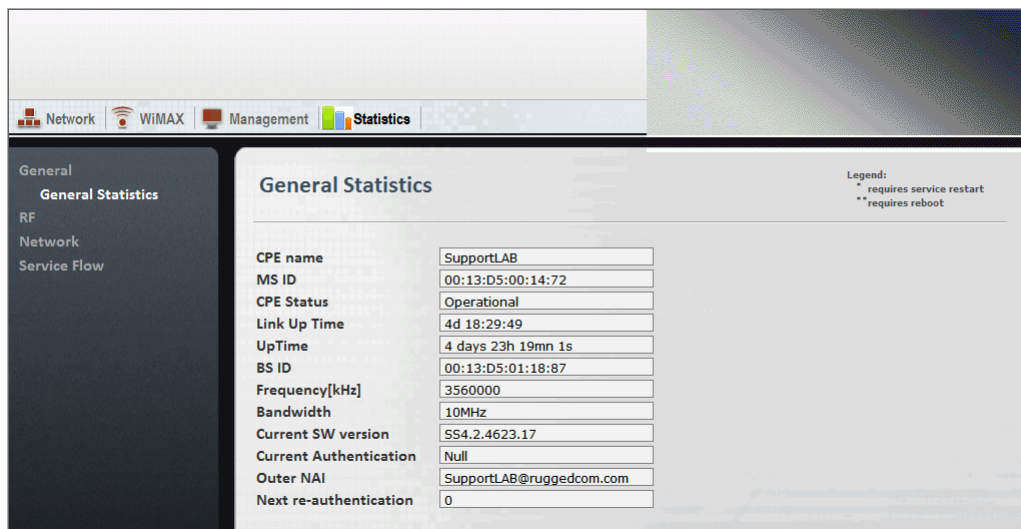
**Figure 5.5. IP Settings pane**

- Configure the CPE IP addresses in the following fields:

Field	Description
Configured LAN IP Address	Sets the CPE LAN IP address. Use this address for local CPE management through a direct connection between the CPE and a computer.
Configured LAN Mask	Sets the CPE LAN subnet mask.
RF IP Address	Sets the CPE RF network IP address. Use this address for remote CPE management through the core network.
RF IP Subnet Mask	Sets the CPE RF network subnet mask.
RF IP Default GW	Sets the CPE RF network default gateway.

**Table 5.2. IP Settings fields**

- Click the **Apply** button.
- If you changed the **Configured LAN IP Address** or **Configured LAN Mask** fields, reboot the CPE:
  - Click the **Management** button. The **System Functions** pane appears.
  - Click the **Reboot** button. The CPE reboots.
- Review the CPE statistics and ensure that the CPE is operational. Click the **Statistics** button. The **General Statistics** pane appears.



**Figure 5.6. General Statistics pane**

- Confirm that the **CPE Status** field indicates that the CPE is “Operational”.
- Review the service flow information and ensure that the service flows are created. Click the **Statistics** button and select **Service Flow**. The **Service Flow** pane appears.



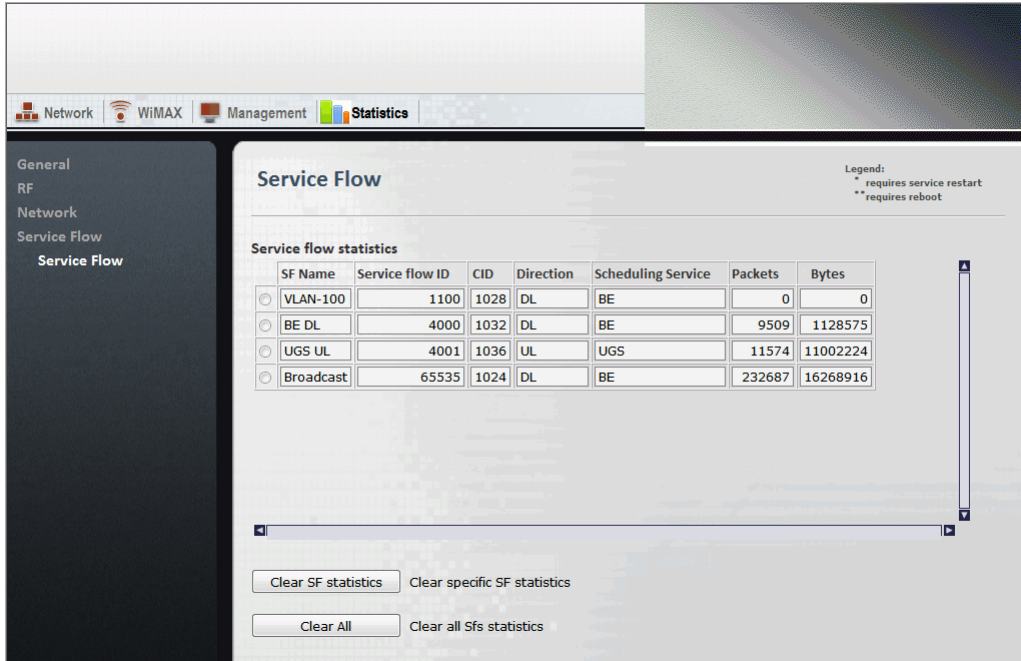


Figure 5.7. Service Flow pane

15. Log out of the CPE management interface. Click the **Management** button. The **System Functions** pane appears.
16. Click the **Logout** button. You are logged out of the CPE management interface.

## 6. CPE Management Interface

This chapter describes how to use the CPE management interface. Use the CPE management interface to configure and control CPE settings and functions. You can access the CPE management interface through the CPE’s LAN or RF IP address.

### 6.1. Using the CPE Management Interface

The CPE management interface consists of four main areas:

- Configuration Buttons — a set of buttons providing access to configuration options. To select a group of configuration options, click a button.
- Options Pane — a set of links providing access to individual configuration panes. To select a specific configuration pane, click a link.
- Display Pane — displays fields and controls for configuration options and system information displays.

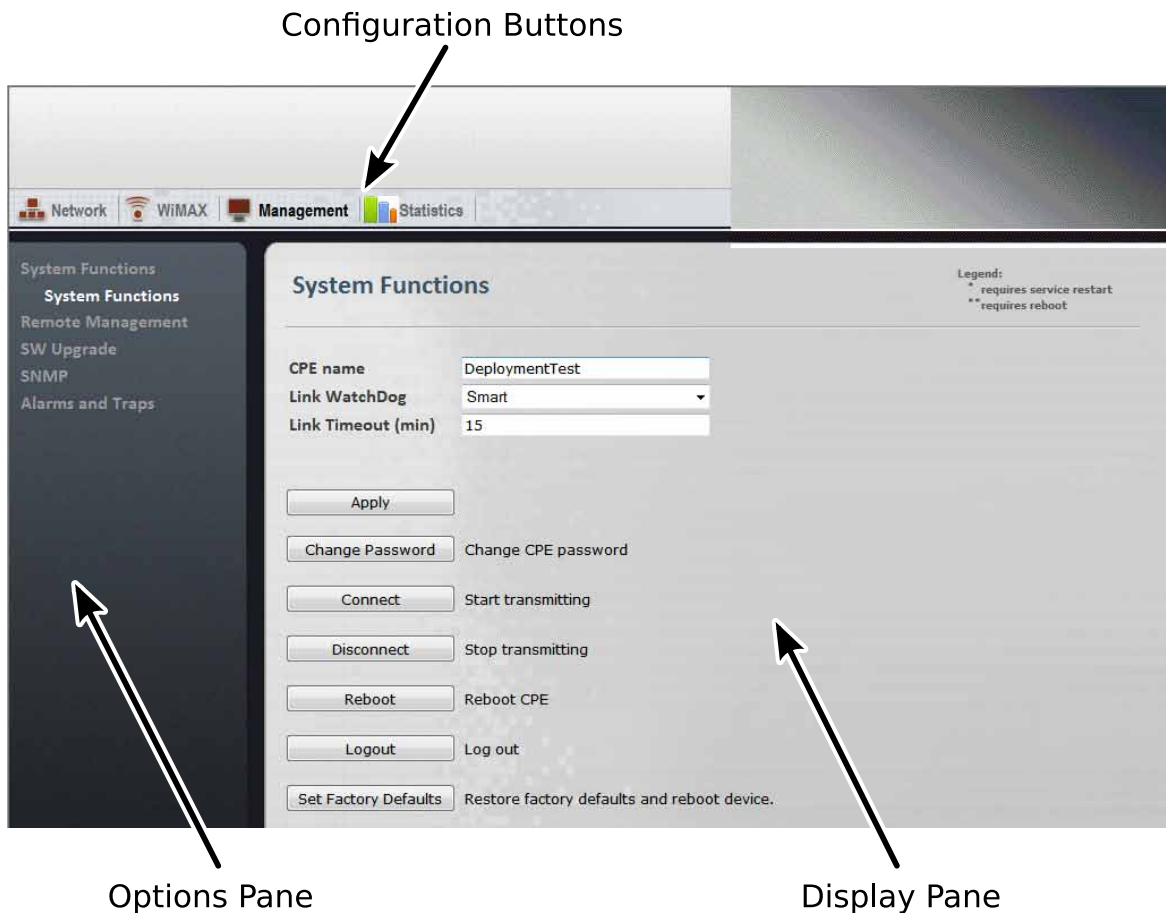


Figure 6.1. CPE Management Interface Controls

### 6.1.1. Configuration Buttons

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



Figure 6.2. CPE Configuration Buttons

Configuration Button	Description	Option Pane Links
<i>Network</i>	Access to CPE network settings.	<i>IP Settings</i> <i>Ethernet Settings</i>
<i>WiMAX</i>	Access to WiMAX scanner, authentication, mobility, and radio settings.	<i>Scanner Settings</i> <i>Authentication</i> <i>Mobility</i> <i>Radio</i>
<i>Management</i>	Access to general CPE management settings and functions.	<i>System Functions</i> <i>Remote Management</i> <i>SW Upgrade</i> <i>SNMP</i> <i>Alarms &amp; Traps</i>
<i>Statistics</i>	Displays general CPE, RF, network, and service flow statistics.	<i>General</i> <i>RF</i> <i>Network</i> <i>Service Flow</i>

Table 6.1. Configuration Buttons and Options Pane Links

## 6.2. System Management

This section describes how to:

- manage general system functions. See [Section 6.2.1, “Managing System Functions”](#).
- change the management interface password. See [Section 6.2.2, “Changing the CPE Management Interface Password”](#).
- configure the remote management parameters. See [Section 6.2.3, “Remote Management Parameters”](#).
- manage software versions and perform software upgrades. See [Section 6.2.4, “Software Version Management”](#).
- manage SNMP. See [Section 6.2.5, “SNMP Administration”](#).
- manage Alarms & Traps. See [Section 6.2.6, “Alarms & Traps”](#).

### 6.2.1. Managing System Functions

The **System Function** pane displays the CPE name and provides general system controls. On this pane, you can change the CPE password, connect to and disconnect from the base station, reboot the CPE, log out from the management interface, and restore the CPE to its factory default settings.

#### Procedure 6.1. Accessing the System Functions pane

1. Click the **Management** button. The **System Functions** pane appears.

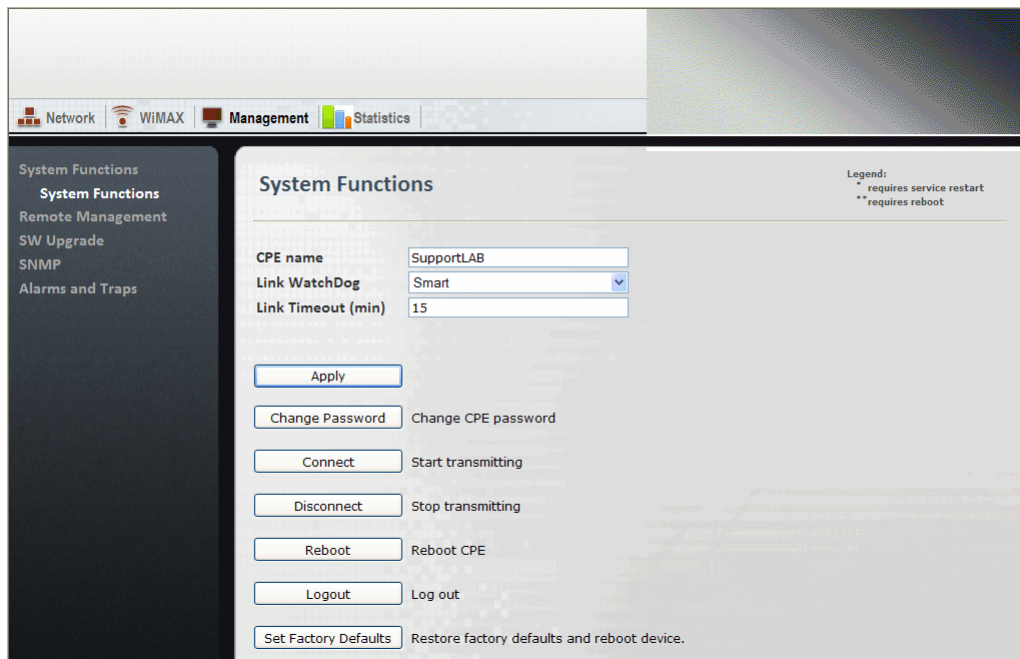


Figure 6.3. System Functions pane

2. The following operations can be performed from this pane:
  - **Set the CPE name:** The CPE name appears at the top of many of the management interface panes, identifying the CPE unit as you work with the management interface. In

the **CPE name** field, type a name and click the **Apply** button. The CPE name appears in the at the top of the management interface panes.

- **Link Watchdog:** You can set the Link Watchdog function to reset the device if it is not in an operational state for a continuous time. In the **Link WatchDog** field, select **Disabled**, **Smart** or **Always** and click the **Apply** button. The default setting is **Smart**.
- **Link Timeout (min):** You can change the number of minutes before the Link Watchdog function times out. In the **Link Timeout (min)** field, enter the number of minutes and click the **Apply** button. The default setting is **15**.
- **Change the CPE password:** You can change the password used to log in to the CPE management interface. For more information, see [Section 6.2.2, “Changing the CPE Management Interface Password”](#).
- **Connect the CPE to the base station:** To begin broadcasting and connect to the base station, click the **Connect** button.
- **Disconnect the CPE from the base station:** To stop broadcasting and disconnect from the base station, click the **Disconnect** button.
- **Reboot the CPE:** To reboot the CPE and run the software in the “Primary” memory bank, click the **Reboot** button.
- **Log out of the management interface:** To log out of the CPE management interface, click the **Logout** button.
- **Restore the CPE to factory defaults:** To restore the CPE to its factory default settings and reboot the CPE, click the **Set Factory Defaults** button.

### 6.2.2. Changing the CPE Management Interface Password

The **Change Password for User Admin** pane appears when you click the Change Password button on the System Functions pane. On this pane, you can change the the CPE management interface password for the user “admin”.

#### Procedure 6.2. Changing the Admin Password

1. Click the **Management** button. The **System Functions** pane appears.
2. Click the **Change Password** button. The **Change Password for User Admin** pane appears.

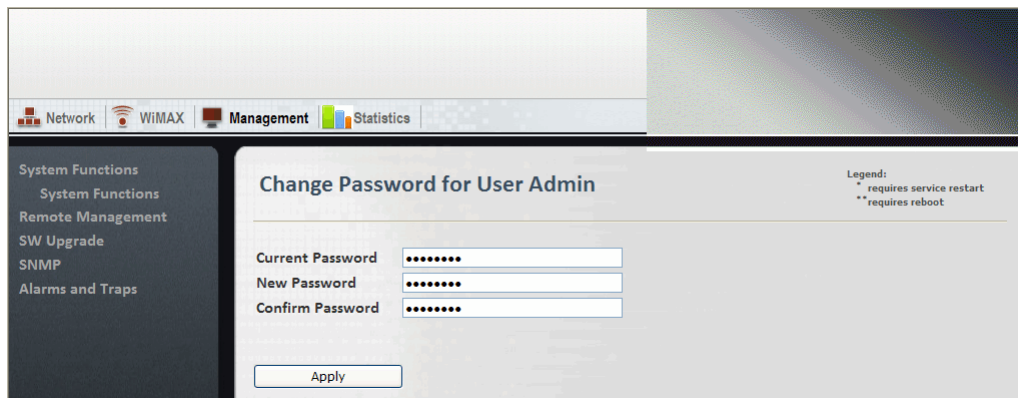


Figure 6.4. Change Password for User Admin pane

3. In the **Current Password** field, type the current password. The default password is “Axxess”.

4. In the **New Password** field, type the new password.
5. In the **Confirm Password** field, retype the new password.
6. Click the **Apply** button.

### 6.2.3. Remote Management Parameters

On the **Remote Management** panes, you configure the management port, management VLAN, and DSCP marking parameters:

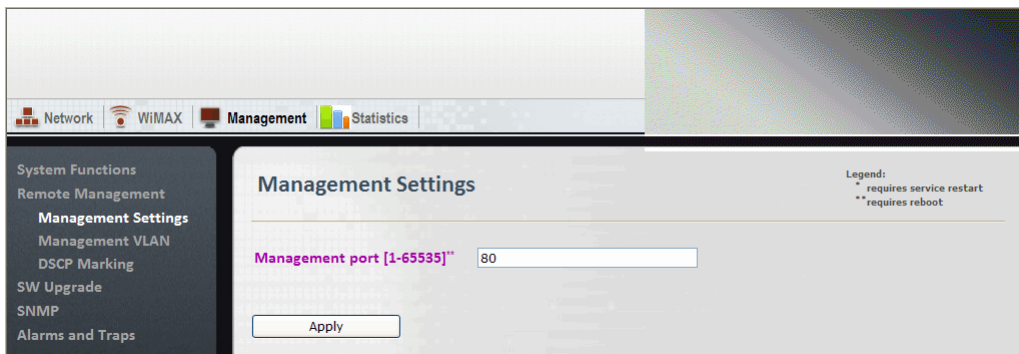
- [Section 6.2.3.1, “Configuring the Management Port”](#)
- [Section 6.2.3.2, “Configuring the Management VLAN”](#)
- [Section 6.2.3.3, “Configuring DSCP Marking”](#)

#### 6.2.3.1. Configuring the Management Port

On the **Management Port** pane, you configure the CPE management port. Note that changing the management port affects both local and remote management access.

##### Procedure 6.3. Setting the Management Port

1. Click the **Management** button. The **System Functions** pane appears.
2. In the options pane, click the **Remote Management** link. The **Management Settings** pane appears.



**Figure 6.5. Management Settings pane**

3. In the **Management port [1-65535]** field, type the port number you want to use for the management port. The default port is 80.
4. Click the **Apply** button.
5. After changing the **Management port [1-65535]** field, reboot the CPE:
  - a. Click the **Management** button. The **System Functions** pane appears.
  - b. Click the **Reboot** button. The CPE reboots.

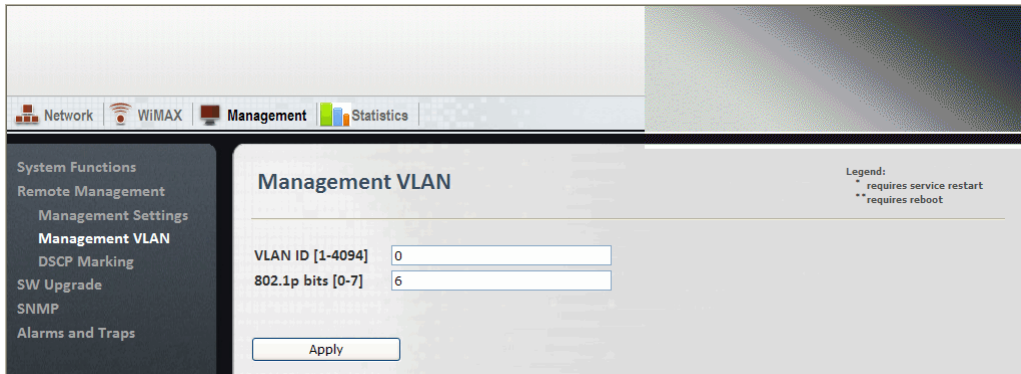
#### 6.2.3.2. Configuring the Management VLAN

On the **Management VLAN** pane, you configure the management VLAN options. The options include the VLAN number and the 802.1p priority value. Outgoing management frames are tagged

with the configured VLAN number and priority. Incoming management frames must be tagged with the same values, or the CPE drops the incoming frames.

**Procedure 6.4. Setting Management VLAN Configuration Options**

1. Click the **Management** button. The **System Functions** pane appears.
2. In the options panel, click the **Remote Management** link, and then click the **Management VLAN** link. The **Management VLAN** pane appears.



**Figure 6.6. Management VLAN pane**

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

Field	Description
VLAN Number	Displays an identifier for the management VLAN. When setting this value, ensure that the relevant VLAN service is created on the base station and that remote management is enabled. Values: Any numeric value Default: 0
802.1p bits [0-7]	Sets the 802.1p priority value for the management VLAN. Type a value from 0 to 7. Values: A number in the range of 0 to 7 Default: 6

**Table 6.2. Management VLAN Fields**

4. Click the **Apply** button.

**6.2.3.3. Configuring DSCP Marking**

On the **DSCP Marking** pane, you configure the Differentiated Services Code Point marking value. DSCP marking identified outgoing management traffic only.

**Procedure 6.5. Setting the DSCP Marking Parameter**

1. Click the **Management** button. The **System Functions** pane appears.
2. In the options panel, click the **Remote Management** link, and then click the **DSCP Marking** link. The **DSCP Marking** pane appears.



**Figure 6.7. DSCP Marking pane**

3. In the **DSCP marking [0-63]** field, type a value in the range of 0 to 63. The default value is 48.
4. Click the **Apply** button.

### 6.2.4. Software Version Management

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

This section describes how to manage CPE software versions 4.2 and later, including how to upload and download files, manage the memory banks and their “Primary” and “Secondary” designations, and how to backup and restore the operating system.

#### 6.2.4.1. Upgrading CPE Software

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

1. Load the new software image to the secondary memory bank:
  - Configure the FTP server from which the new software files will be downloaded (see [Section 6.2.4.3, “Downloading CPE Software”](#)):
  - Download the software update files to the secondary memory bank (see [Section 6.2.4.3, “Downloading CPE Software”](#)).
  - Verify that the downloaded software files have been correctly saved to the secondary memory bank (see [Section 6.2.4.5, “Managing the Secondary Memory Bank”](#)).

2. Perform a trial run of the new software image:

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

The CPE will reset and load the software image in the secondary memory bank. This process will take approximately two minutes.

3. Commit the new software image as the new default software:



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

### 6.2.4.2. Viewing Software Properties

The **SW Properties** pane displays information about the software loaded into each CPE memory bank. On this pane, you can reboot the CPE from the secondary bank, set the current bank as the primary bank, and reboot the CPE.

#### Procedure 6.6. Viewing software properties

1. Click the **Management** button. The **System Functions** pane appears.
2. In the options pane, click the **SW Upgrade** link. The **SW Properties** pane appears.

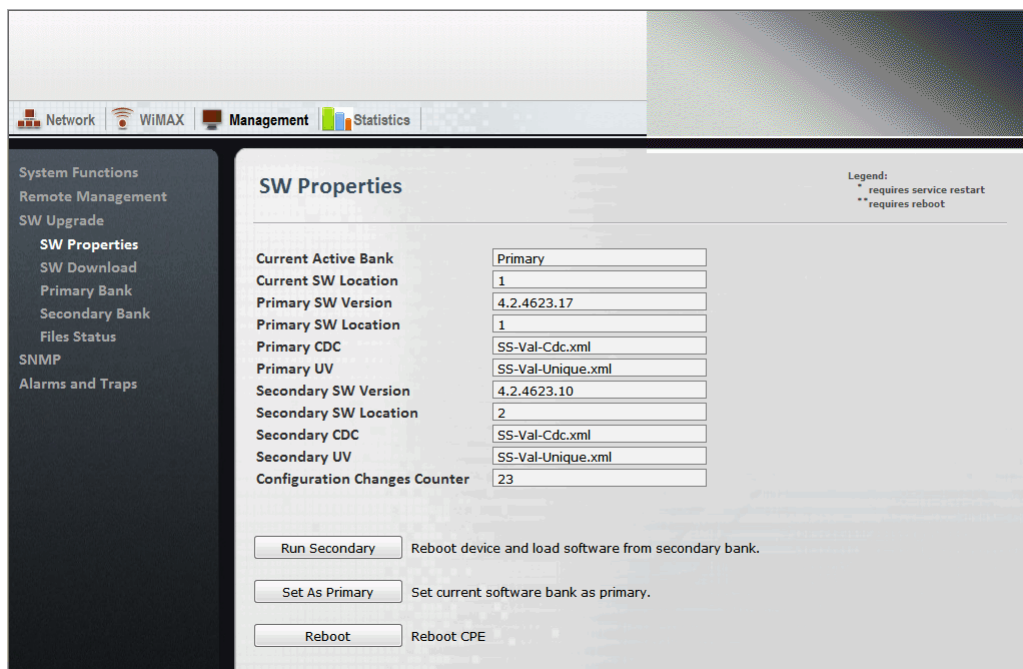


Figure 6.8. SW Properties pane

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

Field	Description
Current Active Bank	Displays the name of the memory bank from which the CPE software is running. Values: Primary   Secondary
Current SW Location	Displays the number of the memory bank from which the CPE software is running. Values: 1   2
Primary SW Version	Displays the version number of the software in the Primary memory bank.
Primary SW Location	Displays the number of the current Primary memory bank. Values: 1   2
Primary CDC	Displays the filename of the CDC (Customer Defaults Configuration) file in the Primary memory bank.
Primary UV	Displays the filename of the UV (Unique Value) file in the Primary memory bank.
Secondary SW Version	Displays the version number of the software in the Secondary memory bank.
Secondary SW Location	Displays the number of the memory bank selected as the Secondary memory bank.

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

**Table 6.3. SW Properties**

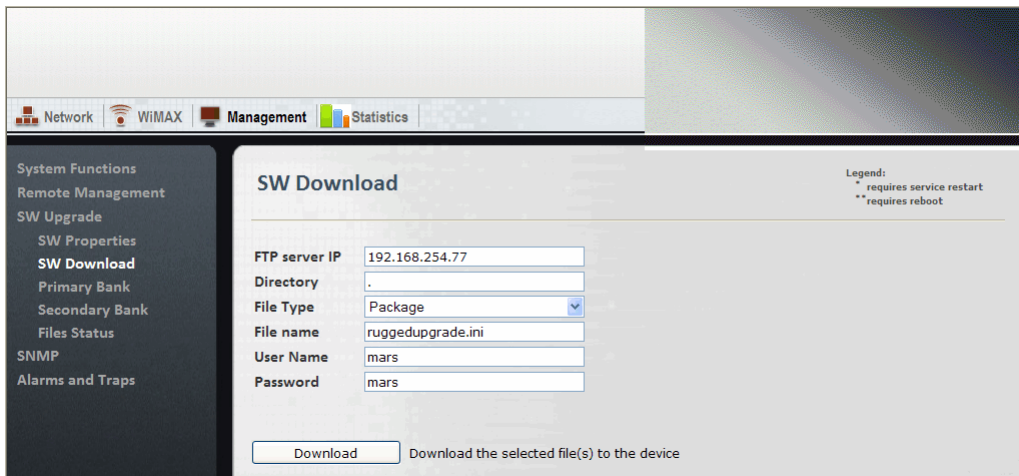
- The following operations can be performed from this pane:
  - Run Secondary** — Reboot the CPE and run the “Secondary” software image. Reboot a second time to run the CPE using the “Primary” software image.
  - Set as Primary** — Set the current running software as the “Primary” image. For example, if the CPE is running from the “Secondary” image, the “Primary” and “Secondary” designations are exchanged.
  - Reboot** — Reboot the CPE and run the “Primary” image.

### 6.2.4.3. Downloading CPE Software

Use the **SW Download** pane to download CPE software from your FTP server. The CPE downloads all software to the “Secondary” memory bank.

#### Procedure 6.7. Downloading software

- Click the **Management** button. The **Current Status** pane appears.
- In the options pane, click the **SW Upgrade** link, and then click the **SW Download** link. The **SW Download** pane appears.



**Figure 6.9. SW Download pane**

- Set the download parameters in the following fields:

Field	Description
FTP Server IP	Type the IPv4 address for the FTP server from which the CPE software is to be downloaded.
Directory	Type the directory path to the CPE software on the FTP server.
File Type	Select the type of file to download:

Field	Description
	<ul style="list-style-type: none"><li>• Package — The software package file provided with an upgrade package. For example: ruggedupgrade.ini</li><li>• Web Resource — A web console template file. For example: web.rc</li><li>• CDC — A Common Default Configuration file. For example: BS-Val-Cdc.xml</li><li>• UV — A Unique Value file. For example: BS-Val-Unique.xml</li></ul>
File Name	Type the name of the file you want to download.
User Name	Type the user name used to log in to the FTP server.
Password	Type the password used to log in to the FTP server.

**Table 6.4. Download Parameters**

4. Click the **Download** button. The CPE downloads the specified file from the FTP server directory to the “Secondary” memory bank.

### 6.2.4.4. Managing the Primary Memory Bank

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

Before uploading files to an FTP server, you must configure an FTP server on the **SW Download** pane. For instructions on how to configure the FTP server properties, see [Section 6.2.4.3, “Downloading CPE Software”](#).

#### **Procedure 6.8. Viewing files in the Primary memory bank**

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

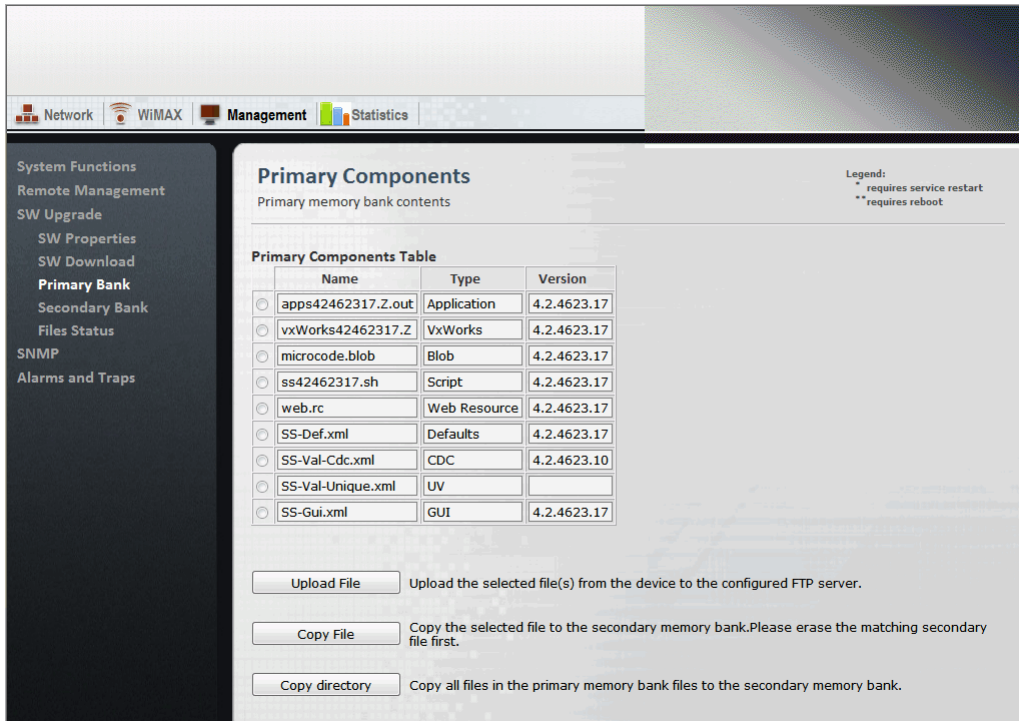


Figure 6.10. Primary Bank Components pane

- The **Primary Components Table** displays the following information:

Field	Description
Name	Displays the software component filename.
Type	Displays the software component file type. Values: Package   Application   VxWorks   Blob   Script   WebResource   Defaults   CDC   Regulation   UV   GUI
Version	Displays the software component version number.

Table 6.5. Primary Components Table

- To upload a file to your FTP server:

**i** Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, see [Section 6.2.4.3, “Downloading CPE Software”](#).

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

- To copy a file to the “Secondary” memory bank:

**i** Before copying the file, ensure that it does not already exist in the “Secondary” memory bank. If the file is present in the “Secondary” memory bank, delete the file from the “Secondary” memory bank before copying. For instructions on how to delete files from the “Secondary” memory bank, see [Section 6.2.4.5, “Managing the Secondary Memory Bank”](#).

- Select a file from the **Primary Components Table**.

- Click the **Copy File**.
6. To copy all files to the “Secondary” memory bank:
- Click the **Copy directory**.

### 6.2.4.5. Managing the Secondary Memory Bank

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

Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, see [Section 6.2.4.3, “Downloading CPE Software”](#).

#### Procedure 6.9. Viewing files in the Secondary memory bank

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

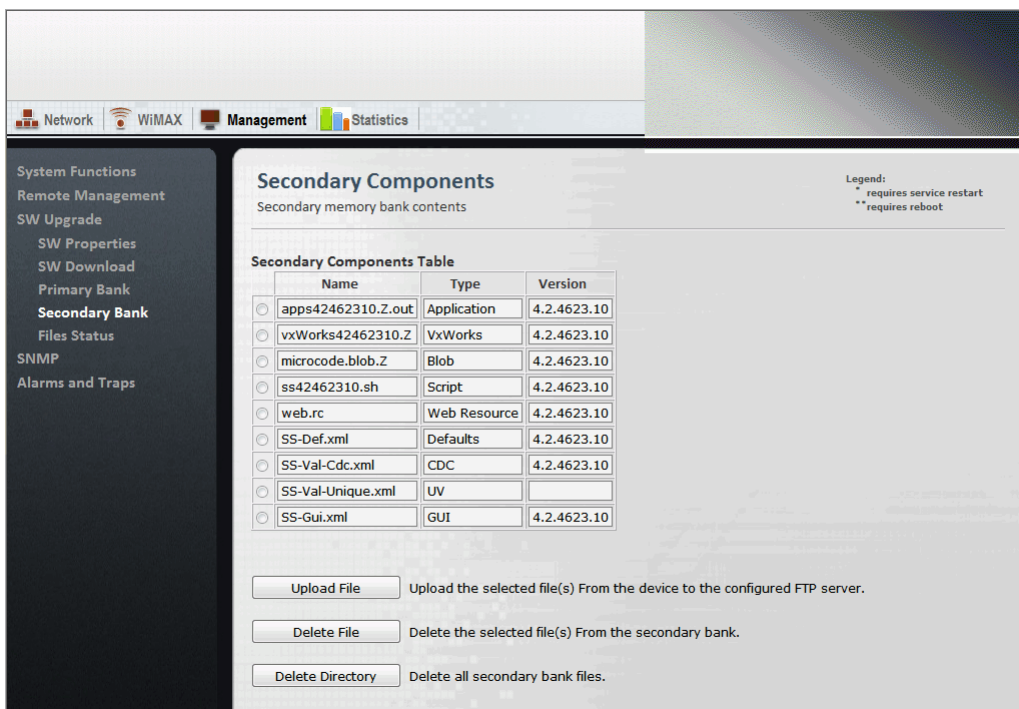


Figure 6.11. Secondary Bank Components pane

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

Field	Description
Name	Displays the software component filename.
Type	Displays the software component file type. Values: Package   Application   VxWorks   Blob   Script   WebResource   Defaults   CDC   Regulation   UV   GUI
Version	Displays the software component version number.

Table 6.6. Secondary Components Table

- To upload a file to your FTP server:



*Before uploading files to an FTP server, you must configure an FTP server on the **FTP Server Properties** pane. For instructions on how to configure the FTP server properties, see [Section 6.2.4.3, “Downloading CPE Software”](#).*

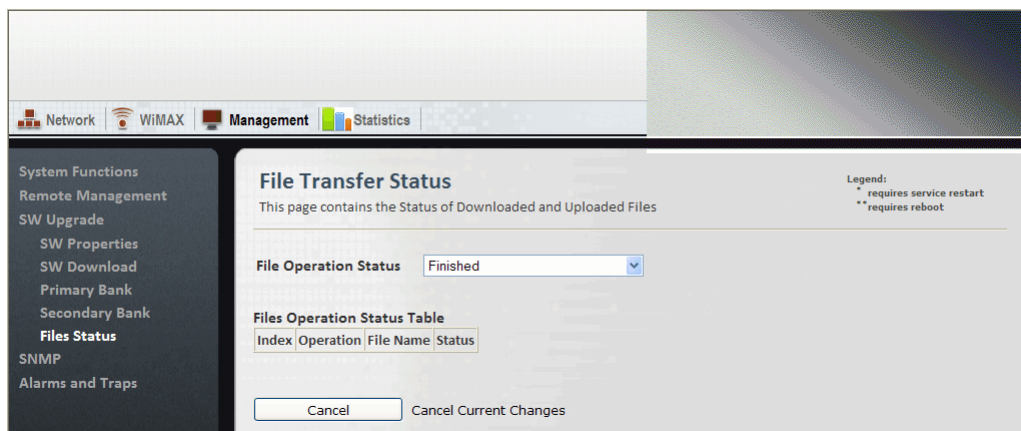
- Select a file from the **Secondary Components Table**.
  - Click the **Upload File**.
- To delete a file:
    - Select a file from the **Secondary Components Table**.
    - Click the **Delete File**.
  - To delete all files:
    - Click the **Delete Directory**.

### 6.2.4.6. File Status

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

#### Procedure 6.10. Viewing File Transfer Status

- Click the **Management** button. The **Current Status** pane appears.
- In the options pane, click the **SW Upgrade** link, and then click the **Files Status** link. The **File Transfer Status** pane appears.



**Figure 6.12. File Transfer Status pane**

- From the **File Operation Status** list, select an operation status:
  - OK — displays successfully completed file transfers.
  - Not Started — displays requested file transfers that have not yet started.
  - In Process — displays file transfers that are currently in progress.
  - Failure — displays failed file transfers.

4. The **File Transfer Operation Status** table displays the following information for the files in the selected operation status:

Field	Description
Index	Displays a unique identifier for the file.
Operation	Displays the file transfer operation performed on the file. Values: Download   Upload   Delete   Copy   Operations (indicates the completion of a batch operation on several files)
File Name	Displays the filename for the uploaded or downloaded file.
Status	Displays the status of the file transfer operation. Values: OK   Not Started   In Process   Failure

**Table 6.7. File Transfer Operation Status table**

5. To cancel a download or upload operation that is currently in progress:
  - Click the **Cancel** button.

### 6.2.5. SNMP Administration

In SNMP administration, you configure SNMP communities, trap destinations, and MIB2 system identification parameters.

For instructions on setting SNMP communities and trap destinations, see [Section 6.2.5.1, “SNMP Communities and Trap Destination Addresses”](#).

For instructions on setting the MIB2 system identification information, see [Section 6.2.5.2, “MIB2 System”](#).

#### 6.2.5.1. SNMP Communities and Trap Destination Addresses

On the **SNMPv2c Access Settings** pane, configure the SNMP communities and set the SNMP trap destinations. You can specify up to five trap destination addresses.

##### Procedure 6.11. Setting the SNMPv2c access parameters

1. Click the **Management** button. The **Management** options appear in the options pane.
2. In the options pane, click the **SNMP** link, and then click the **SNMP Managers** link. The **SNMPv2c Access Settings** pane appears.

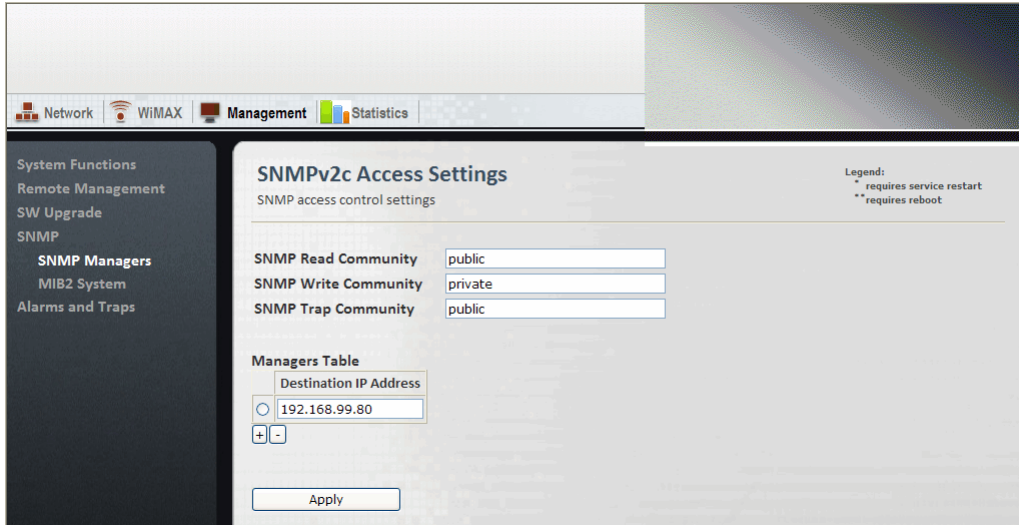





Figure 6.13. SNMPv2c Access Settings pane

- Review and set the SNMPv2c settings in the following fields:

Field	Description
SNMP Read Community	The SNMP community name for read access. This name can be used as a password for secure information retrieval. Type a name in the field. Default: public
SNMP Write Community	The SNMP community name for write access. This name can be used as a password for secure set commands. Type a name in the field. Default: private
SNMP Trap Community	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. Default: public

Table 6.8. SNMPv2c Configuration table

- In the **Managers Table**, add up to five trap destination addresses:
  - Click the  button. A new row appears in the **Managers Table**.
  - Type an IP address in the new row.
- To remove an SNMP trap destination, select a row and click the  button. If no rows are selected, clicking the  button removes the last entry in the table.
- Click the **Apply** button.

### 6.2.5.2. MIB2 System

The SNMP MIB2 settings provide subscriber station system identification information.

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

#### Procedure 6.12. Setting SNMP MIB2 system identification information

- Click the **Admin** button. The **Admin** options appear in the options pane.



- In the options panel, click the **SNMP** link, and then click the **MIB2 System** link. The **SNMP - MIB2 Settings** pane appears.

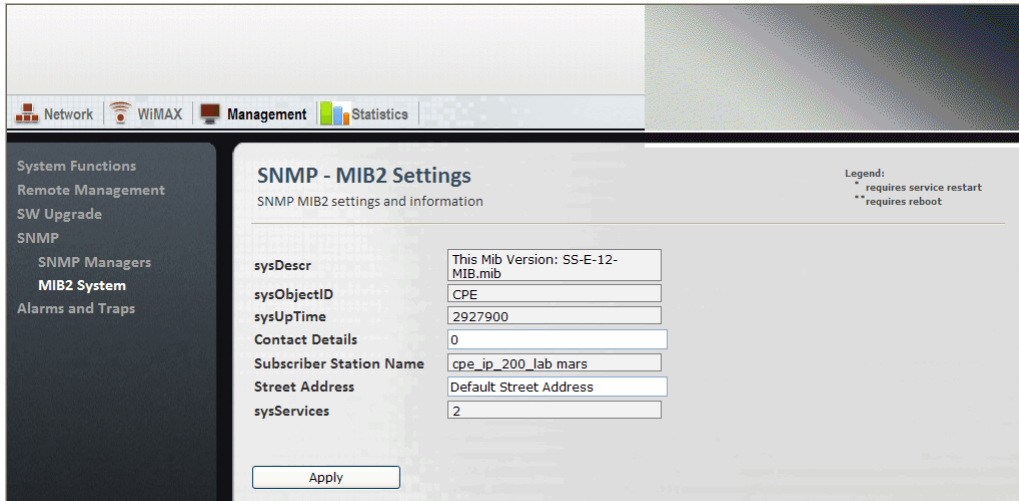


Figure 6.14. SNMP MIB2 Settings pane

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

Field	Description
sysDescr	Displays the SNMP MIB version. Default: This MIB version: BS-E-12-MIB.mib
sysObjectID	Displays the private enterprise number and object identifier for the subscriber station SNMP subsystem. Default: .1.3.6.1.4.1.15004.2.7.1
sysUpTime	Displays the length of time, in hundredths of a second, since the SNMP subsystem was last initialized.
Contact Details	Contains subscriber station contact information. Type a name and contact details, such as an e-mail address, in this field.
Subscriber Station Name	Contains the subscriber station name. Type a descriptive name in this field.
Street Address	Contains the subscriber station street address or location. Type an address or location in this field.
sysServices	Displays a value indicating the set of services provided by the system. The value 2 indicates the datalink/subnetwork layer.

Table 6.9. MIB2 System Table

- Click the **Apply** button.

## 6.2.6. Alarms & Traps

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

### 6.2.6.1. System Alarms

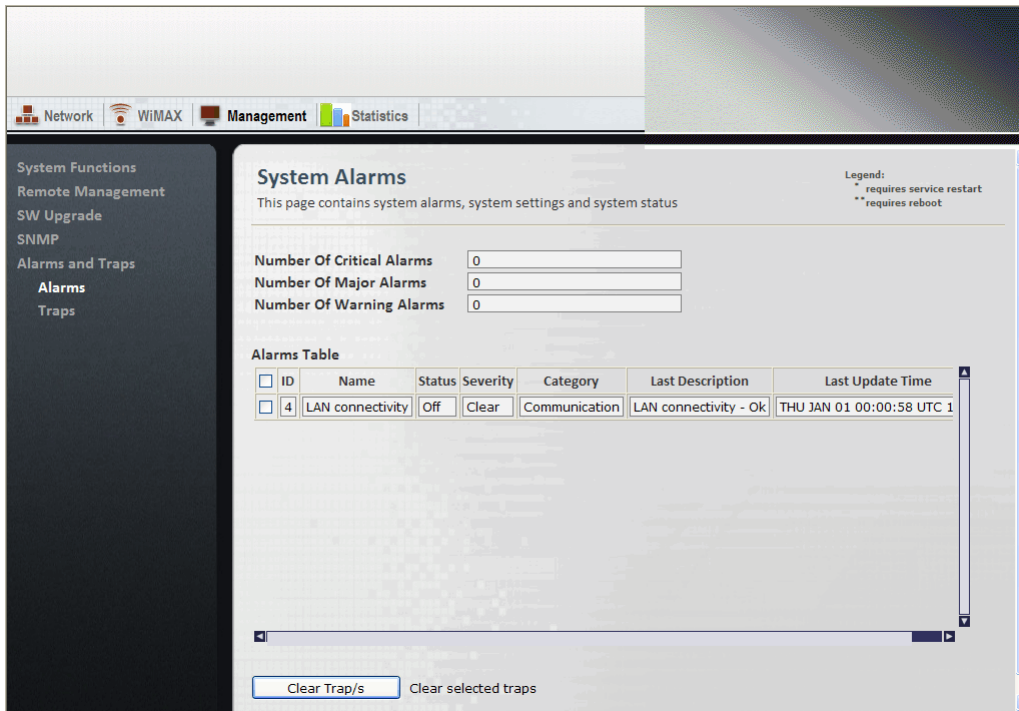
The **System Alarms** pane displays current system alarms. This pane is read-only; there are no parameters to set on this pane.

#### Procedure 6.13. Viewing System Alarms

- Click the **Management** button. The **Management** options appear in the options pane.

## 6. CPE Management Interface

- In the options panel, click the **Alarms and Traps** link. The **System Alarms** pane appears.



**Figure 6.15. System Alarms pane**

- Review the current number of alarms in the following fields:

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

**Table 6.10. System Alarms**

- Review the current alarm settings in the Alarms Table:

Column	Description
ID	Displays the alarm type identification number.
Name	Displays the alarm type. For a list of alarm and trap conditions, see <a href="#">Section 6.2.6.3, "SNMP Traps List"</a> .
Status	Indicates if the alarm type is enabled or disabled. Values: Off   On
Severity	Displays the severity of the alarm. Values: Clear   Critical   Major   Warning
Category	Displays the category for the alarm type. Values: Restart   Communication   RF   Hardware   Security   Environmental   Redundancy   Services   Link Status
Last Description	Displays a message describing the alarm.
Last Update Time	Displays the date and time of the most recent alarm.

**Table 6.11. Alarms Table**

### 6.2.6.2. SNMP Trap Settings

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

**i** *To send traps, you must have SNMP Trap Destinations configured. For instructions on configuring SNMP Trap Destinations, see [Section 6.2.5.1, “SNMP Communities and Trap Destination Addresses”](#)*

#### Procedure 6.14. Setting SNMP traps

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

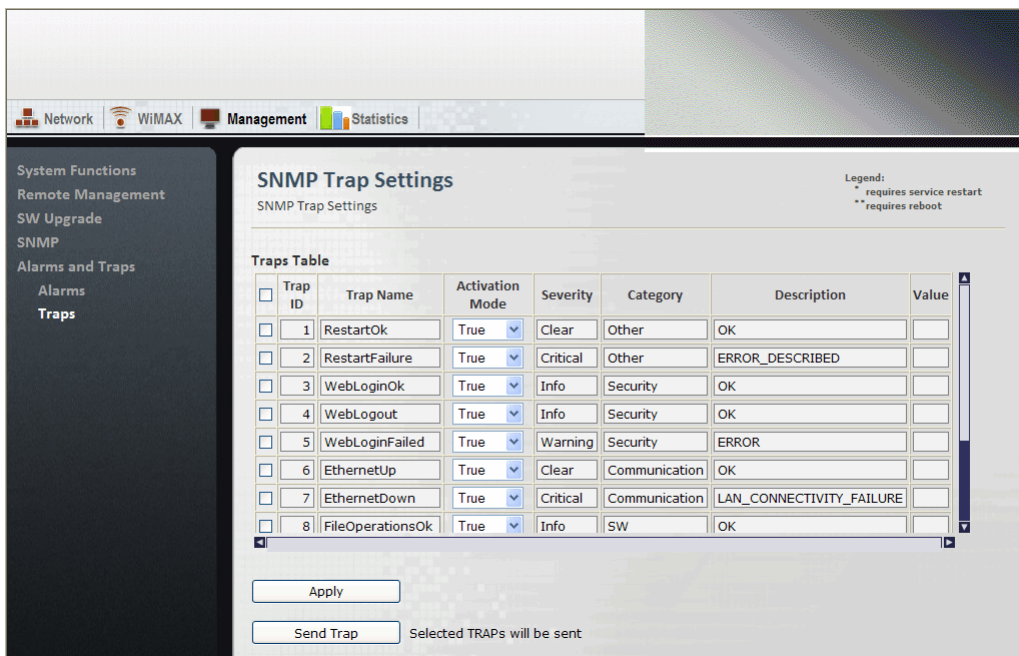


Figure 6.16. SNMP Trap Settings

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

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

Table 6.12. Traps Table

4. Click the **Apply** button.

For testing purposes, you can send selected traps on demand. To send traps, you must have SNMP Trap Destinations configured. For instructions on configuring SNMP Trap Destinations, see [Section 6.2.5.1, “SNMP Communities and Trap Destination Addresses”](#).

### **Procedure 6.15. Sending SNMP traps on demand**

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

### 6.2.6.3. SNMP Traps List

Event Name	Description
RestartOK	The subscriber station restarted successfully.
RestartFailure	The subscriber station failed to restart. This event reports all causes of initialization errors.
WebLoginOK	Web interface login was successful.
WebLogout	Web interface logout.
WebLoginFailed	Web login has failed for 10 consecutive attempts.
EthernetUp	Ethernet link is up.
EthernetDown	Ethernet link is down.
FileOperationsOK	File operations are successful.
FileOperationsFail	File operations failed.
ConfigChanged	Configuration was changed successfully.
DuplicateNsilp	Duplicate LAN IP address.
DuplicateRfilp	Duplicate RF IP address.

**Table 6.13. SNMP Traps List**

## 6.3. CPE Network Configuration

This section describes how to:

- set the CPE LAN and RF IP settings. See [Section 6.3.1, “ Network IP Settings ”](#).
- set the CPE Ethernet settings. See [Section 6.3.2, “ Ethernet Settings ”](#).

### 6.3.1. Network IP Settings

On the the **IP Settings** pane, configure the CPE’s LAN and RF IP addresses.

- Use the LAN IP address when you access the CPE through a direct connection to its physical Ethernet port.
- Use the RF IP address when you access the CPE through the RF network.

#### Procedure 6.16. Configuring the IP Settings

1. Click the **Network** button. The **IP Settings** pane appears.

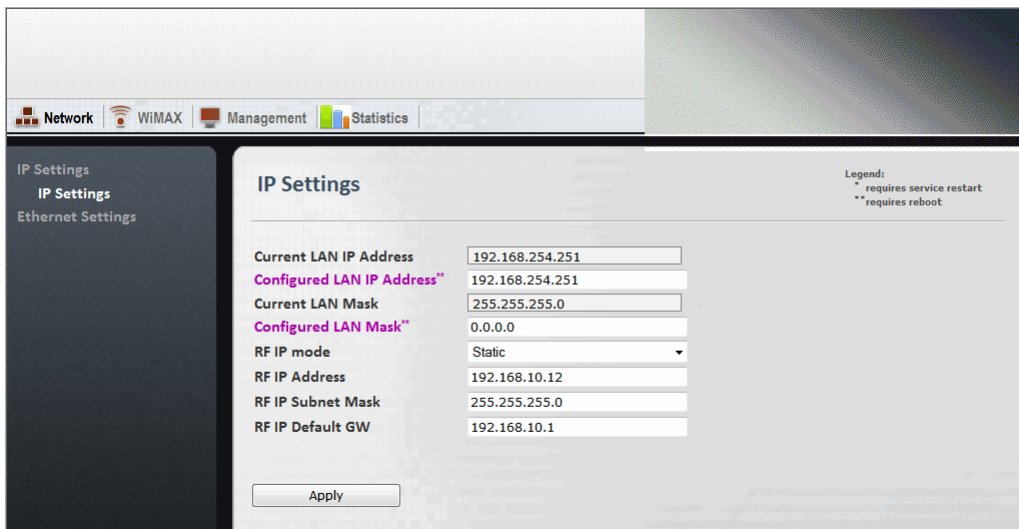


Figure 6.17. IP Settings pane

2. View and configure the LAN and RF IP settings in the following fields:

Field	Description
Current LAN IP Address	Displays the currently configured CPE LAN IP address.
Configured LAN IP Address	To change the LAN IP address, type an IPv4 address in this field. After changing this field, you must reboot the CPE.
Current LAN Mask	Displays the currently configured LAN netmask.
Configured LAN Mask	To change the LAN mask, type a dotted-decimal mask in this field. After changing this field, you must reboot the CPE.
RF IP mode	Displays the RF IP mode: Static or DHCP. To change the mode, select a value from the list.
RF IP Address	Displays the RF IP address. To change the address, type an IPv4 address in this field.
RF IP Subnet Mask	Displays the RF IP subnet mask. To change the subnet mask, type a dotted-decimal mask in this field.
RF IP Default Gateway	Displays the RF default gateway. To change the gateway, type an IPv4 address in this field.

Table 6.14. IP Settings fields

3. Click the **Apply** button.

4. If you changed the value in the **Configured LAN IP Address** or **Configured LAN Mask** fields, reboot the base station:
  - a. Click the **Management** button. The **System Functions** pane appears.
  - b. Click the **Reboot** button. The CPE reboots.

### 6.3.2. Ethernet Settings

On the **Ethernet Settings** panes, you configure VLAN tagging, the MAC address table, and MTU parameters:

- [Section 6.3.2.1, “Configuring VLAN Tagging”](#)
- [Section 6.3.2.2, “Configuring the MAC Address Table”](#)
- [Section 6.3.2.3, “Configuring the MTU”](#)

#### 6.3.2.1. Configuring VLAN Tagging

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

#### Procedure 6.17. Setting the VLAN Tagging Parameters

1. Click the **Network** button. The **IP Settings** pane appears.
2. In the options panel, click the **Ethernet Settings** link. The **VLAN Tagging** pane appears.

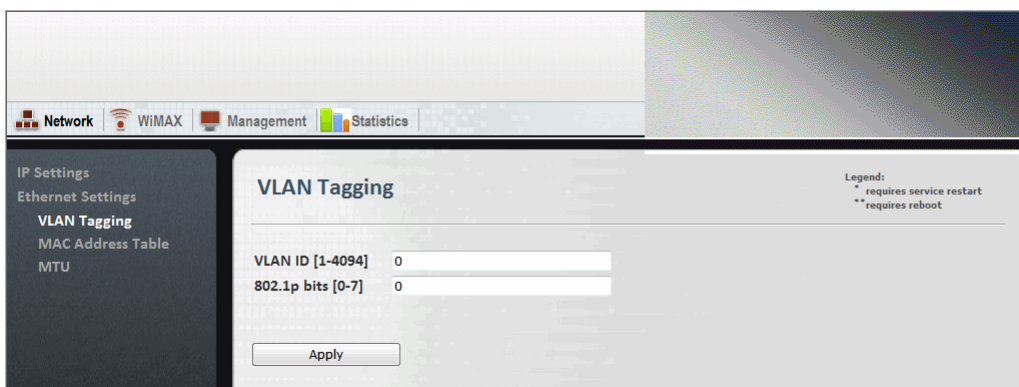


Figure 6.18. VLAN Tagging pane

3. View and configure the LAN and RF IP settings in the following fields:

Field	Description
VLAN ID [1-4094]	Displays an identifier for the management VLAN. Values: A number in the range of 1 to 4094. Default: 0
802.1p bits [0-7]	Sets the 802.1p priority value for the management VLAN. Type a value from 0 to 7. Values: A number in the range of 0 to 7 Default: 0

Table 6.15. IP Settings fields

4. Click the **Apply** button.

5. If you changed the value in the **Configured LAN IP Address** or **Configured LAN Mask** fields, reboot the base station:
  - a. Click the **Management** button. The **System Functions** pane appears.
  - b. Click the **Reboot** button. The CPE reboots.

### 6.3.2.2. Configuring the MAC Address Table

The MAC Address Table displays the MAC addresses learned by the CPE. On the **MAC Address Table** pane, you can set the MAC address aging time and clear the MAC Address Table.

#### Procedure 6.18. Managing the the MAC Address Table

1. Click the **Network** button. The **IP Settings** pane appears.
2. In the options panel, click the **Ethernet Settings** link, and then click the **MAC Address Table** link. The **MAC Address Table** pane appears.

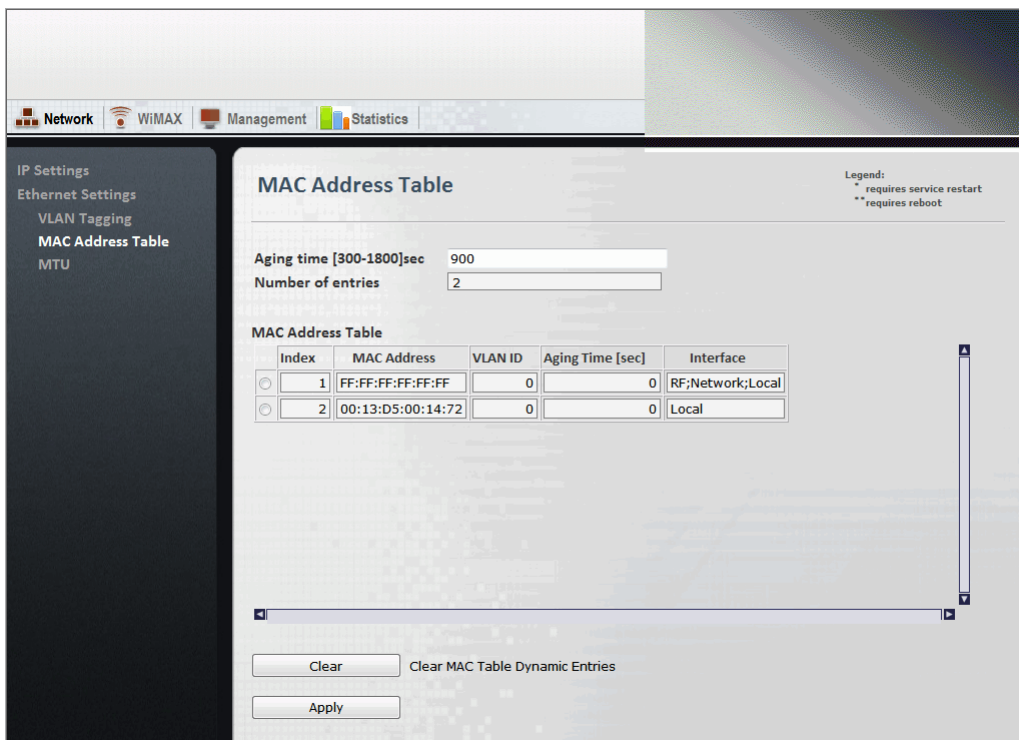


Figure 6.19. MAC Address Table pane

3. In the **Aging time [300-1800] sec** field, set the MAC address aging time. This is the time until table entries are removed from the MAC address table. Type a value in the range of 300 to 1800 seconds.
4. The MAC Address Table displays the following information:

Field	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 [sec]	Displays the time, in seconds, until the entry will be removed from the table.

Field	Description
Interface	<p>Displays the interface from which the CPE learned the MAC address. Possible values include:</p> <ul style="list-style-type: none"> <li>• Network — the base station acquired the address from the Ethernet network interface</li> <li>• RF — the base station acquired the address from the RF interface</li> <li>• Local — indicates the MAC address of the base station itself</li> </ul>

**Table 6.16. IP Settings fields**

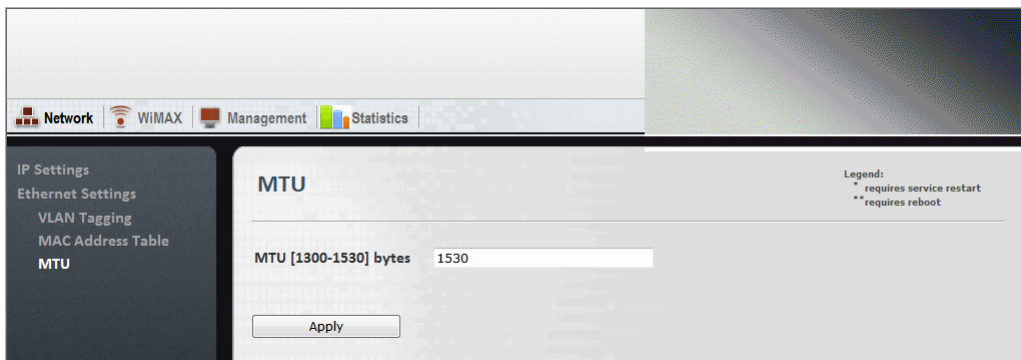
- To remove an entry from the MAC address table, select a row in the table and click the **Clear** button.
- After changing the Aging time [300-1800] sec field, click the **Apply** button.

### 6.3.2.3. Configuring the MTU

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

#### Procedure 6.19. Setting the MTU

- Click the **Network** button. The **IP Settings** pane appears.
- In the options panel, click the **Ethernet Settings** link, and then click the **MTU** link. The **MTU** pane appears.



**Figure 6.20. MTU pane**

- In the **MTU [1300-1530] bytes** field, set the MTU value. Type a value in the range of 1300 to 1530 bytes. The default value is 1530.
- Click the **Apply** button.



## 6.4. CPE Statistics

This section describes how to:

- view general CPE system statistics. See [Section 6.4.1, “ General Statistics ”](#).
- view and clear CPE RF statistics. See [Section 6.4.2, “ RF Statistics ”](#).
- view and clear network statistics. See [Section 6.4.3, “ Network Statistics ”](#).
- view and clear service flow statistics. See [Section 6.4.4, “ Service Flow Statistics ”](#).

### 6.4.1. General Statistics

On the the **General Statistics** pane, you can review general CPE status and information. The **General Statistics** pane is read-only; there are no parameters to set on this pane.

#### Procedure 6.20. Viewing General Statistics

1. Click the **Statistics** button. The **General Statistics** pane appears.

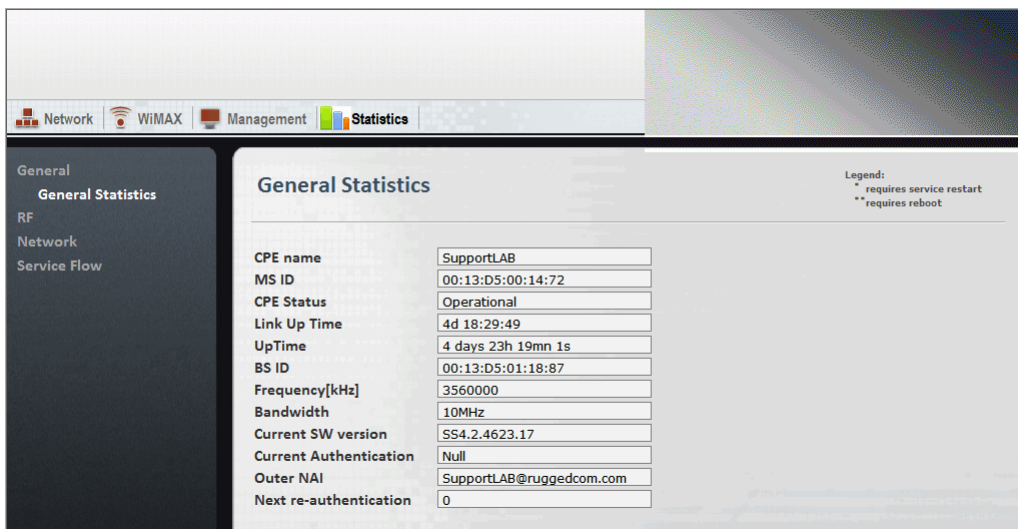


Figure 6.21. General Statistics pane

2. View the CPE general information in the following fields:

Field	Description
CPE Name	Displays the name of the CPE. This name identifies the CPE on the base station and in the base station management interface. The name is set on the <b>System Functions</b> pane. For instructions on how to set the name, see <a href="#">Section 6.2.1, “Managing System Functions”</a> .
MS ID	Displays the mobile station MAC address.
CPE Status	Displays the current CPE status. Values: Init   DL Synchronization   Handover DL acquisition   UL Acquisition   Ranging   Handover ranging   Capabilities negotiation   Authorization   Registration   DHCP   TOD   TFTP   Operational   Sleep   IDLE   Aborted
Up Time	Displays the time since the last CPE start-up.
BS ID	Displays the base station MAC address.
Frequency [kHz]	Displays the CPE broadcast frequency, in kilohertz.
Bandwidth	Displays CPE bandwidth setting. Values: 3.5MHz   5MHz   10MHz

Field	Description
Current SW version	Displays the current CPE software version number.
Current Authentication	Displays the current CPE authentication mode. Values: Null   EAP-TTLS   EAP-TLS
Outer NAI	Displays the outer network access identifier.
Next re-authentication	

**Table 6.17. General Statistics fields**

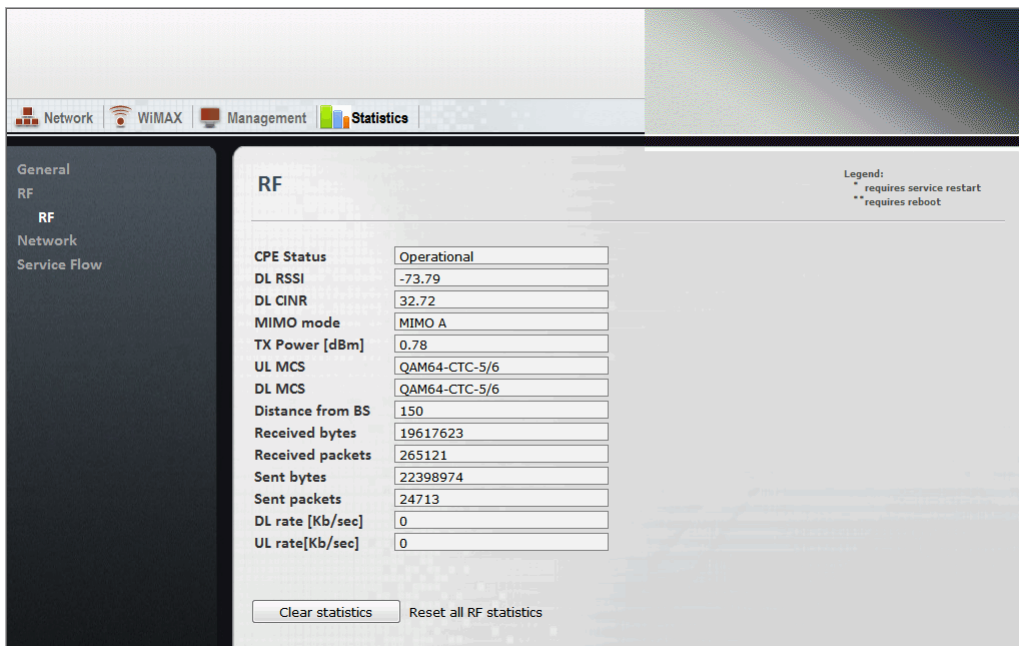
### 6.4.2. RF Statistics

On the the **RF Statistics** pane, you can review CPE RF status and information. The **RF Statistics** pane is read-only; there are no parameters to set on this pane.

#### Procedure 6.21. Viewing RF Statistics

1. Click the **Statistics** button. The **General Statistics** pane appears.

In the options panel, click the **RF** link. The **RF** pane appears.



**Figure 6.22. RF pane**

2. View the CPE RF statistics in the following fields:

Field	Description
CPE Status	Displays the current CPE status. Values: Init   DL Synchronization   Handover DL acquisition   UL Acquisition   Ranging   Handover ranging   Capabilities negotiation   Authorization   Registration   DHCP   TOD   TFTP   Operational   Sleep   IDLE   Aborted
DL RSSI	Displays the downlink received signal strength, in dBm.
DL CINR	Displays the downlink carrier to interference and noise ratio, in dBm.
MIMO mode	Displays the CPE Multiple-Input, Multiple-Output mode. Values: SISO   MIMO A   MIMO B
TX Power [dBm]	Displays the CPE transmission power, in dBm.
UL MCS	Displays the uplink Modulation and Coding Scheme.

Field	Description
	Values: 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
DL MCS	Displays the downlink Modulation and Coding Scheme. Values: 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
Distance from BS	Displays the estimated distance of the CPE from the base station, in meters.
Received bytes	Displays the amount of data received by the CPE, in bytes.
Received packets	Displays the number of packets received by the CPE.
Sent bytes	Displays amount of data sent by the CPE, in bytes.
Sent packets	Displays the number of packets sent by the CPE.
DL rate [Kb/sec]	Displays the downlink rate, in kilobits per second.
UL rate [Kb/sec]	Displays the uplink rate, in kilobits per second.

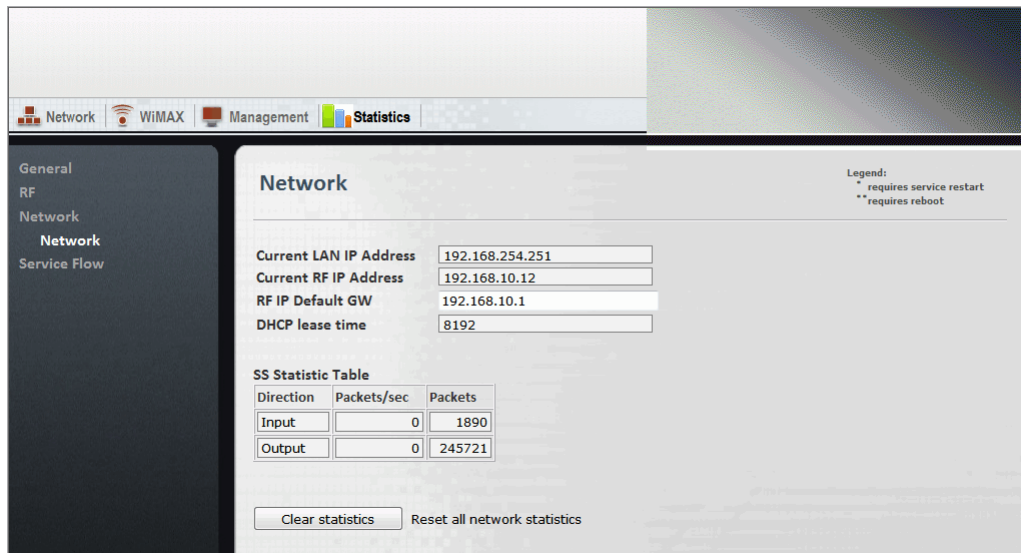
**Table 6.18. RF Statistics fields**

### 6.4.3. Network Statistics

On the the **Network** pane, you can review LAN and RF network information and statistics. On this pane, you can clear the network statistics.

#### Procedure 6.22. Viewing Network Statistics

1. Click the **Statistics** button. The **General Statistics** pane appears.  
In the options panel, click the **Network** link. The **Network** pane appears.



**Figure 6.23. Network pane**

2. View the LAN and RF network information in the following fields:

Field	Description
Current LAN IP Address	Displays the current CPE LAN IP address. Use the LAN IP address when you access the CPE through a direct connection to its physical Ethernet port.
Current RF IP Address	Displays the current CPE RF IP address. Use the RF IP address when you access the CPE through the RF network.
RF IP Default GW	Displays the CPE default gateway on the RF network.

Field	Description
DHCP Lease Time	Displays the CPE default DHCP lease time.

**Table 6.19. Network Statistics fields**

- View the network statistics in the **SS Statistic Table**:

Field	Description
Direction	Displays the direction of network traffic to and from the CPE: Input or Output.
Packets/sec	Displays the packet transmission rate for inbound and outbound traffic, in packets per second.
Packets	Displays the total number of inbound and outbound packets.

**Table 6.20. SS Statistic Table**

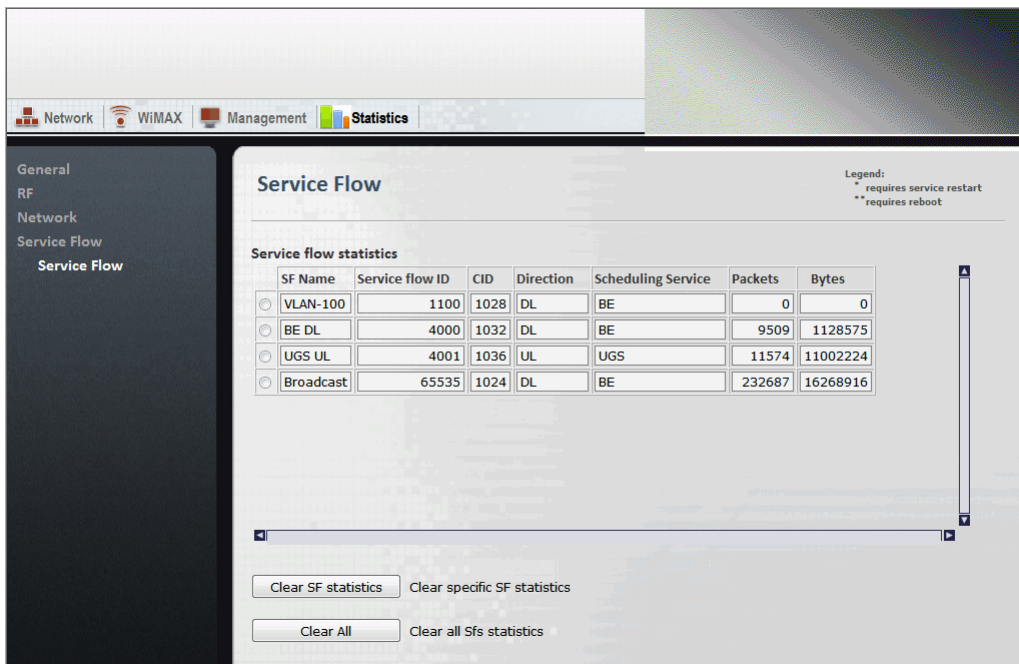
- To clear the SS Statistics Table, click the **Clear statistics** button.

### 6.4.4. Service Flow Statistics

On the the **Service Flow** pane, you can review service flow statistics for each service flow defined on the CPE. Each row in the **Service flow statistics** table displays information for a service flow. On this pane, you can clear the statistics all of the service flows or for selected service flows.

#### Procedure 6.23. Viewing Service Flow Statistics

- Click the **Statistics** button. The **General Statistics** pane appears.
- In the options panel, click the **Service Flow** link. The **Service Flow** pane appears.



**Figure 6.24. Network pane**

- View the service flow statistics in the **Service flow statistics** table:

Field	Description
SF Name	Displays the name of the service flow.
Service flow ID	Displays a numeric identifier for the service flow.

Field	Description
CID	Displays the connection identifier for the service flow.
Direction	Displays the direction for the service flow: uplink or downlink. Values: DL   UL
Scheduling Service	Displays the scheduling service for the service flow: Best Effort, Near-Real Time, Real Time, Extended Real Time, or Unsolicited Grant Service. Values: BE   nRT   RT   eRT   UGS
Packets	Displays the number of packets handled by the service flow.
Bytes	Displays the number of bytes handled by the service flow.

**Table 6.21. Service flow statistics Table**

4. To clear the statistics for a selected service flow, select the service flow in the **Service flow statistics** table and click the **Clear SF statistics** button.
5. To clear the statistics for all service flows, click the **Clear All** button.

## 6.5. WiMAX Settings

This section describes how to:

- configure the scanner settings. See [Section 6.5.1, “Scanner Settings”](#).
- configure WiMAX authentication. See [Section 6.5.2, “WiMAX Authentication”](#).
- view information for the serving and neighboring base stations. See [Section 6.5.3, “Viewing Base Station Information”](#).
- configure the WiMAX radio options. See [Section 6.5.4, “Configuring WiMAX Radio Parameters”](#).

### 6.5.1. Scanner Settings

On the the **Scanner Settings** pane, you set the CINR (Carrier to Interference + Noise Ratio) value and define the scanning frequencies for the CPE. The CPE uses this information to scan for and locate available base stations.

During the scan, the CPE builds a table of detected base stations. If the CPE finds a base station with a CINR greater than the user-defined threshold, it stops the scan and connects to the base station immediately. This technique scanning time.

On this pane, you can also start and stop CPE’s scan for base stations.

#### Procedure 6.24. Working with WiMAX Scanner Settings

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.

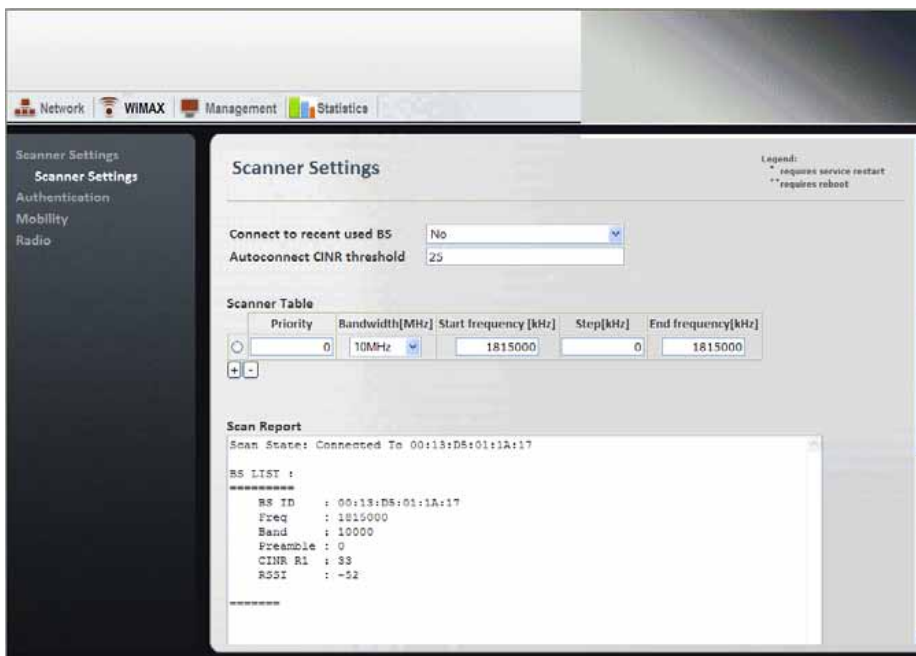




Figure 6.25. Scanner Settings pane

2. The **Autoconnect CINR threshold** field displays the Carrier to Interference + Noise Ratio threshold.
3. The **Connect to recent used BS** field can be set to connect to a recently used base station. The default option is **No**.

4. The **Scanner Table** lists the frequencies scanned by the CPE to locate its base station. The **Scanner Table** displays the following information:

Column	Description
Priority	Sets the priority for the scanning table entry. Priority is ranked in numeric order. Values: A numeric value.
Bandwidth [MHz]	Displays the bandwidth of the scanning table entry. Values: 3.5MHz   5MHz   10MHz
Start frequency [kHz]	Displays the start of the scanning range as a frequency in kilohertz.
Step [kHz]	Displays scanning increment in the scanning range, in kilohertz.
End frequency [kHz]	Displays the end of the scanning range as a frequency in kilohertz.

**Table 6.22. Scanner Table fields**

5. The **Scan Report** field displays a list of base stations located by the scan. The list includes the following information for each base station:
- the base station MAC address
  - the base station frequency
  - the base station bandwidth
  - the transmission preamble
  - the CINR R1 value
  - the RSSI value, in dBm
6. To add an entry to the **Scanner Table**, click the  button. A new row appears in the table. You can add up to 32 rows to the table.
- Set the values for the new scanning range in the **Priority**, **Bandwidth [MHz]**, **Start frequency [kHz]**, **Step [kHz]**, and **End frequency [kHz]** fields.
7. To remove a row from the table, select the row and click the  button. The row is removed from the table.
8. After adding or editing rows in the **Scan Report** table, or after changing the values in the **Autoconnect CINR threshold** or **Connect to recent used BS** fields, click the **Apply** button.
9. To begin scanning for base stations, click the **Connect** button.
10. To stop scanning for base stations, click the **Disconnect** button.
11. To delete all scanning configuration information, click the **Delete All** button.

## 6.5.2. WiMAX Authentication

On the the **Authentication** panes, you set view and set the WiMAX authentication parameters. The CPE supports EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) and EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) authentication. You can also set the CPE to use null (no) authentication.

This section describes how to:

- view the current CPE authentication setting. See [Section 6.5.2.1, “Viewing the CPE Authentication Method”](#).
- configure EAP-TLS authentication. See [Section 6.5.2.2, “Configuring EAP-TLS Authentication”](#).
- configure EAP-TLLS authentication. See [Section 6.5.2.3, “Configuring EAP-TTLLS Authentication”](#).
- configure null authentication. See [Section 6.5.2.4, “Configuring Null Authentication”](#).
- view the authentication certificate filenames. See [Section 6.5.2.5, “Viewing Authentication Certificates”](#).

### 6.5.2.1. Viewing the CPE Authentication Method

The **Authentication Setting** pane displays the current CPE WiMAX authentication configuration. The **Authentication Setting** pane is read-only; there are no parameters to set on this pane.

#### Procedure 6.25. Viewing CPE Authentication

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Authentication** link. The **Authentication Method** pane appears.
3. On the **Authentication Method** pane, click the **Show Settings** button. The **Authentication Setting** pane appears.

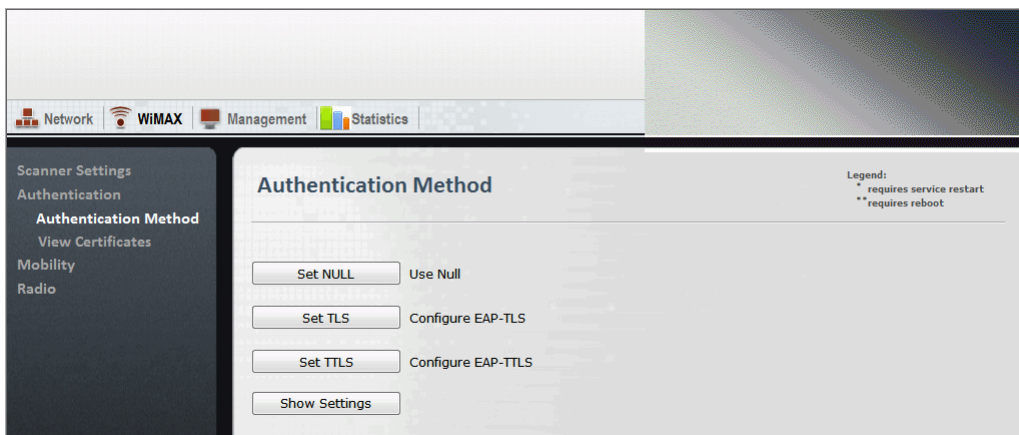


Figure 6.26. Authentication Setting pane

4. The **Configured Authentication** field displays the current configuration setting: Null or EAP.
5. The **Outer NAI** field displays the outer Network Access Identifier.



### 6.5.2.2. Configuring EAP-TLS Authentication

On the EAP-TLS pane, you configure Extensible Authentication Protocol - Transport Layer Security authentication by specifying the authentication realm. After configuring EAP-TLS, you must reboot the CPE.

#### Procedure 6.26. Configuring EAP-TLS

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Authentication** link. The **Authentication Method** pane appears.
3. On the **Authentication Method** pane, click the **Set TLS** button. The **EAP TLS** pane appears.

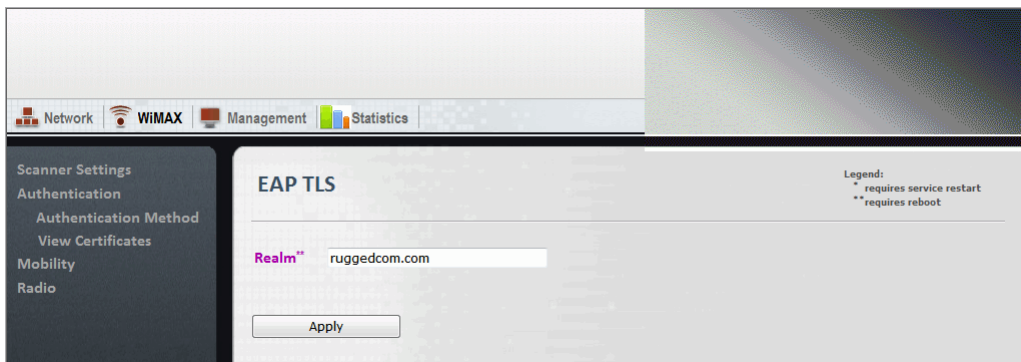


Figure 6.27. EAP TLS pane

4. In the **Realm** field, type the authentication realm.
5. After changing the **Realm** field, reboot the CPE:
  - a. Click the **Management** button. The **System Functions** pane appears.
  - b. Click the **Reboot** button. The CPE reboots.

### 6.5.2.3. Configuring EAP-TTLS Authentication

On the EAP-TTLS pane, you configure Extensible Authentication Protocol - Tunneled Transport Layer Security authentication by specifying the authentication realm and a username and password. After configuring EAP-TTLS, you must reboot the CPE.

#### Procedure 6.27. Configuring EAP-TTLS

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Authentication** link. The **Authentication Method** pane appears.
3. On the **Authentication Method** pane, click the **Set TTLS** button. The **EAP TTLS** pane appears.

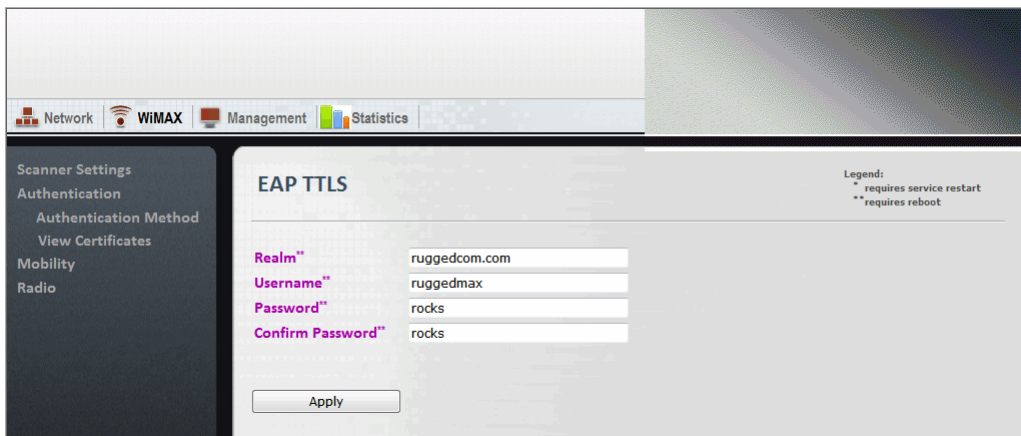


Figure 6.28. EAP TTLS pane

4. Set the EAP-TTLS parameters in the following fields:

Column	Description
Realm	Specify the EAP-TTLS authentication realm.
Username	Specify the EAP-TTLS user name.
Password	Specify the password for the EAP-TTLS user.
Confirm Password	Re-type the password to confirm it.

Table 6.23. EAP-TTLS Authentication fields

5. Click the **Apply** button.
6. After changing any of the fields on the **EAP TTLS** pane, reboot the CPE:
  - a. Click the **Management** button. The **System Functions** pane appears.
  - b. Click the **Reboot** button. The CPE reboots.

### 6.5.2.4. Configuring Null Authentication

You enable null authentication on the **Authentication Method** pane.

#### Procedure 6.28. Enabling Null Authentication

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Authentication** link. The **Authentication Method** pane appears.
3. On the **Authentication Method** pane, click the **Set Null** button.

### 6.5.2.5. Viewing Authentication Certificates

You can view the authentication certificate filenames on the **View Certificates** pane. The **View Certificates** pane is read-only; there are no parameters to set on this pane.

#### Procedure 6.29. Viewing Authentication Certificate Filenames

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Authentication** link and then click the **View Certificates** link. The **View Certificates** pane appears.



Figure 6.29. View Certificates pane

3. The fields on the **View Certificates** pane list the filenames for the Device Certificate, the Device Private Key, the CA Certificate, and the Random Seed file.

### 6.5.3. Viewing Base Station Information

On the **Mobility** pane, you can view information about the base station serving the CPE and information about neighboring base stations. The **Mobility** pane is read-only; there are no parameters to set on this pane.

#### Procedure 6.30. Viewing Base Station Information

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Mobility** link. The **Mobility** pane appears.

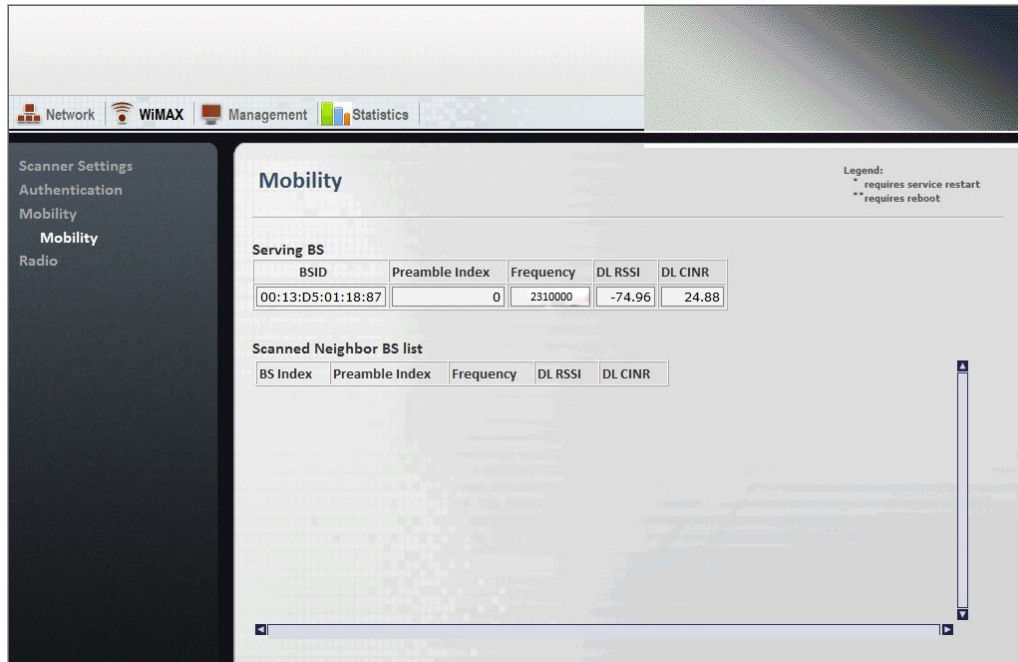


Figure 6.30. Mobility pane

3. The **Serving BS** table displays information about the base station to which the CPE is connected:

Column	Description
BSID	Displays the MAC address of the base station to which the CPE is connected.
Preamble Index	Displays the base station's preamble index.
Frequency	Displays the frequency (According to CPE's frequency band).
DL RSSI	Displays the downlink RSSI (Received Signal Strength Indication).
UL RSSI	Displays the uplink RSSI (Received Signal Strength Indication).

Table 6.24. Serving BS table

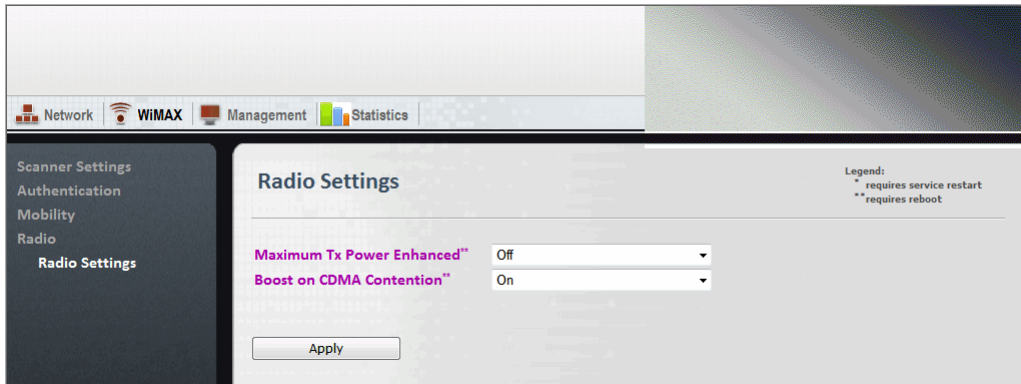
4. The **Scanned Neighbor BS list** table displays information about neighboring base stations detected by the CPE. This table displays the same information for neighboring base stations as that shown in [Table 6.24, "Serving BS table"](#).

### 6.5.4. Configuring WiMAX Radio Parameters

On the **Radio Settings** pane, you can enable and disable WiMAX radio settings. After making changes on the **Radio Settings** pane, you must reboot the CPE.

**Procedure 6.31. Setting WiMAX Radio Parameters (Not available for WCS 2.3GHz)**

1. Click the **WiMAX** button. The **Scanner Settings** pane appears.
2. In the options panel, click the **Radio** link. The **Radio Settings** pane appears.



**Figure 6.31. Radio Settings pane**

3. Set the following WiMAX radio options:

Column	Description
Maximum Tx Power Enhanced	Displays the setting for transmission power enhancement. When <b>On</b> , transmission power is enhanced. When <b>Off</b> , transmission power is not enhanced. The default setting is <b>Off</b> . Values: On   Off
Boost on CDMA Contention	Determines if transmission power is boosted on CDMA (Code Division Multiple Access) contention. When <b>On</b> , transmission power is boosted when another station competes for the same bandwidth. When <b>Off</b> , transmission power is not boosted when the CPE detects contention. The default value is <b>Off</b> . Values: On   Off

**Table 6.25. Radio Settings fields**

4. After making changes, click the **Apply** button.
5. After changing the **Maximum Tx Power Enhanced** or **Boost on CDMA Contention** fields, reboot the CPE:
  - a. Click the **Management** button. The **System Functions** pane appears.
  - b. Click the **Reboot** button. The CPE reboots.

## Appendix A. WiN5100 / WiN5200 Specifications

### Radio and Modem

- Frequency (by CPE Model Number)
  - WiN5124: 1350 MHz to 1525 MHz
  - WiN5218: 1800 MHz to 1830 MHz
  - WiN5123/WiN5223: 2305 MHz to 2320 MHz, 2345 MHz to 2360 MHz
  - WiN5225: 2496 MHz to 2690 MHz
  - WiN5235: 3300 MHz to 3800 MHz
- Radio Access Method: IEEE802.16-2005 (16e OFDMA)
- Operation Mode: TDD
- Compatibility: Wave 2 Profile (MIMO)
- Channel Bandwidth: 3.5 MHz, 5 MHz, 7MHz (not available for WiN5123/WiN5223), 10 MHz
- Frequency Resolution: 0.25 MHz
- Antenna Support: Integrated Dual Slant Antenna
- Antenna Diversity Support: STC / MRC / MIMO
- Output Power (average): 24 dBm +/-1 dB  
(Note: for WCS CPE 2.3GHz the output power is 18 dBm, fixed)
- TPC: 54 dB
- FFT / Modulation: 1024 / 512 FFT points; QPSK, 16 QAM, 64 QAM
- FEC: Convolutional Turbo Code
- Dynamic Range:
  - RX: -100 dBm : -20 dBm
  - TX: -30 dBm : +24 dBm

### Data Communication (Through Indoor Unit)

- Ethernet Standard Compliance: IEEE 802.3 CSMA/CD
- Ethernet Port: 10/100 Mbps, Half / Full Duplex with Auto Negotiation
- Traffic Classification:
  - DSCP/IP TOS Field
  - IP Protocol / Next Header Field
  - IP Masked Source Address
  - IP Destination Address
  - Protocol Source Port Range
  - Protocol Destination Port Range
  - Source MAC Address (SA Mode)
  - Destination MAC Address (SA Mode)

- VLAN ID (SA Mode)
- Ethertype (SA Mode)
- Max User Throughput:
  - DL: 20 Mbps
  - UL: 10 Mbps

**Indoor Unit (ETH) Compatibility:**

- WiN1010: Data Adaptor
- RP100: RuggedPower Injector supporting 10-60VDC or 88-300VDC or 85-264VAC
- RP110: Supporting embedded serial protocols

**Configuration and Management**

- Local Management: Telnet, Web Browser
- Remote Management: SNMP Agent
- Authentication: EAP-TTLS, Device, X509 digital certificate
- Software Upgrade: FTP
- Remote Configuration: FTP

**Mechanical, Electrical, and Environmental**

- Dimensions (without antenna): 224 mm × 92 mm × 61 mm
- Weight: 1.5 kg
- Power Source: 48 VDC from the indoor unit over the indoor-outdoor cable
- Power Consumption: 8 W typical
- Operating Temperature: -40°C to +75°C
- Operating Humidity: 5% to 95% non-condensing

**Standards Compliance**

- EMC:
  - FCC Part 15, Subpart B, Class B
  - ETSI EN 301489-1/4
- Safety:
  - TUV-UL 60950-1
  - EN 60950-1
- Radio:
  - FCC Part 27
  - FCC Part 90
  - ETSI EN 302 326-1/2/3
- Environmental: ETS 300 019

## Appendix B. List of Acronyms

Acronym	Description
AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
ALG	Application-Level Gateway
AMC	Adaptive Modulation and Coding
API	Application Programming Interface
ARPU	Average Revenue Per Unit
ASN	Access Service Network
ASP	Application Service Provider
ATPC	Automatic Transmit Power Control
BE	Best Effort
BPSK	Binary Phase Shift Keying
BST	Base Station
BWA	Broadband Wireless Access
CAPEX	Capital Expenditure
CBST	Compact Base Station
CINR	Carrier to Interference + Noise Ratio
CPE	Customer Premise Equipment
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNS	Domain Name System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Multiplexer
DVB	Digital Video Broadcast
EAP	Extensible Authentication Protocol
ErtPS	Extended Real-Time Polling Service
FCAPS	Functionality Configuration Accountability Performance Security
FFT	Fast Fourier Transfer
FTP	File Transfer Protocol
FUSC	Fully Used Sub-Channelization
FXS	Foreign Exchange Subscriber
GW	Gateway
HA	Home Agent
HTTP	HyperText Transport Protocol
IAD	Integrated Access Device
ICMP	Internet Control Message Protocol
IDU	Indoor Units
IEEE	Institute of Electronic and Eclectic Engineers
IGMP	Internet Group Multicast Protocol
IMS	IP Multimedia System
IOS	Internetwork Operating System
IP	Internet Protocol



## Appendix B. List of Acronyms

Acronym	Description
IPSec	IP Security
LAN	Local Area Network
LOS	Line-of-sight
MAC	Media Access Control
MAI	Multiple Access Interference
MAN	Metropolitan Area Network
MCS	Modulation and Coding Scheme
MGCP	Media Gateway Control Protocol
MIMO	Multiple-Input, Multiple-Output
MIP	Mobile IP
MOS4	Mean Opinion Score (voice quality 1-5)
MOS5	Mean Opinion Score (voice quality 1-5)
MS	Mobile Station
MSG	Multi-Service Gateways
MTU	Maximum Transmission Unit
MTU	Multiple Tenant Unit
NAI	Network Access Identifier
NAP	Network Access Provider
NAPT	Network Address Port Translation
NEBS	Network Equipment Building System
NMS	Network Management System
NLOS	Non-line-of-sight
nrtPS	Non-Real Time Polling Service
NSP	Network Service Provider
NVoD	Near Video on Demand
NWG	Network Working Group
OAM	Operations and Maintenance
ODU	Outdoor Units
OEM	Original Equipment Manufacturer
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal frequency division multiple access
OPEX	Operational Expenditure
P-CSCF	Proxy - Call Session Control Function
PDA	Personal Digital Assistant
PDF	Portable File Format
PMIP	Proxy Media IP
POP	Point of Presence
POP3	Post Office Protocol 3
POTS	Plain Old Telephony System
PPP	Point-to-Point Protocol
PPTP	Point-to-Point Tunneling Protocol
PSK	Phase Shift Keying
PSTN	Public Switched Telephone Network
PUSC	Partially used sub-channelization

## Appendix B. List of Acronyms

Acronym	Description
PVR	Personal Video Recorder
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RC	Return Channel
RF	Radio Frequency
RG	Residential Gateway
RIP	Routing Information Protocol
ROI	Return of Investment
RSSI	Received Signal Strength Indication
rtPS	Real-Time Polling Service
SF	Service Flow
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
S-OFDMA	Scalable Orthogonal frequency division multiple access
SOHO	Small Office/Home Office
SS	Subscribers
STB	Set Top Box
STC	Space-time coding
SU	Subscriber Unit
TCP	Transmission Control Protocol
TDD	Test Driven Design
TFTP	Trivial File Transfer Protocol
TMN	Telecommunication Management System
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
URL	Universal Resource Locator
USB	Universal Serial Bus
VoD	Video on Demand
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
RuggedMAX	WiNetworks WiMAX Product Family
WiNMS	WiNetworks Network Management System
WLL	Wireless Local Loop
WMAN	Wireless Metropolitan Area Networks

**Table B.1. List of Acronyms**

## Appendix C. RuggedMAX CPE Warranty

RuggedMAX™ CPEs can be ordered with one (1) year or five (5) year warranty periods.

RuggedCom warrants this product for the ordered warranty period from the date of purchase. This product contains no user-serviceable parts. Attempted service by unauthorized personnel shall render all warranties null and void. For warranty details, visit [www.RuggedCom.com](http://www.RuggedCom.com) or contact your customer service representative.

Should this product require service, contact the factory at:

*RuggedCom Inc.*

300 Applewood Crescent

Concord, Ontario

Canada L4K 5C7

Phone: +1 905 856 5288

Fax: +1 905 856 1995