



FullMax System

User Guide

February 2014, Version 4.0

Copyright © 2014 Full Spectrum Inc. All rights reserved.

TABLE OF CONTENTS

About This Guide.....	v
Intended Audience	v
Document Conventions.....	v
How This Guide is Organized.....	vi
Obtaining Documentation.....	vi
Documentation Feedback	vi
Chapter 1: Overview	1
FullMax System Architecture	2
FullMax Base Stations and Remote Stations.....	4
FullMax Base Station	4
FullMax Fixed Remote Stations	5
FullMax Mobile Station	6
FullMAX Base Station and Remote Station Hardware Architecture.....	7
Chapter 2: Installing the FullMax System	10
Base Station Installation.....	10
Single Base Station installation.....	10
Multiple Base Station Installation	11
Indoor FS4000/FS4010 Installation	11
Outdoor FS4500/FS4510 Installation	12
FullMax Base Stations and Remote Station Configuration	12
Command Line Interface (CLI) for FullMAX Base Stations	14
General	14
Downlink Configuration.....	14

IP Address Configuration	15
CLI Commands for remote Stations	16
General	16
Channel Acquisition Table Configuration	16
IP Address Configuration	17
Installing FullMax NMS.....	18
Hardware Requirements	18
Database Requirements	18
Client Requirements	18
Install Procedure.....	18
Chapter 3: Operating FullMax System	19
Getting Started with FullMax NMS	19
Web Client	19
Invoking FullMax NMS Client.....	19
Logging In.....	20
Logging Out.....	21
Client User Interface.....	21
Adding New Devices to the NMS database	22
Configuring the FullMax System	23
Working with Profiles	23
Creating and Editing the Base Station Configuration Profile	23
Applying Base Station Configurations	32
Configuring Subscriber Stations	33
Applying Subscriber Stations Configuration	34

Quality of Service	35
Service Classes	35
Service Flows	39
Classifiers	41
Payload Header Suppression (PHS)	44
Packet Filtering	47
Chapter 4: Monitoring FullMax System	48
Monitoring Device Status	48
Monitoring Device Status	48
Displaying Device Status	48
Device Status Tab	49
Monitoring Network Changes	51
Events Features	51
Major System Events	53
Event Details	54
Searching for Events	55
Performance Monitoring	57
Displaying Device Performance	57
Selecting Graph Time Range	58
Chapter 5: Fullmax Security	59
Security Associations	59
Authentication and Authorization	60
Encryption Key Establishment	64
Data Confidentiality	66

Network Management Security	66
Users and Roles	67
Secured Device CLI	68
Secured Remote Software Upgrade.....	68
ANNEX A: FullMAX Specifications	69
RF Specifications.....	69
PHY Specifications	70
MAC Specifications.....	70
Security.....	71
Remote Management and Control	71
Interface	71
Mechanical Environment	71
FCC compliance statement (United States)	73

ABOUT THIS GUIDE

The FullMax System User Guide is the complete user guide documentation for the FullMax System. This guide describes the FullMax network entities (Base Station, Fixed and Mobile Stations and Network Management System) and their use.

Intended Audience

This guide is intended to instruct service personnel about how to install, configure and operate and maintain the FullMax System.

Document Conventions

The following icons appear throughout this guide:



Note: This is a note. It provides additional information on the current topic.



Warning: This is a warning. It contains cautionary information on the current topic.

How This Guide is Organized

Chapter 1: Overview

This chapter provides an overview of the FullMax System, definition of key parameters in the system and FullMax System description.

Chapter 2: Installing the FullMax System

The chapter provides an overview of how to install FullMax base stations and fixed / mobile stations and perform essential configuration for initial operation. The chapter also details the FullMax NMS installation process.

Chapter 3: Operating the FullMax System

In this chapter the user can learn how to configure the system, provision new services and monitor the installed system.

Chapter 4: Monitoring FullMax System

The chapter provides details on how to monitor device statuses, detect failures and changes in the network and how to monitor the network performance.

Chapter 5: FullMax System Security

The chapter provides a detailed explanation on the FullMax security mechanisms.

Annex A: Base Station and Subscriber Station Specifications

Annex B: Regulatory Information

Obtaining Documentation

To obtain additional documentation, please contact info@fullspectrumnet.com.

Documentation Feedback

We welcome your comments about this guide. Please send comments to:

info@fullspectrumnet.com or call customer service at (1) 888-350-9994.

Please include in the comment the name and version number of the guide.

CHAPTER 1: OVERVIEW

FullMax is a multi-cell, Point-to-Multipoint (PtMP) broadband wireless system based on the WiMax-e (IEEE 802.16e-2005) protocol with modifications to enable its operation in a wide range of frequencies below 1 GHz. The system is used to establish a private, broadband wireless service for electrical utilities and other mission critical industries. It supports both fixed and mobile applications.

The main characteristics of the FullMax System include the following:

FullMax operates in unpaired spectrum using Time Division Duplexing (TDD). FullMax also operates in paired spectrum employing each portion of the paired spectrum as independent unpaired spectrum. FullMax Base Stations employ GPS for TDD framing synchronization.

FullMax is capable of operating in any frequency band between 40 MHz and 958 MHz¹ and in any channel size between 200 KHz and 5 MHz².

The FullMax system offers the private system operator wide area coverage by leveraging the following:

- High transmit power from both the Base Station and Subscriber Stations
- Exceptional receiver sensitivity
- Superior propagation due to the operation in narrower non-standard WiMax channel sizes and low band frequencies

The FullMax system offers excellent frequency utilization through the following capabilities:

- Adaptive Modulation and Coding in both the downlink and uplink
- Optimization of the downlink and uplink ratio for the user's main applications. For example, in the case of SCADA applications, the FullMax frame is configured as reverse

¹ Currently, FullMax has FCC certification to operate in United States NPCS band (FCC Part 24), in the 700 MHz guard band (FCC Part 27) in the AMTS band (FCC Part 80) and in the IVDS band (FCC Part 95). FCC certification for other bands will be acquired upon demand.

² FullMax has been fully tested to operate in 500 KHz wide channel, 700 KHz wide channel and 1 MHz wide channels. Other channel sizes should be verified with Full Spectrum engineering support before implementation to guarantee proper network configuration.

asymmetrical, i.e., more bandwidth is allocated to the uplink than to the downlink.

- Packet header suppression (PHS) and other compression techniques.

FullMax includes a versatile set of QoS tools that can optimize traffic performance for each application and prioritize the access to the available bandwidth according to the operator's requirements. QoS tools include various scheduling methods, service flows with various QoS parameters such as minimum and maximum traffic rates, guaranteed delay, jitter, etc.

FullMax provides secured connections with strong encryption (AES-128), strong authentication (EAP after RSA with X.509 certificates) and advanced key management protocol (PKMv2).

FullMax supports various frequency reuse methods including full channel based frequency reuse, sub-channel based frequency reuse and time segregation based frequency re-use.

FullMAX comprises of one or more Base Stations, Fixed Remote Stations and Mobile Stations. The term "Remote Stations" when used, refers to both the fixed Remote Stations and Mobile Stations.

The FullMax Remote Stations support a pre-configured channel acquisition plan, i.e., a preconfigured list of channel alternatives, characterized by their center frequency and the bandwidth. During startup, the MS4000 or FS4000 goes through the list and perform successive channel acquisition attempts until an attempt is successful.

FullMax has an advanced remote management system that enables the system operator to monitor, configure, manage, detect failures and diagnose problems. The FullMax system configuration and FullMax system provisioning support central management profiles.

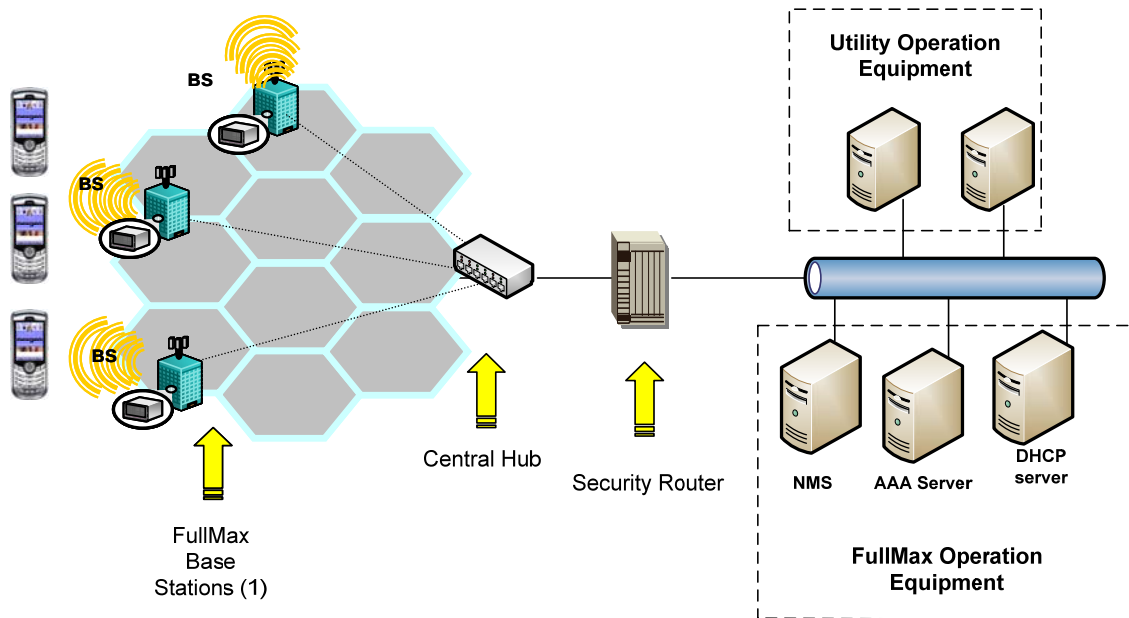
FullMax System Architecture

The FullMax system architecture is described in Figure 1 below. It consists of Base Stations, Fixed Subscriber Stations, Mobile Stations, backhaul networking equipment connecting the Base Stations to the Network Operations Center (NOC) and a Network Management System (NMS).

FullMax Base Stations are typically installed in the existing Private Land Mobile Radio (PLMR) towers serving their respective cells.

The Base Station is designed as a single sector device. Any number of sectors can be designed per tower and any number of Base Station units can be used in the same sector.

The most common configuration however is a 3 sector design with a single Base Station unit per sector. The sector configuration dictates the type of antenna that should be used. A router is used at the tower to connect all Base Station units to the Network Operating Center (NOC) via backhaul facilities. FullMax fixed and mobile Remote Stations are deployed throughout the tower's serving area.



(1) FullMax base station consists of 3 independent base station sectors and a base station hub

Figure 1: FullMax System Architecture

FullMax Base Stations and Remote Stations

FullMax Base Station

The FullMax Base Station is shown in Picture . It is housed in a 1U, 19" rack mount enclosure designed for indoor operation.



Front View



Rear View



Picture 2: Base Station Front and Rear View on top, Front Panel on Bottom

The Base Station employs a DC power supply which can take any DC voltage between 9 VDC to 36 VDC.

A FullMAX system with more than a single Base Station unit, requires GPS synchronization to ensure frame synchronization across the entire system. Two variants with respect to GPS synchronization are available:

- The BS1000: Multiport GPS receiver is used to provide an external 10 MHz clock and a 1 PPS signal to all the BS1000 units in the tower. This is typically used when multiple sectors are installed in the same tower.
- The BS1010: This has an internal single port GPS module which is connected directly to the GPS antenna.

The FullMax Base Station has the following external interfaces:

- An Ethernet 10/100 Base T interface.
- An RS232 serial interface for Command Line Interface (CLI) access.
- An RF interface which is connected via an RF cable and an external RF bandpass filter to the outdoor antenna on the tower.
- 2 GPS interfaces marked GPS1 and GPS2 as follows:
 - BS1000: GPS1 is connected to a GPS antenna. GPS2 is unused.
 - BS1010: GPS1 is connected to 1 PPS signal from GPS receiver, GPS2 is connected to external 10 MHz clock from GPS receiver.

The FullMax Base Station employs a high power amplifier (PA) with a P1dB of 44 dBm. A backoff of 8 dB is needed for proper 64QAM operation and therefore the maximum recommended downlink transmit power is 36 dBm (or 4 watts). If Modulation is restricted to QPSK, the TX power can be increased upto 10 watts (40 dBm). An optional higher power PA can be provided with upto 20 watts (43 dBm) TX power.

FullMax Fixed Remote Stations

The FullMax fixed remote Stations has two variants:

- FS4000/FS4010: An indoor unit as shown in picture 3 below.
- FS4500/FS4510: A sealed outdoor unit as shown in picture 4 below.



Picture 3



Picture 4

The fixed Remote Station employs a DC power supply which can take any DC voltage between 9 VDC to 36 VDC.

The Remote Fixed Station has an optional GPS module (unlike in the case of the Base Station, this is not mandatory). The indoor fixed Remote Station with no GPS module is referred to as the FS4000 while the same unit when equipped with the GPS module is referred to as FS4010. Similarly, the outdoor fixed Remote Station with no GPS module is referred to as the FS4500 while the same unit when equipped with the GPS module is referred to as FS4510

FullMax Remote Station has the following external interfaces:

- An Ethernet 10/100 BaseT interface.
- An RS232 serial interface for CLI/console
- An RF interface which is connected via an RF cable to the antenna on the Pole.
- A GPS interface which in the case of the FS4010/FS4510 is connected to a GPS antenna.

FullMax Mobile Station

FullMax MS4000 is identical to the high power FS4000. It is designed for installation in a Utility truck and as such it employs the DC power supply configuration.

FullMax MS4000 has the same interfaces as the FS4000 but the GPS interface is used for Automatic Vehicle Location (AVL).



Picture 5: FS4000 Outdoor Views: Front (left), Right Side (top-right) and Left Side (bottom-right)

FullMAX Base Station and Remote Station Hardware Architecture

The FullMax Base Station and Remote Station architecture is described in the figure 6 below. They consist of a Baseband Processor Board (BBP), an Analog Front End (AFE) section and a Power Supply.

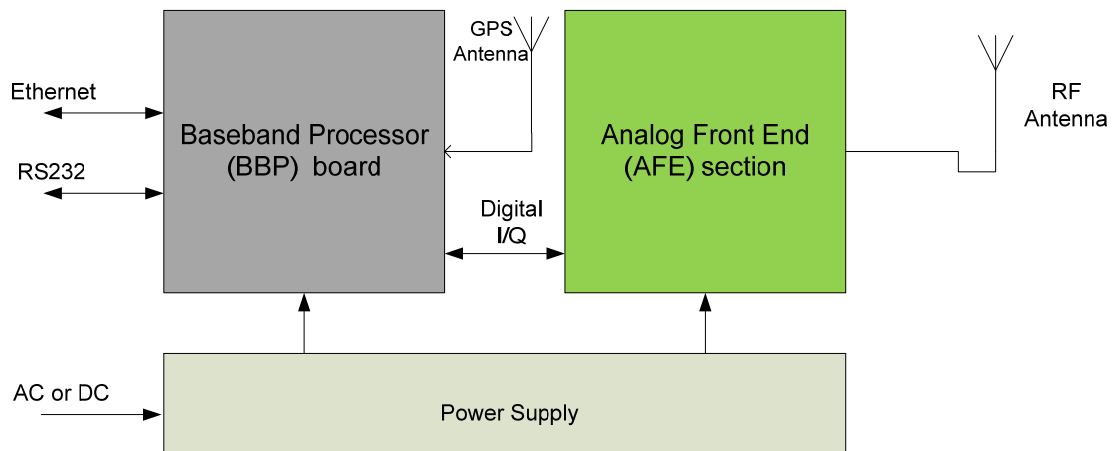


Figure 6: FullMax Base Station and Remote Station High Level Architecture

The BBP is the main control board of the FullMax radio. It is designed to perform MAC, PHY, networking, network management and other key functions required by broadband wireless Base Station and Remote Stations. The BBP has the following main characteristics:

- Processing resources:
 - A Texas Instruments (TI) Digital Signal Processor (DSP) and a Xilinx Spartan 3A FPGA to execute the PHY layer functions
 - A Freescale PQ3 processor to execute the MAC layer and complementary embedded software functions
- 10/100 BaseT and RS232 user interfaces
- A digital I/Q interface

The Analog Front End (AFE) section block diagram is described in the figure 7 below. The AFE section performs signal processing functions needed to deliver the signal to the antenna and to receive the signal from the antenna. The AFE consists of an RF Small Signal (RFSS) board and a RF Front End (RFFE) board.

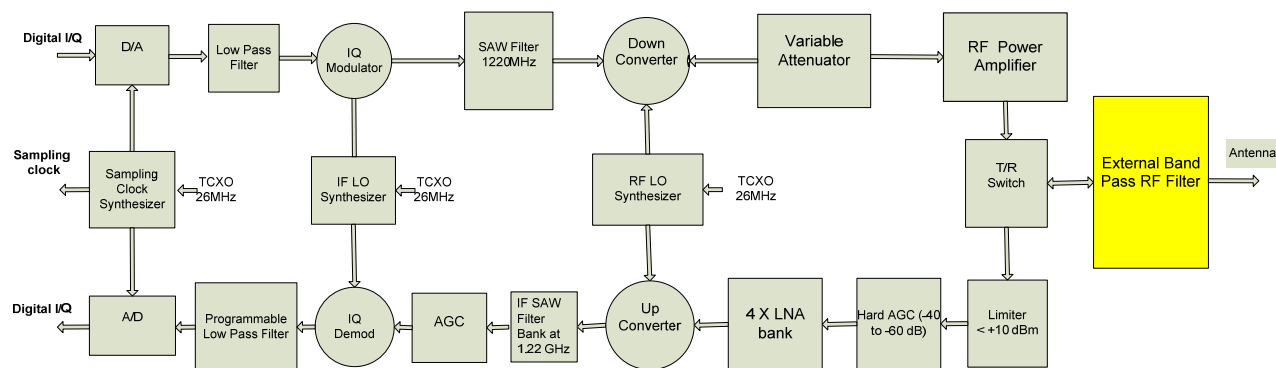


Figure 7: Analog Front End (AFE) Block Diagram

The RFSS performs analog to digital conversion (ADC), digital to analog conversion (DAC), receive and transmit signal filtering, up/down frequency conversion and Automatic Gain Control (AGC).

The RFSS employs a two stage up/down frequency conversion including an IF stage at 1.22 GHz and an RF stage. The IF stage employs a SAW filter bank for receive signal filtering independent of the RF frequency used. The individual SAW filter in the bank is selected based on the channel bandwidth used. The RF stage down converts the frequency of the signal in the transmit (TX) direction from the 1.22 GHz IF frequency to the selected RF frequency in any range between 40 MHz and 958 MHz. This is done through the RF synthesizer which can be tuned between a frequency of 1.26 GHz and a frequency of 2.178 GHz in 10 KHz steps. Similarly, the RF synthesizer is used to up convert the frequency of the received signal to the IF frequency.

In addition to the filtering at the IF stage, the RFSS has a programmable receive analog baseband filter which is programmed to the precise bandwidth of the channel used. This programmable analog baseband filtering along with the programmable baseband digital filter at the BBP is needed to enable the AFE to transmit and receive over a wide range of channel bandwidths. Furthermore, the RFSS has a sampling clock synthesizer which is programmed to generate the sampling clock needed for each channel bandwidth.

The RFSS AGC is used to map a wide range of receive power levels to an optimal processing window at the input to the ADC. The AGC is used in the Remote Station to adjust the demodulator gain depending on its distance and path-loss from the Base Station.

The RF Front End (RFFE) board performs amplification in both transmit and receive directions.

In the transmit direction, the RFFE contains a wide-range variable attenuator and an RF Power Amplifier (PA). The variable attenuator determines the power level into the PA which, in turn, determines the TX power out of the radio. Considering that the Base Station transmits to all Remote Stations in its sector, the TX power at the Base Station is typically maintained at a constant 36 dBm. The TX power at the Remote Station however is determined by a closed loop power control algorithm in the Base Station depending on the path loss to each remote Station.

In the receive direction, the RFFE has a bank of Low Noise Amplifiers (LNAs). Each LNA is optimized for a portion of the 40 to 958 MHz range.

A Transmit/Receive (T/R) switch at the RFFE is used to switch the AFE from receive mode to transmit mode and vice-versa as needed for the implementation of Time Division Duplexing (TDD). The TDD frame is divided between a downlink sub-frame and an uplink sub-frame. The length of each sub-frame is configurable. Note that while the Base Station always transmits in the downlink sub-frame, the Remote Stations only transmits in the uplink sub-frame in time slots allocated by the Base Station.

The AFE employs 8051 microcontrollers for monitoring and control of all aspects of the AFE operation. A serial interface protocol is available to support control of the master microcontroller on the RFSS board by the main PQ3 processor on the BBP board.

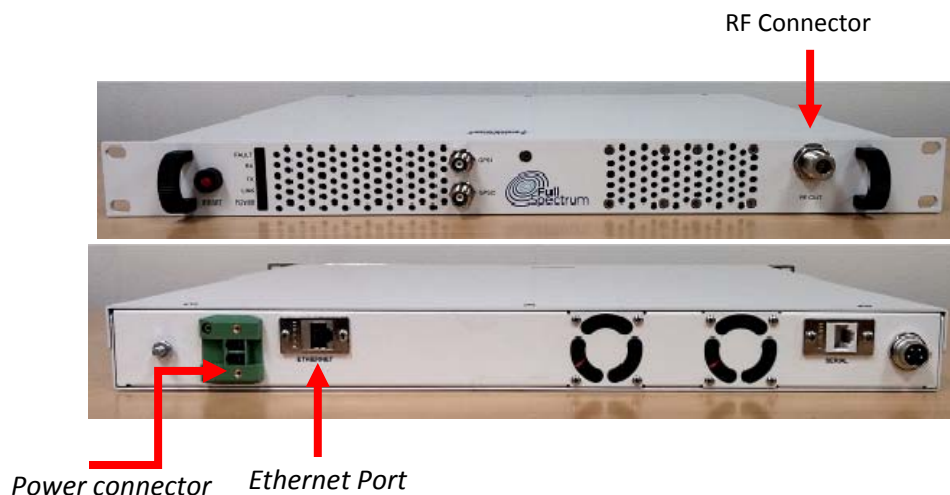
Note: The AFE employs a non-agile external RF band-pass filter which is shown in yellow block in the AFE block diagram in Figure 7 above.

CHAPTER 2: INSTALLING THE FULLMAX SYSTEM

Base Station Installation

Single Base Station installation

1. Install the Base Station on a shelf in a standard 19" rack. Make sure that air can run freely to the fans on the rear side of the enclosure and to the holes on the sides and the front of the enclosure.
2. Connect an RF cable from the RF connector on the front panel of the enclosure to the antenna on the tower.



3. Connect a Cat 5 cable to the Ethernet port on the front panel to a router at the tower.
4. Connect a power cable from the power connector on the rear side of the enclosure to a DC power source. The Base Station will start to boot.
5. Base Station LED Description:
 - PWR – On when the Base Station is powered on
 - FAULT – On when a fault condition is detected
 - RX – Indicates traffic is received from remote Subscriber Stations
 - TX – Indicates traffic is transmitted to remote Subscriber Stations
 - Link – On when one or more Remote Station is connected to the Base Station.

Multiple Base Station Installation

A Base Station functions as a single sector in the tower. A typical installation includes multiple (typically 3) sectors in a tower. In this case, each of the BS1000 units will be placed on a different shelf in the rack and the installation procedure outlined in the above paragraph will be repeated for each of the BS1000 units.

In addition to the above, multiple BS1000 operation requires the use of a GPS antenna for TDD frame synchronization. The GPS connectors of each BS1000 unit will be connected to an external GPS based time synchronization device (OctoClock). The time synchronization device provides time reference (GPS synchronized external 10 MHz clock and 1 PPS signal) to all BS1000 units in the tower and connects to a single GPS antenna.

Indoor FS4000/FS4010 Installation

1. FS4000/FS4010 installation procedure is the same as the Base Station installation described above.
2. The FS4000 does not have an on/off switch. The unit is turned on when connected to the power supply.
3. FS4000/FS4010 LED Description:
 - Power – On when FS4000 is powered on
 - BIT – On when a fault condition is detected
 - RX – Indicates traffic is being received
 - TX – Indicates traffic is being transmitted
 - Link – On when FS4000 is connected to the BS1000.
 - Fault LED: On indicates an AFE fault. The specific fault is indicated by one of the other 5 LEDs (Green Color) as follows (from left to right):
 - One of the synthesizers is unlocked
 - Over current
 - TX PWR leakage
 - TX PWR mismatch
 - Over temperature
 - When the AFE OK, the 4 left LEDs indicate RSSI as follows:
 - One LED on if the RSSI > -105 dBm
 - Two LEDs on if the RSSI > - 95 dBm

- Three LEDs on if the RSSI > -85 dBm
- Four LEDs on if the RSSI > -75 dBm

Outdoor FS4500/FS4510 Installation

1. Mount the FS4500 on a pole or wall by inserting 4 screws at the 4 corners of the mounting plate
2. Connect an RF cable from the RF connector on the enclosure left side to the outdoor antenna.



3. Use a Cat 5 cable to connect the Ethernet port on the enclosure to the end equipment



4. Connect a power cable from the power connector on the rear side of the enclosure to a 9 to 36 VDC power source.

FullMax Base Stations and Remote Station Configuration

The FullMAX Base Stations and Remote Stations are shipped with a generic configuration done through configuration files at Full Spectrum. The generic configuration contains the values of all parameters which are the same across the entire system are a portion of the system such as:

- Center RF frequency

- Channel bandwidth
- Base Station transmit power
- # of symbols for downlink subframe
- # of symbols for uplink subframe
- Gaps (RTG, TTG) duration
- Frame duration
- Base Station demod gain
- Base Station and remote Station sector configuration
- An automatic channel acquisition table with up to 10 entries. Each entry includes the center frequency, the channel bandwidth and other parameters for each available channel in the system.

The configuration of each Base Station and Remote Station is customized to the specifics of each site. The most common configuration involves the specific networking parameters:

- Type of IP address (dynamic or static)
- IP Address
- Subnet Mask
- Default Gateway

Both the FullMAX Base Station and Remote Stations employ a non-agile RF band-pass filter. This is an additional safeguard which guarantees that the FullMAX Base Station and Remote Station will not transmit outside the band.

Command Line Interface (CLI) for FullMAX Base Stations

General

CLI commands can be used to monitor the FullMAX Base Station performance and configure some of its parameter while the Base Station is up and running.

CLI commands are grouped together to create a structural hierarchy. In order to run a specific CLI command, you should first get into its group. A parameter value can be showed by using the 'SHOW' command. Some of the parameters can be changed by using the 'SET' command.

After logging in through telnet

```
[FULLMAX]$ Prompt for user is displayed.
```

Type help or ? to look at different groups.

Downlink Configuration

Go to downlink configuration group

Lock to dl-config group by typing dl-config on the prompt:

```
[FULLMAX]$  
[FULLMAX]$ dl-config
```

```
You are locked to dl-config group.  
Only dl-config operations are allowed.  
Use help or ? for help.
```

```
[FULLMAX (dl-config)]$
```

Center Frequency

```
[FULLMAX (dl-config)]$ show center-freq  
center-freq 940500 khz
```

```
[FULLMAX (dl-config)]$ set center-freq 930800
updated center-freq 930800 khz
```

Transmit Power

```
[FULLMAX (dl-config)]$ show tx_power
tx_power 9 dbm
```

```
[FULLMAX (dl-config)]$ set tx_power 16
updated tx_power 16 dbm
```

Channel Bandwidth

```
[FULLMAX (dl-config)]$ show bandwidth
bandwidth 500 khz
```

```
[FULLMAX (dl-config)]$ set bandwidth 500 khz
Updated bandwidth 500 khz
```

IP Address Configuration

IP Acquisition Method

The IP acquisition method can be either dynamic (1), meaning the BS1000 will use DHCP protocol to acquire its IP address, or static (0) meaning the BS1000 will use its locally configured CLI.

```
[FULLMAX$] show ip-status
ip-status 0
```

```
[FULLMAX$] set ip-status
Updated ip-status to static
```

Static IP Address

```
[FULLMAX$] show ip-address
ip-address 192.168.0.1
```

```
[FULLMAX$] set ip-address 192.168.0.2
Updated ip-address 192.168.0.2
```

Subnet Mask

```
[FULLMAX$] show subnet-mask
Updated subnet-mask 255.255.255.0
```

```
[FULLMAX$] set subnet-mask 255.255.255.0
Updated subnet-mask 255.255.255.0
```

Default Gateway

```
[FULLMAX$] show gateway-ip
```

```
gateway-ip 192.168.0.10
```

```
[FULLMAX$] set gateway-ip 192.168.1.1  
Updated gateway-ip 192.168.1.1
```

CLI Commands for remote Stations

General

CLI commands can be used to monitor the FullMAX Remote Station performance and configure some of its parameter while the remote Station is up and running.

Channel Acquisition Table Configuration

[Go to Subscriber Channel Configuration Group](#)

Lock to subscriber channel configuration group by typing `ss-chconfig` at the prompt:

```
FullMax#  
FullMax# ss-chconfig  
FullMax(ss-chconfig)#
```

```
You are locked to ss-chconfig group.  
Only ss-chconfig operations are allowed.  
Use help or ? for help.
```

```
[FULLMAX (ss-chconfig)]$
```

[Show Channel table](#)

To show a line in the table type: **show channel-config-table** <line-number>. For example the following command will display the first line of the table:

```
[FULLMAX (ss-chconfig)]$ show channel-config-table 1  
  
center-freq for chn-index 1 is 217775 kHz  
bandwidth for chn-index 1 is 500 kHz  
center-config-status for chn-index 1 is ACTIVE
```

[Set table entry](#)

```
[FULLMAX (ss-chconfig)]$ set center-freq 900000 1
Updated center frequency for chn-index 1 to 900000 khz

[FULLMAX (ss-chconfig)]$ set bandwidth 500 khz 1
Updated bandwidth for chn-index 1 to 500 khz
```

IP Address Configuration

IP Acquisition Method

The IP acquisition method can be either dynamic (1), meaning the FS4000 will use DHCP protocol to acquire its IP address, or static (0) meaning the FS4000 will use its locally configured CLI.

```
[FULLMAX$] show ip-status
ip-status 0

[FULLMAX$] set ip-status
Updated ip-status to static
```

Static IP Address

```
[FULLMAX$] show ip-address
ip-address 192.168.0.1

[FULLMAX$] set ip-address 192.168.0.2
Updated ip-address 192.168.0.2
```

Subnet Mask

```
[FULLMAX$] show subnet-mask
subnet-mask 255.255.255.0

[FULLMAX$] set subnet-mask 255.255.255.0
Updated subnet-mask 255.255.255.0
```

Default Gateway

```
[FULLMAX$] show gateway-ip
gateway-ip 192.168.0.10

[FULLMAX$] set gateway-ip 192.168.1.1
Updated gateway-ip 192.168.1.1
```

Installing FullMax NMS

Hardware Requirements

- Dual core based machine
- Minimum 2 GB RAM
- 100 GB free disk space + 1MB for each managed element– all on the system drive.

Database Requirements

The FullMax NMS application requires SQL database. The system supports any JDBC compliant SQL database.

Client Requirements

- Adobe Flash Plug-in
- Web browsers: Internet Explorer (IE) version 7 or 8, FireFox, Google Chrome

Install Procedure

- See NMS Installation Instructions (separate document)

CHAPTER 3: OPERATING FULLMAX SYSTEM

Getting Started with FullMax NMS

Web Client

The server can be accessed from any client with appropriate system requirements. The only client software required is a supported web browser. This can be Microsoft Internet Explorer, Mozilla FireFox or Google Chrome.

Note: The NMS is best viewed with 1024x768 resolutions.

Invoking FullMax NMS Client

To invoke the FullMax NMS, enter the URL for your FullMax NMS server in your web browser:

`http://server_ip_address`

where the SERVER_IP_ADDRESS is the IP address of the FullMax NMS Server.

FullMax NMS displays the Login page. You can proceed by logging into FullMax NMS.

Logging In

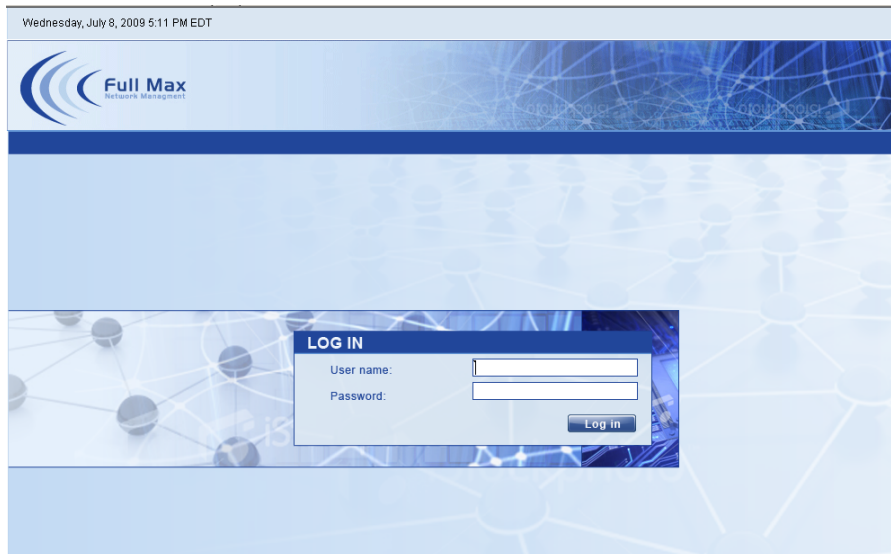


Figure 2: NMS Log in Page

If you have installed the FullMax NMS and are logging in for the first time, use the reserved *admin* user name and password. To log in:

Enter “**admin**” in the “User name” field and the default password for admin which is “qazwsx” in the password field of the Login Manager.

Note: The User Name and Password are case sensitive.

Click the Log in button or press Enter.

You are now logged into FullMax NMS. By default, the FullMax Home Page is displayed.

You can change the admin password through Admin > User Accounts > user options



WARNING! *The admin user cannot be deleted. It is highly recommended, for security purposes, that you change the admin user password.*



Note: *Login sessions time out after thirty minutes of inactivity. If the session is not used for thirty minutes, you will be prompted to login again*

Logging Out

The Logout link appears on the top right hand side of your browser. Clicking the Logout link, logs out the user from FullMax NMS Client. The Login page appears.

Client User Interface

The following are the main panes in the FullMax NMS client:

- Header Pane
- Application Pane

Header Pane

The header pane of the FullMax NMS client is located at the top of the screen and contains links to various applications. When you click on a link, that application, or its tasks/sub-tasks are displayed in the application pane.

The header includes the following:

- Time of day – the time showed is the time in the FullMax NMS server
- Search box – this is used to locate new devices
- Log in information
- Log out link
- Menu



The FullMax NMS menu includes these menu items:

- Home
- Network
- Map View
- Events
- Reports
- Admin
- Support

Application Pane

The application pane of the FullMax NMS client is located below the header pane and contains different views for the various applications.

Adding New Devices to the NMS database

Adding a New Tower to the NMS Database

In the menu go to Admin > new BS Tower

The only mandatory field is the tower name.

- Tower name
- Router IP address
- Latitude
- Longitude
- Tower height
- Installer name
- Installation date

Adding a New Base Station Sector to the NMS Database

In the menu go to Admin > new BS Sector

Mandatory fields are: sector name, tower and IP address

- Sector name
- Tower
- IP Address
- Latitude

If not manually configured, the NMS will use the latitude of one of the BS sectors associated with this tower.

- Longitude

If not manually configured, the NMS will use the longitude of one of the BS sectors associated with this tower.

- Antenna Height
- Antenna Gain

- Installer name
- Installation date

Adding a New Fixed / Mobile Station to the NMS Database

The NMS will automatically learn the Fixed and Mobile Station if not manually inserted.

In the menu go to Admin > New Station

Mandatory fields are station name and MAC address

- Station Name
- Base Station
- MAC Address
- IP Address
- Type

Configuring the FullMax System

Working with Profiles

The FullMax Network Management system uses profiles to apply the same configuration parameters to a group of base stations or a group of fixed/mobile stations. The system administrator may generate one or more configuration profiles.

Creating and Editing the Base Station Configuration Profile

To add new BS Sector configuration profile use Admin > BS Configuration Profile.

Click the Add button.

Base Station Management Configuration

General	RF	PHY	Burst Profile	MAC	Security
Profile Name: Default					
Measurement Configuration					
Throught Measurement Interval		4	sec		
Counter Report Interval		15	Min		
Trap Configuration					
RSSI Status Alarm Trap Threshold		0	dBm		
RSSI Status Clear Trap Threshold		0	dBm		
☒ Station Status ☐ Dynamic Service Failure ☒ Station RSSI Status Change ☐ Performance Counters ☐ Station Registration ☐ PKM Failure					
Save					

- **Profile Name:**
The name of the profile is used as reference when associating a profile with a base station or a subscriber station.
- **Throughput Measurement Interval:**
This parameter determines the interval that the BS1000 uses to measure the peak and average data rate statistics
- **Counter Report Interval:**
 - This parameter determines the interval of the BS1000 reset performance counters.
 - RSSI Status Alarm Trap Threshold
 - An RSSI alarm trap is generated when the base station measures an RSSI value that is lower than the set threshold. This parameter is used for default value, and can be overwritten in the base station action tab screen.
- **RSSI Status Clear Trap Threshold**
A RSSI Status Clear Trap is sent the first time it measures a RSSI value that is higher than this threshold after the base station has sent an RSSI alarm. This parameter is used for default value, and can be overwritten in the base station action tab screen.

■ Send traps:

These parameters are used to enable or disable Base Station traps. Base station traps include:

- Station Status
- Dynamic Service Failure
- Station RSSI Status Change
- Performance Counters
- Station Registration
- PKM Failure

Base Station RF Configuration

General	RF	PHY	Burst Profile	MAC	Security
Center Frequency	0 kHz				
Transmit Power	0 dBm				
Transmit EIRP	0 dBm				
Antenna Gain	0 dBi				
Max Receive EIRP	0 dBm				
Maximum BS MS Tx Power	0 dBm				
Power offset adjustment range	0 - 0				
Uplink power adjustment step	0 dB				
Downlink power adjustment step	0 dB				
Save					

- Center Frequency
- Transmit Power
- Transmit EIRP
- Antenna Gain
- Max Receive EIRP
- Power Offset Adjustment Range
- Uplink Power Adjustment Step
- Downlink Power Adjustment Step

Base Station PHY Configuration

Symbol Rate	400	Ksym
FFT Size	0	
Uplink Frame Duration	0	OFDMA symbols
Downlink Frame Duration	0	OFDMA symbols
TTG	0	uSec
RTG	0	uSec
Cyclic Prefix	1/4	

Downlink Zones		Uplink Zones	
Sector Id	0	Sector Id	0
Preamble Index	0	Preamble Index	0
Permutation Type	STC	Permutation Zone	PUSC
Permutation Zone	PUSC	Permutation Base	0
Starting Symbol	0	Starting Symbol	
Use ALL SubChannel	☒	Use subChannels	☐ ☐ ☐ ☐
CINR Threshold		CINR Threshold	

Save

Contact Technical Support | Copyright 2010 Full Spectrum All right reserved

- **Symbol Rate**
- **FFT Size:**
The Fast Fourier Transform (FFT) value.
- **Downlink Frame Duration:**
The number of OFDMA codes allocated for the downlink transmission
- **Uplink Frame Duration:**
The number of OFDMA codes allocated for the uplink transmission
- **TTG:**
The TTG is a gap between the downlink burst and the subsequent uplink burst. This gap allows time for the base station to switch from transmit to receive mode. During this gap, the base station is not transmitting modulated data but simply allowing the base station transmitter carrier to ramp down, the transmit/receive antenna switch to actuate, and the base station receiver section to activate. After the gap, the base station receiver shall look for the first symbols of the uplink burst. The gap is measured in units of microseconds.

■ RTG:

The RTG is a gap between the uplink burst and the subsequent downlink burst. This gap allows time for the base station to switch from receive to transmit mode. During this gap, the base station is not transmitting modulated data but simply allowing the base station transmitter carrier to ramp up the transmit/receive antenna switch to actuate. After the gap, the subscriber station receivers look for the first symbols of QPSK modulated data in the downlink burst. The gap is measured in units of microseconds.

■ Cyclic Prefix

The parameter indicates the ratio of cyclic prefix time to 'useful' time.

Base Station Burst Profile Configurations

The downlink and uplink channels support adaptive burst profiling on the user data portion of the frame. The system can define up to twelve downlink burst profiles and ten uplink burst profiles. The parameters of each are communicated to the subscriber station through internal MAC messages during the frame control section of the downlink frame.

General	RF	PHY	Burst Profile	MAC	Security
Uplink Burst Profile Downlink Burst Profile					
UIUC	Modulation and coding	Power Reduction	DIUC	Modulation and coding	
1	QPSK CC 1/2	0 dB	0	QPSK CC 1/2	
2	QPSK CC 1/2	0 dB	1	QPSK CC 1/2	
3	QPSK CC 1/2	0 dB	2	QPSK CC 1/2	
4	QPSK CC 1/2	0 dB	3	QPSK CC 1/2	
5	QPSK CC 1/2	0 dB	4	QPSK CC 1/2	
6	QPSK CC 1/2	0 dB	5	QPSK CC 1/2	
7	QPSK CC 1/2	0 dB	6	QPSK CC 1/2	
8	QPSK CC 1/2	0 dB	7	QPSK CC 1/2	
9	QPSK CC 1/2	0 dB	8	QPSK CC 1/2	
10	QPSK CC 1/2	0 dB	9	QPSK CC 1/2	
			10	QPSK CC 1/2	
			11	QPSK CC 1/2	
			12	QPSK CC 1/2	
Save					

Each of the burst profiles includes the following parameters:

- Modulation type:
Either QPSK, 16QAM or 64QAM
- Forward Error Correction (FEC) Type:

The FullMax system currently supports Convolutional Coding (CC) FEC. In the future, FullMax will also support Convolutional Turbo Coding (CTC) FEC.

- Coding ratios:

1/2 or 3/4 are currently supported.

In addition, the uplink burst profile includes:

- Power Reduction:

- Power reduction in 1 dB units between the power used for the burst profile and the power used for CDMA Ranging.

Base Station MAC Configuration

General	RF	PHY	Burst Profile	MAC	Security
Dcd Interval	0	msec	T7	0	msec
Dcd Transition	0	MAC Frames	T8	0	msec
Ucd Interval	0	msec	T9	300	msec
Ucd Transition	3	MAC Frames	T10	0	msec
Initial Ranging Interval	0	Frames	T13	0	msec
Ct Reserved Timeout	1	msec	T17	0	msec
DSx Request Retries	0		T22	0	msec
DSx Response Retries	0				
Start Of Ranging Codes	0				
Number of Initial Ranging Codes	0				
Number of Periodic Ranging	0				
Number of Bandwidth Request Codes	0				
Number of Handover Codes	0				

Save

- Downlink Channel Descriptor (DCD) Interval:

The time between transmissions of DCD messages measured in units of milliseconds.

- DCD Transition:

The number of frames the base station will wait after transmitting a DCD message with an incremented Configuration Change Count before issuing a downlink MAP message referring to the downlink burst profiles defined in that DCD message from the end of the frame carrying the DCD message.

The minimum value for this parameter is 20 milliseconds following the last fragment of the message.

- Uplink Channel Descriptor (UCD) Interval:

The time between transmissions of UCD messages measured in units of milliseconds.

■ UCD Transition:

The number of frames the base station will wait after transmitting a UCD message with an incremented Configuration Change Count before issuing a downlink MAP message referring to the uplink burst profiles defined in that UCD message from the end of the frame carrying the UCD message.

The minimum value for this parameter is 20 milliseconds following the last fragment of the message.

■ Initial Ranging Interval:

The time between Initial Ranging regions assigned by the base station measured in units of milliseconds.

■ Ct. Reserved Timeout

■ DSx Request Retries:

Number of Timeout Retries on Dynamic Service Add Request, Dynamic Service Change Request and Dynamic Service Delete Request.

System default value is 3 retries.

■ DSx Response Retries:

Number of Timeout Retries on Dynamic Service Add Response, Dynamic Service Change Response and Dynamic Service Delete Response.

System default value is 3 retries.

■ Start of Ranging Codes

■ Number of Initial Ranging Codes:

Number of initial ranging CDMA codes.

■ Number of Periodic Ranging Codes:

Number of periodic ranging CDMA codes

■ Number of Bandwidth Request Codes:

Number of bandwidth request CDMA codes

Note: the sum of Number of Initial Ranging Codes, Number of Periodic Ranging Codes and Number of Bandwidth Request Codes must not exceed 256

■ T7:

The time the base station will wait for Dynamic Service Add Response, Dynamic Service Change Response and Dynamic Service Delete Response before timeout. The time is measured in units of milliseconds.

- T8:
The time the base station will wait for Dynamic Service Add Acknowledge, Dynamic Service Change Acknowledge and Dynamic Service Delete Acknowledge before timeout. The time is measured in units of milliseconds.
- T9:
Registration Timeout, the time allowed between the base station sending a Ranging Response (success) to a subscriber station, and receiving a Subscriber Basic Capabilities Request (SBC-REQ) from that same subscriber station. The timeout is measured in units of milliseconds.
- T10:
The time the base station will wait for Dynamic Service Transaction to end before timeout. The time is measured in units of milliseconds.
- T13:
The time allowed for a subscriber station, following receipt of a Registration Response message to send a TFTP complete message to the base station.
The time is measured in units of minutes.
- T17:
Time allowed for a subscriber station to complete the Subscriber Authorization process and the key exchange.
The time is measured in units of minutes.
- T22:
The wait time for an ARQ Reset. The time is measured in units of minutes.

Base Station Security Configuration

General	RF	PHY	Burst Profile	MAC	Security
SA Challenge Timer	500	msec			
SA Challenge Max Resends	1 ▼				
SA TEK Timer	100	msec			
2nd EAP Timeout	300	msec			
EAP Complete Resends	1				
PKM PMK PrehandShake Lifetime	5	Sec			
PKM PMK Lifetime	60	Sec			
SA Challenge Timeout	600	msec			
Max SA TEK Challenge	3	transmissions			
SA TEK Timeout	100	msec			
Max SA TEK Request	1 ▼				
Save					

- **SA Challenge Timer:**
Time prior to SA-TEK Challenge
The parameter is measured in milliseconds. The FullMax system default is one second (=1,000 milliseconds).
- **SA Challenge Max Resends:**
Maximum number of transmissions of SA-TEK-Challenge
The FullMax system default is 3 resends.
- **SA TEK Timer:**
Time prior to re-send of SA-TEK Request.
The parameter is measured in milliseconds. The FullMax system default is 300 milliseconds.
- **2nd EAP Timeout**
Time, in seconds, the base station will wait for PKMv2_EAP_Start or PKMv2_Authenticated_EAP_Start after the success of the first EAP in double EAP mode.
The parameter is measured in milliseconds. The FullMax system default is one second (=1,000 milliseconds).
- **EAP Complete Resends**
Total number of sending PKMv2_EAP_Complete message in double EAP mode.
The FullMax system default is 3 resends.

- Private Key Management: PKM PMK Pre-handshake Lifetime
The PMK or PAK pre-handshake lifetime.
The parameter is measured in units of seconds. The FullMax system default value is 10 seconds.
- PKM PMK Lifetime
When the MSK lifetime is unspecified this parameter defines the PMK lifetime.
The parameter is measured in units of seconds. The FullMax system default value is one hour (=3600 seconds).
- SA Challenge Timeout
The timeout value for SA-TEK Challenge retransmission
The parameter is measured in milliseconds.
- Max SA TEK Challenge
The maximum number of SA-TEK-Challenge transmissions. The FullMax system default value is 3 transmissions.
- SA TEK Timeout
Max SA TEK Request

Applying Base Station Configurations

To apply a Base Station configuration profile to a specific base station:

- Go to the Base Station window
- Select the Actions tab
- Click the  on the list selection right to the Set Configuration Profile button
- Select the profile you want to associate with this base station
- Click the Set Configuration Profile button



Note: the new configuration parameters are now saved in the base station but are not yet active. The new parameters will be activated once the base station is reset.

Home Network Map View Events Reports Admin Support You are logged in as admin , [Log out](#)

Status Subscribers Configuration Diagnostics Statistics Information Actions Service Flows

Network View > Sterling > Quasar



Actions

[Reset](#) Sector will perform reset

[Synchronize Configuration](#) Synchronize management database with base station device information

[RSSI Alarm](#) dBm Threshold for generating the RSSI alarm

[RSSI Clear](#) dBm Threshold for clearing the RSSI alarm

[Telnet](#)

[Set configuration profile](#)

--Choose profile--
 --Choose profile--
 Sector-A
 520-MHz
 217-MHz
 Default



[Contact Technical Support](#) | Copyright 2010 Full Spectrum All right reserved

Configuring Subscriber Stations

Edit Station Configuration Profile:

Name:

Channel Acquisition

Center Frequency (kHz)	Channel Bandwidth	FCC part
217000	500 kHz	24.133
217500	500 kHz	24.133
218000	500 kHz	24.133

[Save](#) [Delete](#)

Applying Subscriber Stations Configuration

To apply a subscriber station configuration profile to a specific station:

- Go to the subscriber station window
- Select the Actions tab
- Click the  on the list selection right to the Set Configuration Profile button
- Select the profile you want to associate with this station
- Click the Set Configuration Profile button



Note: *the new configuration parameters are now saved in the base station but are not yet active. The new parameters will be activated once the base station is reset.*

Quality of Service

Support for Quality of Service (QoS) is a fundamental part of the FullMax system design. Strong QoS control is achieved by using a connection-oriented architecture where all downlink and uplink connections are controlled by the serving BS1000. Before any data transmission happens, the BS1000 and the FS4000 establish a unidirectional logical link, called a connection, between the two MAC-layer peers. Each connection is identified by a connection identifier (CID), which serves as a temporary address for data transmissions over the particular link. In addition to connections for transferring user data, FullMAX defines three management connections—the basic, primary, and secondary connections — that are used for functions such as ranging.

Service Classes

QoS sets of parameters are saved in a service class. Different QoS parameters are used for different applications types.

Scheduling

To support a wide variety of applications, FullMAX defines five scheduling services that are supported by the base station MAC scheduler for data transport over a connection:

Unsolicited grant services (UGS): This is designed to support fixed-size data packets at a constant bit rate (CBR). Examples of applications that may use this service are VoIP without silence suppression. The mandatory service flow parameters that define this service are: maximum sustained traffic rate, maximum latency, tolerated jitter, and request / transmission policy.

Extended real-time Polling Service (ErtPS) service: This service is designed to support real-time applications, such as SCADA or VoIP with silence suppression, that have variable data rates but require guaranteed data rate and delay. The mandatory service flow parameters that define this service are maximum sustained traffic rate, maximum latency, tolerated jitter, and request/transmission policy.

Real-time polling services (rtPS): This service is designed to support real-time service flows, such as surveillance cameras that generate variable-size data packets on a periodic basis. The mandatory service flow parameters that define this service are minimum reserved

traffic rate, maximum sustained traffic rate, maximum latency, and request/transmission policy.

Non-real-time polling service (nrtPS): This service is designed to support delay-tolerant data streams, such as an FTP, that require variable-size data grants at a minimum guaranteed rate. The mandatory service flow parameters to define this service are minimum reserved traffic rate, maximum sustained traffic rate, traffic priority, and request/transmission policy.

Best-effort (BE) service: This service is designed to support data streams, such as Web browsing, that do not require a minimum service-level guarantee. The mandatory service flow parameters to define this service are maximum sustained traffic rate, traffic priority, and request/transmission policy.

Service Classes Configuration in FullMax

To create / delete / edit service classes in the FullMax system go to Admin > Service Class.

Click the Add button to add a new service class.

Edit service management:

Name:

QoS Traffic Parameters:

QoS scheduling type: ertPS	
Traffic Priority:	2
Minimum Reserved Rate:	16 Kbps
Maximum Rate:	32 Kbps
Maximum Traffic Burst:	512 Bytes
Maximum Latency:	50 mSec
Tolerated Jitter:	20 mSec
☐ Fixed Size SDU	Bytes

ARQ

☐ Enable ARQ	
Window size:	1 Fragments
Block Lifetime:	0 msec * 0=unlimited
Sync Loss Timeout:	0 msec * 0=unlimited
Purge Timeout:	0 msec * 0=unlimited
Block size:	1 Bytes
☐ Deliver in order	

- **Name:**
The service class name is used as a reference when associating a service flow with a service class.
- **Scheduling Type:**
This parameter specifies which scheduling service type is associated with the service flow.
- **Traffic Priority:**

The value of this parameter specifies the priority of an associated service flow. This parameter is available in case of a downlink or uplink service flow which is associated with any other uplink scheduling type except UGS.

- **Minimum Reserved Traffic Rate:**

The Minimum Reserved Traffic Rate parameter specifies the minimum rate, in kilobits per second (kbps), reserved for this service flow. The base station should be able to satisfy connection bandwidth demand up to its minimum reserved traffic rate. If less bandwidth is requested for a connection than its Minimum Reserved Traffic Rate, the base station will reallocate the excess reserved bandwidth for other purposes. A Minimum Reserved Traffic Rate set to zero shall mean no minimum reserved traffic rate requirement.

- **Maximum Traffic Rate:**

The Maximum Traffic Rate parameter defines the peak information rate of the service. The rate is expressed in kilobits per second (kbps) and pertains to the service data at the input to the system. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. However, at the destination network interface in the uplink direction, the service shall be policed to conform to this parameter, on the average, over time. On the network in the downlink direction, it may be assumed that the service was already policed at the ingress to the network. If this parameter is set to zero, then there is no explicitly mandated maximum rate. The maximum traffic rate field specifies only a bound, not a guarantee that the rate is available.

- **Maximum Traffic Burst:**

The Maximum traffic burst parameter defines the maximum burst size that must be accommodated for the service. Since the physical speed of ingress/egress ports, the air interface, and the backhaul, will in general be greater than the maximum traffic rate parameter for a service, this parameter describes the maximum continuous burst the system should accommodate for the service assuming the service is not currently using any of its available resources. Maximum Traffic Burst set to zero means no Maximum Traffic Burst reservation requirement.

- **Maximum Latency:**

The value of this parameter specifies the maximum interval between the reception of a packet at the base station or the subscriber station and the forwarding of the packet to its Air Interface. A value of zero for Maximum Latency is interpreted as no commitment.

- **Tolerated Jitter:**

The value of this parameter specifies the maximum delay variation (jitter) for the connection. This parameter is available in case of a downlink or uplink service flow which are associated with Uplink Grant Scheduling Type = UGS or ertPS. A value of zero for Tolerated Jitter is interpreted as no commitment.

- **Enable ARQ:**

This parameter indicates whether the Automatic Repeat Request (ARQ) use is requested for the connection that is being setup.

- **Window Size:**

Window size indicates the maximum number of unacknowledged fragments at any time.

- **Block Size:**

The value of this parameter specifies the size of an ARQ block.

- **Block Lifetime:**

The maximum time interval an ARQ fragment will be managed by the transmitter ARQ machine, once initial transmission of the fragment has occurred. If transmission or retransmission of the fragment is not acknowledged by the receiver before the time limit is reached, the fragment is discarded. A value of 0 means infinite.

- **Sync Loss Timeout:**

This parameter indicates the maximum interval before declaring a loss of synchronization of the sender and receiver state machines. A value of 0 means infinite.

- **Purge Timeout:**

Indicates the time interval the ARQ window is advanced after a fragment is received. A value of 0 means infinite.

- **Deliver in Order:**

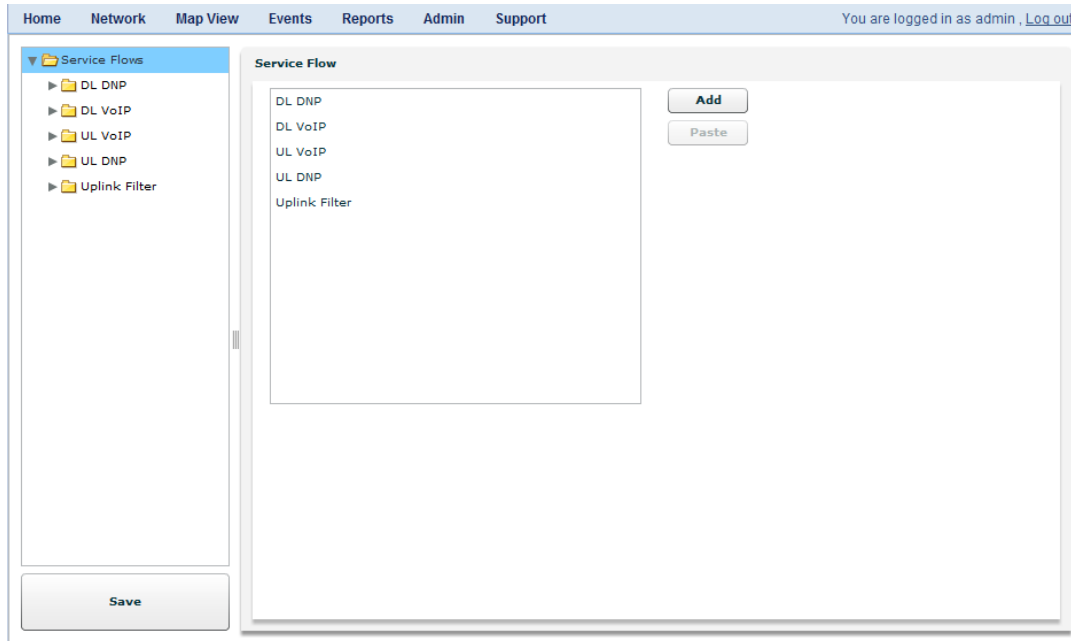
When checked, the data of this service will be delivered by the receiving MAC to its client application in the order in which data was handed off to the originating MAC.

Service Flows

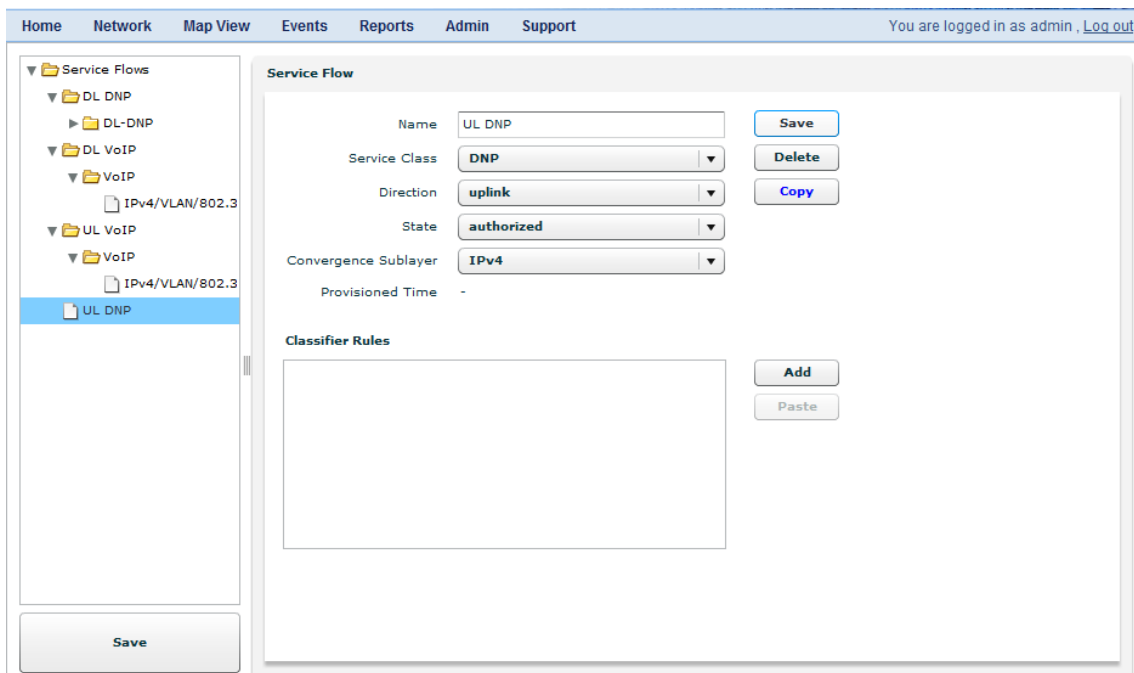
FullMAX also defines a concept of a service flow. A service flow is a unidirectional flow of packets with a particular service class. The service flow is provisioned through the Network Management System (NMS).

Service Flows Configuration in FullMax

To create / delete / edit service flows in the FullMax system go to Admin > Service Flow Profiles. The application may take some time to load during the first time it runs in a browser.



Click the Add button to add a new service flow. Click one of the service flows in the list to edit the service flow or delete it.



The service flow window displays the following parameters.

- **Name:**
The service flow name is used as a reference when associating a subscriber station with a service flow.
- **Service Class:**
The set of Quality of Service (QoS) parameters associated with the service flow.
- **Direction:**
This parameter indicates whether the direction of the service flow is uplink or downlink
- **State:**
This parameter determines the requested state of a service flow. The following states are available:
 - **Authorized State:** a service flow is provisioned but no resource is reserved yet
 - **Admitted State:** a service flow has resources reserved.
 - **Active State:** a service flow has resources committed by the BS1000
- **Convergence Sublayer:**
Ethernet is supported at this stage.

Classifiers

Classification is the process by which a packet is mapped onto a particular transport connection for transmission between peers. The mapping process associates a packet with a transport connection, which also creates an association with the service flow characteristics of that connection. This process facilitates the delivery of packets with the appropriate QoS constraints. A classification rule is a set of matching criteria applied to each packet entering the FullMax network. It consists of some protocol-specific packet matching criteria (destination IP address, for example), a classification rule priority, and a reference to a Connection ID (CID). If a packet matches the specified packet matching criteria, it is then delivered on the connection defined by the CID. The service flow characteristics of the connection provide the QoS for that packet. Several classification rules may each refer to the same service flow. The classification rule priority is used for ordering the application of classification rules to packets. Explicit ordering is necessary because the patterns used by classification rules may overlap. The priority need not be unique, but care should be taken within a classification rule priority to prevent ambiguity in classification. Downlink classification rules are applied by the base station to packets it is transmitting and uplink classification rules are applied at the subscriber station.

Classifiers Configuration in FullMax

To add a classifier to a service flow, click the Add button in the service flow window. To edit or delete a service flow's classifier, click the classifier from the classifiers' list in the service flow window.

The screenshot shows the 'Classifier Rule' configuration window in the FullMax interface. The left sidebar displays a tree view of 'Service Flows' with 'UL DNP' selected. The main window shows the configuration for the 'UL DNP/TCP' classifier. The configuration includes fields for Name, Priority, Action Rule, IP ToS, IP Protocol, Source IP, Destination IP, Source Port, Destination Port, Source MAC Address, Dest. MAC Address, Ethernet Protocol, User Priority, and VLAN ID. There are buttons for Save, Delete, Copy, Add, and Paste.

- **Name:**
Classifier name
- **Priority:**
The value specifies the priority for the Classifier, which is used for determining the order of the Classifier. A higher value indicates higher priority.
- **Action Rule:**
Specifies an action associated with this classifier. If set to accept, a packet that matches all criteria defined in the classifier rule will be delivered with the service flow that is associated with this classifier rule. If set to discard, a packet that matches all criteria defined in the classifier rule will be discarded.

IP Header Fields

- ToS: *low-high mask*

These parameters specify the matching criteria for the IP type of service or DSCP in the IP header of the packet. An IP packet with IP type of service (ToS) byte value *ip-tos* matches this parameter if:

$$\text{Low} \leq \text{ip-tos AND mask} \leq \text{high}$$

- IP Protocol:

This parameter indicates the value of the IP Protocol field required for IP packets to match this rule.

- Source IP: *address mask*:

These parameters specify the value of the IP source address required for packets to match this rule. An IP packet with source IP address value *src-addr* matches this parameter if:

$$\text{src-addr AND mask} = \text{address}$$

- Destination IP: *address mask*:

These parameters specify the value of the IP destination address required for packets to match this rule. An IP packet with destination IP address value *dst-addr* matches this parameter if:

$$\text{dst-addr AND mask} = \text{address}$$

- Source Port: *low high*:

These parameters specify the range matching criteria for the TCP/UDP source port. A TCP/IP packet or UDP/IP packet with TCP/UDP value *src_port* matches this parameter if:

$$\text{Low} \leq \text{src_port} \leq \text{high}$$

- Destination Port: *low high*:

These parameters specify the range matching criteria for the TCP/UDP destination port. A TCP/IP packet or UDP/IP packet with TCP/UDP value *dst_port* matches this parameter if:

$$\text{Low} \leq \text{dst_port} \leq \text{high}$$

Ethernet Fields

- Source MAC: *address mask*:

These parameters specify the value of the Ethernet source address required for packets to match this rule. An Ethernet packet with source Ethernet address value *src-addr* matches this parameter if:

$$\text{src-addr AND mask} = \text{address}$$

- Destination MAC: *address mask*:

These parameters specify the value of the Ethernet destination address required for packets to match this rule. An Ethernet packet with destination Ethernet address value *dst-addr* matches this parameter if:

$$\text{dst-addr AND mask} = \text{address}$$

- Ethernet Protocol: *protocol type*:

These parameters indicate the layer-three protocol ID and its format in the Ethernet packet.

A *type* value *DIX* means that the rule applies only to frames that use the Dec-Intel-Xerox (DIX) encapsulation or the RFC -1042 Sub-Network Access Protocol (SNAP) encapsulation format. A DIX or SNAP encapsulated Ethernet frame with layer-three protocol value *ether_protocol* matches this parameter if:

$$\text{type} = \text{DIX AND ether_protocol} = \text{protocol}$$

A *type* value of *DSAP* means that the rule applies only to frame using the IEEE-802.3 encapsulation format with Destination Service Access Point (DSAP) other than 0xAA (which is reserved to SNAP). A DSAP encapsulated Ethernet frame with DSAP value *dsap* matches this parameter if:

$$\text{type} = \text{DSAP AND dsap} = \text{protocol}$$

If the header contains an 802.1 P/Q Tag header (i.e. Ethernet type = 0x8100), the *type* parameter applies to the embedded EtherType field within the 802.1 P/Q header.

Payload Header Suppression (PHS)

The FullMax system enables the user to associate a payload header suppression (PHS) rule with a classifier. In PHS, a repetitive portion of the payload header is suppressed by the sending entity and restored by the receiving entity. If PHS is enabled at FullMax connection, each packet is prefixed with a PHS index. The sending entity uses classification rules to map packets into a service flow. The classification rule uniquely maps packets to its associated PHS Rule. The receiving entity uses the CID and the PHS index to restore the original.

The PHS configuration function allows the FullMax NMS user to request the fields to be suppressed on a specific classifier. The first packet that matches the classifier causes the sending entity to learn the suppressed fields' values and to update the receiving entity with the values. The PHS has a payload header suppression valid option to verify or not verify the payload header before suppressing it. If validation fails, the sending entity will change the PHS fields' values and will update the receiving entity. The user is expected to select header fields that remain static within a higher layer session (e.g., IP addresses) to be suppressed, while enabling transmission of fields that change from packet to packet (e.g., IP Total Length).

PHS Templates

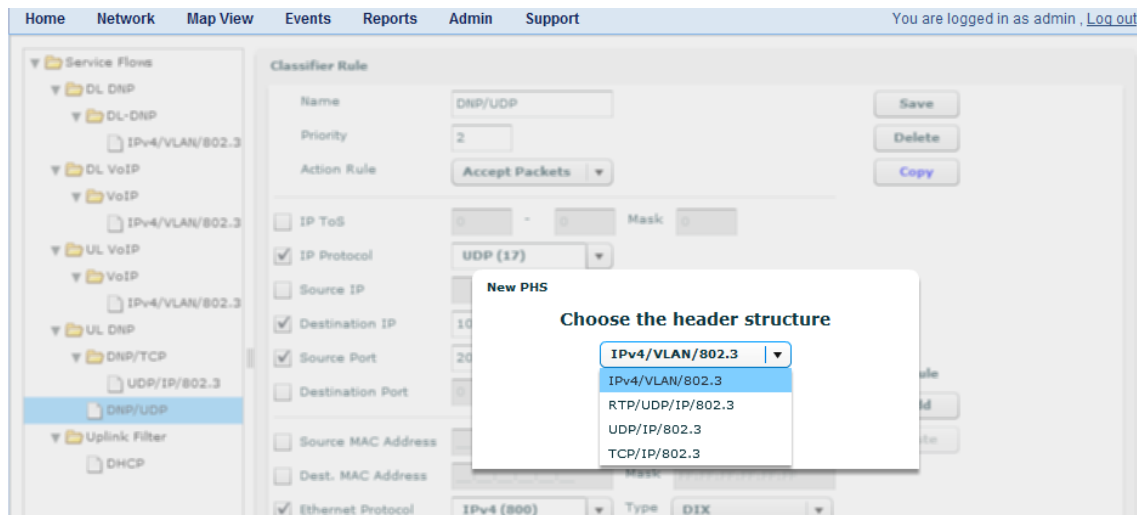
Packet header fields are highly dependent on the packet format. The FullMax system has a set of templates that catches standard frame / packet structures. These include:

- TCP / Ethernet
- TCP / VLAN / Ethernet
- DNP / TCP / Ethernet
- DNP / TCP / VLAN / Ethernet
- UDP / Ethernet
- UDP / VLAN / Ethernet
- DNP / UDP / Ethernet
- DNP / UDP / VLAN / Ethernet
- RTP / UDP / Ethernet

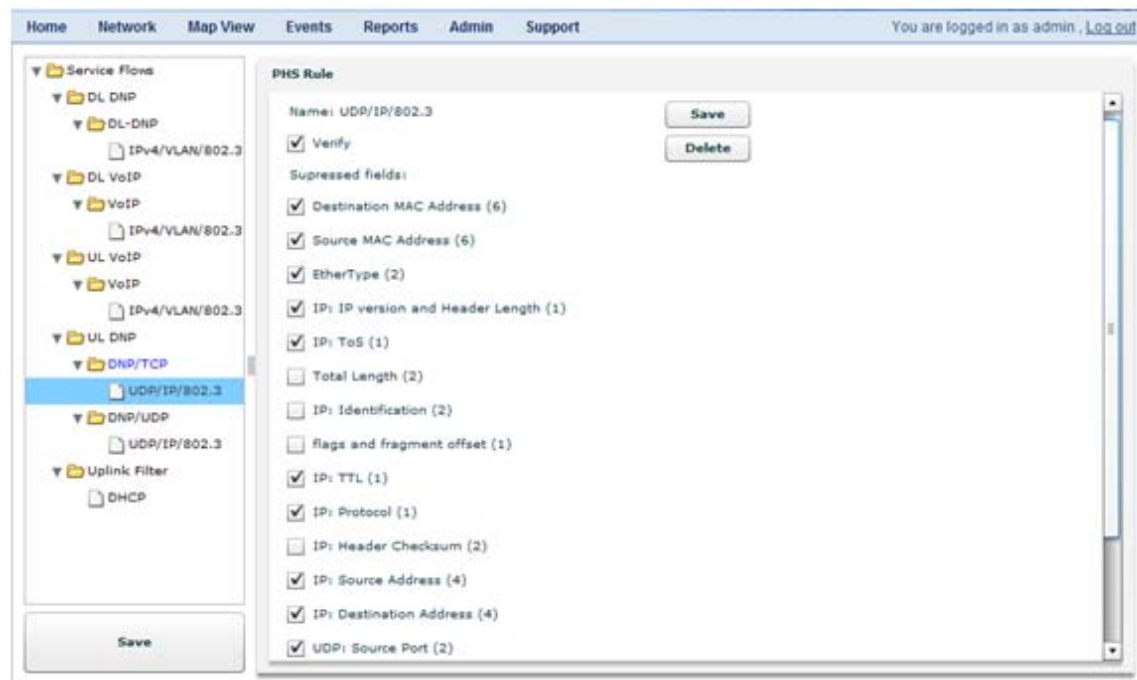
A template is an XML file that includes the list of fields and their sizes. New templates can be generated and added to the system without any change to the FullMax NMS software.

PHS Configuration in FullMax

To add a classifier to a PHS rule to a classifier, click the Add button in the classifier window. To edit or delete a classifier's PHS rule, click the PHS link in the classifiers window or use the tree navigation on the left side of the window.



When clicking the Add button the list of header structure templates is open.



The PHS window displays all header fields of the selected frames / packets along with their sizes. The user may select which of the fields should be suppressed and which should be

transferred untouched. The user must check the 'Verify' checkbox if the classifier rule is not completely specific. For example if the UDP port may vary between sessions, and the classifier states a range of UDP ports, it is required that the sending entity will verify the value and update the receiving entity when a new session starts and the port value has changed.

Packet Filtering

Packet filtering is the selective passing or blocking of data packets as they pass through the FullMax network interface. The FullMax system enables the operator to define packet filtering using service flows and classifiers. If you define a classifier with the action rule 'Discard Packets', all packets that match the classifier will be discarded.

The screenshot displays the 'Classifier Rule' configuration interface. On the left, a sidebar lists 'Service Flows' with categories like 'DL DNP', 'DL VoIP', 'UL VoIP', 'UL DNP', and 'Uplink Filter'. The 'DHCP' rule is highlighted under 'Uplink Filter'. The main configuration area includes the following fields:

- Name:** DHCP
- Priority:** 5
- Action Rule:** Discard Packet
- IP ToS:** 0 - 0, Mask: 0
- IP Protocol:** UDP (17)
- Source IP:** (empty), Mask: 255.255.255.255
- Destination IP:** (empty), Mask: 255.255.255.255
- Source Port:** 0 - 0
- Destination Port:** 67 - 68
- Source MAC Address:** (empty), Mask: FF:FF:FF:FF:FF:FF
- Dest. MAC Address:** FF:FF:FF:FF:FF:FF, Mask: FF:FF:FF:FF:FF:FF
- Ethernet Protocol:** IPv4 (800), Type: DIX
- User Priority:** 0 - 0
- VLAN ID:** 0

Buttons for 'Save' and 'Delete' are located at the top right. A 'PMS Rule' section on the right contains 'Add' and 'Paste' buttons.

CHAPTER 4: MONITORING FULLMAX SYSTEM

Monitoring Device Status

FullMax NMS monitors FullMax devices to track their status. This is done through *polling*. There are different mechanisms to monitor the status of base stations and the status of subscribers' stations. Both mechanisms are operated by the *Poller* module in the FullMax NMS.

Monitoring Device Status

Base Stations

FullMax NMS Poller is a periodic process. The poller wakes-up every configurable time, connects to a FullMax base stations and performs a simple test to see if the resource is responding correctly. If not, the process is repeated several more times. If the base station is still not responding correctly, FullMax NMS will change its status to *disconnected*.

Subscribers Stations

Subscribers' stations status monitoring is performed in two stages:

- Base Stations monitor the subscribers' station status by periodically requesting the subscribers' to perform ranging. If several periodic ranging replies remain unanswered, the base station deregisters the subscriber station and removes the subscriber from its registered subscribers table.
- FullMax NMS periodically reads the base station's registered subscribers table and compares it with the current status of the subscribers and updated it according to the subscriber's new status.

Displaying Device Status

There are two ways to view the current status of a device:

- The device color, as displayed in several different windows such as: the home page tree, device page, subscriber's page and map view.
The color green indicates that the device is connected.

The color red indicates that the device is disconnected.

- The status tab of the device page always displays the device status (e.g. connected / disconnected)

Device Status Tab

Most of the device status parameters are read once every time it boots-up, other parameters updated periodically.

Parameters that are periodically updated are the station status and for mobile station only the latitude and longitude. Other parameters, such as boot time, IP address and software version are updated after the device reboots or a subscriber station performs registration with a new base station.

The screenshot displays the FullMax System User Interface. At the top, there is a navigation bar with tabs: Home, Network, Map View, Events, Reports, Admin, and Support. Below this is a sub-navigation bar with tabs: Status, Configuration, Diagnostics, Statistics, Information, and Actions. The main content area shows the 'Status' tab for a device named 'FS-1'. The device is a 'Fixed station' with a status of 'Connected and Responding'. The interface also displays an 'Alarm Status' section with icons for Critical (0), Major (0), Minor (0), and Warnings (2). A 'View All Alarms' link is provided. The 'Versions' section lists various software components and their versions. A large blue graphic of a radio tower is visible on the left side of the status tab.

Station Summary	
Type	Fixed station
Status	Connected and Responding
Name	FS-1
Latitude	
Longitude	
IP Address	10.1.2.195
MAC Address	00:21:EE:00:00:0C
Boot Time	

Versions	
BBP HW	FSBBP_2009_ver1.0-30
AFE HW	
AFE SW	
SW Build	100-FS_BSMAC-Ver-00.01100-FS_CES-Ver-01.01100-FS_DSP-Ver-01.01100-FS_FPGA-Ver-01.01
LVPS	FSLVPS_2009_ver1.0-38

Alarm Status	
Critical	0
Major	0
Minor	0
Warnings	2

[View All Alarms](#)

The device status tab displays the following status parameters:

Station Summary

- **Type** – is the station type, e.g. base station, fixed subscriber station or mobile subscriber station.
- **Status** – current status of the station e.g. connected or disconnected.
- **Name** – the name assigned to the station.

- **Latitude / Longitude** – the station geographical location
- **IP Address** - IP address assigned to the station
- **MAC Address** – MAC address of the station
- **Boot Time** – latest time the station has started.

Version

- **BBP HW** – Baseband Processor hardware version.
- **AFE HW** – Analog Front End hardware version.
- **AFE SW**– Analog Front End hardware version
- **SW Build** – Software Build number
- **LVPS** – Low Voltage Power Supply version

Alarm Status

Displays count of outstanding alarms related to the station device.

Alarms are events of severity warning, minor, major or critical. Alarms are outstanding if the problem still exists (the alarm was not cleared) and no user had yet acknowledged it.

The alarm status on a base station sector counts alarms of the base station device itself and also alarms of all its associated fixed and mobile stations.

Monitoring Network Changes

One of the main functions of the FullMax NMS is the process of detecting changes within the network. Every change in the network is translated by the FullMax NMS to an event.

There are two main types of events: those generated internally by the FullMax NMS server and those generated by the devices and sent to FullMax NMS using SNMP traps. A FullMax device may generate a trap when one of its fans is malfunctioning, while FullMax NMS may generate an event when a new unknown subscriber station appears in a base station's registered subscribers table.

Events Features

Severity

Each event has a level of severity. An event's severity indicates the order in which the FullMax NMS clients should handle that event relative to events of other severities. Levels of severity are intended to help the FullMax clients to prioritize their work.

The following severities are available for FullMax events:

- **Critical**

This event means a base station device on the network is down.

If such an event is outstanding in the system, all FullMax NMS clients will show a flashing critical warning on the page header.



- **Major**

A subscriber's fixed station is down or in danger of going down.

- **Minor**

A part of a device (a service, and interface, a fan, etc.) has stopped functioning.

- **Warning**

An event has occurred that may require action. This severity can also be used to indicate a condition that should be noted (logged) but does not require direct action.

■ Normal

The event carries informational message. No action required.

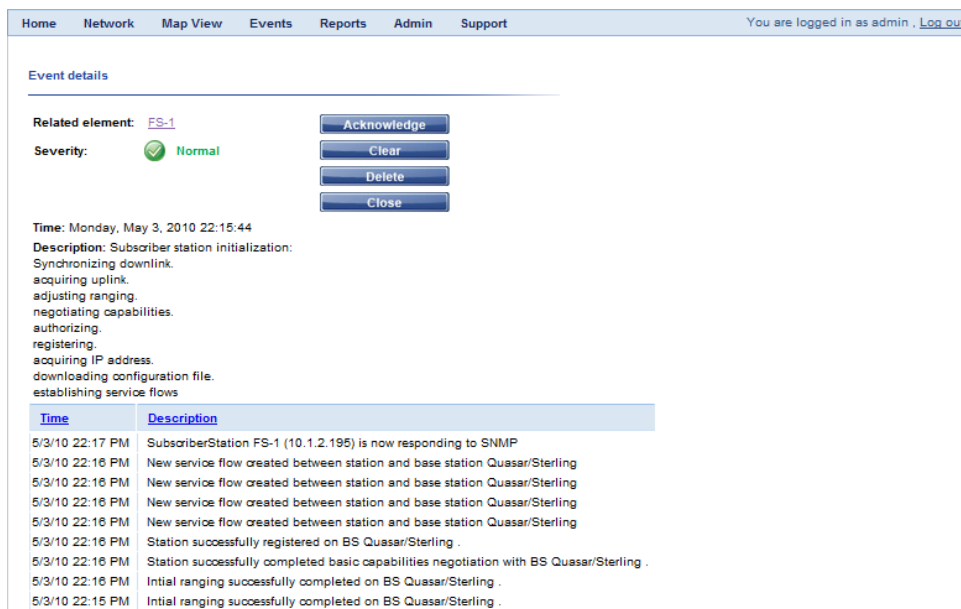
Status

An event with severity *normal* is an informational event and it is not required to monitor its status. Events of higher severities may require monitoring. To assist with monitoring events FullMax NMS maintains status tracking on these events. When a new event is generated the event's status is set to '*outstanding*'. A FullMax NMS user may acknowledge an event, stating that the problem reported by the event is handled by the acknowledging user. The status of the event will be set to '*acknowledged*'. When FullMax NMS detects that the problem reported by the event is fixed, it will change the status of the event to '*cleared*'. A FullMax NMS user may also manually clear the event.

The event status is displayed in all event list pages (e.g. Major System Events). Details on the time when the event was acknowledged and cleared, and the acknowledging user can be displayed in the Event Details page.

Events Correlation

Some of the FullMax system events indicate a step in a process. Such an event can be a subscriber's station initialization process, which includes the steps of ranging, registration, service flow creation etc. FullMax NMS identify these processes and correlate all events that are related to a single process and set them under a single root event.



Home Network Map View Events Reports Admin Support You are logged in as admin . [Log out](#)

Event details

Related element: [FS-1](#)

Severity:  Normal

Time: Monday, May 3, 2010 22:15:44

Description: Subscriber station initialization:
 Synchronizing downlink.
 acquiring uplink.
 adjusting ranging.
 negotiating capabilities.
 authorizing.
 registering.
 acquiring IP address.
 downloading configuration file.
 establishing service flows

Time	Description
5/3/10 22:17 PM	SubscriberStation FS-1 (10.1.2.195) is now responding to SNMP
5/3/10 22:16 PM	New service flow created between station and base station Quasar/Sterling
5/3/10 22:16 PM	New service flow created between station and base station Quasar/Sterling
5/3/10 22:16 PM	New service flow created between station and base station Quasar/Sterling
5/3/10 22:16 PM	New service flow created between station and base station Quasar/Sterling
5/3/10 22:16 PM	Station successfully registered on BS Quasar/Sterling .
5/3/10 22:16 PM	Station successfully completed basic capabilities negotiation with BS Quasar/Sterling .
5/3/10 22:16 PM	Initial ranging successfully completed on BS Quasar/Sterling .
5/3/10 22:15 PM	Initial ranging successfully completed on BS Quasar/Sterling .

Events lists will only display the root events. The details of the different events in the process are displayed in the Event Details page as shown above.

Major System Events

To display the system major events go to Admin > Major Events. The NMS will display the following list:

Select	Time	Related element	Type	Severity	Description	Status
☐	3/14/10 3:44 AM	Hopkins	Sector	Normal	Subscriber station initializing	Outstanding
☐	3/14/10 3:40 AM	McGuire	Sector	Normal	Base station initializing	Outstanding
☐	3/13/10 15:15 PM	McGuire	Sector	Critical	Base station down	Cleared
☐	3/13/10 15:02 PM	Hopkins	Sector	Major	Subscriber station down	Cleared
☐	3/12/10 10:17 AM	Hopkins	Sector	Normal	Subscriber station initializing	Cleared
☐	3/12/10 10:16 AM	McGuire	Sector	Normal	Base station initializing	Cleared
☐	3/12/10 10:12 AM	McGuire	Sector	Critical	Base station down	Cleared
☐	3/11/10 4:48 AM	Hopkins	Sector	Major	Subscriber station down	Cleared
☐	3/10/10 13:04 PM	Hopkins	Sector	Normal	Subscriber station initializing	Cleared
☐	3/10/10 13:03 PM	McGuire	Sector	Normal	Base station initializing	Cleared
☐	3/10/10 12:31 PM	McGuire	Sector	Critical	Base station down	Cleared
☐	3/10/10 12:29 PM	Hopkins	Sector	Major	Subscriber station down	Cleared
☐	3/10/10 12:22 PM	Hopkins	Sector	Major	Subscriber station down	Cleared

Page: 1 [Next](#)

[Acknowledge](#) [Clear](#) [Delete](#) [Select All](#)

The list includes the following columns:

- **Select** allows the user to select several events and perform an action on the selected events.
- **Time** is the first occurrence of the event
- **Related element** is the network element / device on which the change was detected
- **Type** is the network element type (tower, sector, mobile subscriber station or fixed subscriber station)
- **Severity** indicates the level of attention one should pay to the change that occurred in the system. See section **Error! Reference source not found.** for details.
- **Description** is a short text explaining the nature of the change detected in the network.

- **Status** of the event.

Events Lists Navigation

When the list of events does not fit into a single page, FullMax NMS will show at the bottom of the page:

- **Page number** – the number of the list page currently displayed
- **Previous page** – a link to previous events
- **Next page** – a link to more event

Events Actions

The following actions can be performed on a single event or a list of selected events:

- **Acknowledge** – changes the event's status to '*acknowledged*' and stores the acknowledging user and action time in the FullMax NMS database.
- **Clear** – changes the event's status to '*cleared*' and stores the clearing user and action time in the FullMax NMS database.
- **Delete** – delete the event from FullMax NMS database.
- **Select All** – selects all events displayed in an events list page.

Event Details

Events lists display a short description of each event. To show a more detailed description, enhanced status (including acknowledging user and time, clearing user and time) or the list of events composing a correlated event, click the description link in the events list. This action will open the Event Details page.

The following actions can be performed:

- **Acknowledge** – changes the event's status to '*acknowledged*' and stores the acknowledging user and action time in the FullMax NMS database. If the event is already acknowledged or cleared, the action is not available.
- **Clear** – changes the event's status to '*cleared*' and stores the clearing user and action time in the FullMax NMS database. If the event is already cleared, the action is not available.

- **Delete** – delete the event from FullMax NMS database.
- **Close** – close the event details page and go back to events list.

Home Network Map View Events Reports Admin Support You are logged in as admin , [Log out](#)

Event details

Related element: [Sterling](#) Acknowledged on: Tuesday, May 4, 2010 0:05:49 [Delete](#)

Severity:  **Critical** Acknowledged by: admin [Close](#)

Cleared by: System

Cleared on: Monday, May 3, 2010 22:17:06

Time: Monday, May 3, 2010 22:08:39

Description: Base station down

Time	Description
5/3/10 22:08 PM	Base Station Sterling (10.1.2.165) is not responding to SNMP (NMS status = Disconnected)

Searching for Events

FullMax NMS allows the user to filter events according to specific parameters. To filter events click Events > search from the NMS menu.

Event Search

Event description:

IP address:

Occured on: from:  to: 

Station name:

Severity: ☒ Critical ☒ Major ☒ Minor ☒ Warning ☒ Normal

Station type: ☒ Tower ☒ Sector ☒ Fixed Station ☒ Mobile Station

Sort by parameters:

Sort order:

Event status: ☒ Outstanding ☐ Acknowlaged ☐ Cleared

☐ Show archived events

[Search](#)

Filter Parameters

The following parameters can be used for filtering events:

- **Event Description** – filter out events that this text is not part of their description.
- **Occurred on** – filter out events that occurred before the **from** field and after the **to** field
- **Severity** – filter events with requested severities
- **Event Status** – filter events with requested status
- **Show archived events** – FullMax NMS caches the latest events for quick access and optimization purposes. Other events are archived. By default events will be searched on recent events cache. Checking the 'show archived events' checkbox will extend the search to the archived events. Note that this may induce a slower search operation.
- **IP Address** – filter events that are related to a device with IP address that contains the text in this field.
- **Station Name** – filter events that are related to a device with name that contains the text in this field.
- **Station Type** – filter events that are related to a device of this type.

Sorting Parameters

The user can control the order by which the filtered events are displayed. Sorting options include:

- **Sort by Parameter** – events list can be sorted by: occurrence time (default), severity, description or status.
- **Sort Order** – you may sort the results in either ascending or descending order.

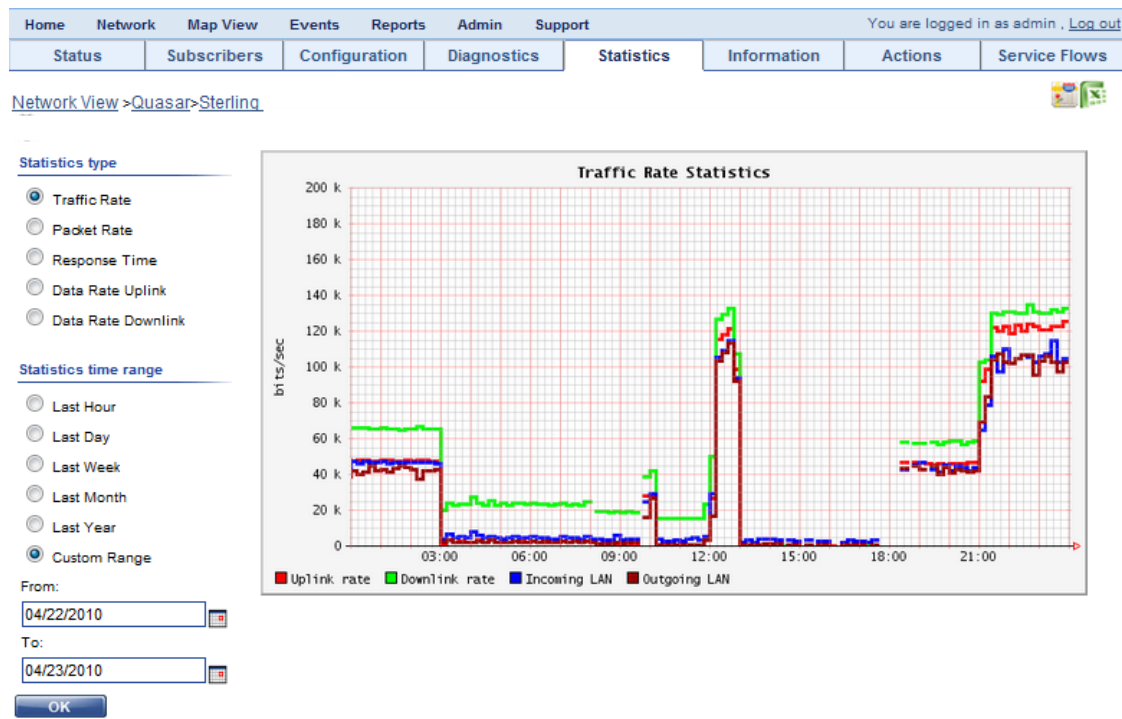
Performance Monitoring

FullMax NMS is equipped with the ability to constantly monitor a wide range of performance parameters such as traffic throughput, signal quality and more. The monitored parameters are collected and kept a designated database for a period of up to one year. These details provide the network operator an in-depth analysis and visibility into the performance of the FullMax devices.

Displaying Device Performance

Performance parameters are displayed in a graphical presentation. Parameters are grouped according to different performance groups. The user can select the performance group and the time range over which the performance will be graphed.

To display performance statistics of a FullMax device, go to the device page and select the Statistics tab.



Base Station Performance Parameters

- **Traffic Rate** group includes received uplink traffic rate, transmitted downlink traffic rate, received LAN traffic rate and transmitted LAN traffic rate. These parameters are measured in units of bits/sec.
- **Packet Rate** group includes received uplink packet rate, transmitted downlink packet

rate, received LAN packet rate and transmitted LAN packet rate. These parameters are measured in units of packets/sec.

- **Response Time** parameter measures the time passed since FullMax NMS sent a PING message to the FullMax device until a PING response was received at the FullMax NMS. Response time is measured in units of milliseconds.
- **Data Rate Uplink** and **Data Rate Downlink** display the amount of clear user data versus the amount of all FullMax data traversing on the uplink and downlink channels. All FullMax data includes user data, WiMax headers and overhead, FullMax management messages and overhead. These parameters are measured in units of bits/sec.



Note! When changing performance parameter on base station or subscriber station statistics tab, it is necessary to click the OK button to activate the query.

Subscriber Station Performance Parameters

- **Traffic Rate** group includes received downlink traffic rate, transmitted uplink traffic rate, received LAN traffic rate and transmitted LAN traffic rate. These parameters are measured in units of bits/sec.
- **Packet Rate** group includes received downlink packet rate, transmitted uplink packet rate, received LAN packet rate and transmitted LAN packet rate. These parameters are measured in units of packets/sec.
- **Response Time** parameter measures the time passed since FullMax NMS sent a PING message to the FullMax device until a PING response was received at the FullMax NMS. Response time is measured in units of milliseconds.
- **Signal Quality** group display the downlink and uplink RSSI and CINR of the subscriber station.

Selecting Graph Time Range

You may select a time range for the displayed performance parameters. You may request to see data collected on: the last hour, last day, last week, last month, last year or add your own time range, starting from a specific date to a specific date.



Note! When asking for specific dates it is necessary to select the Custom Range option as well as selecting the start and end dates for the time range.

CHAPTER 5: FULLMAX SECURITY

This section reviews the security mechanisms included in the FullMax system. The FullMax system provides two basic security services: authentication and confidentiality. Authentication involves the process of verifying the identity claimed by a FullMax device. Confidentiality involves preventing the disclosure of information by ensuring that only authorized devices can view the contents of FullMax data messages.

The FullMax system provides secure communications by performing three steps: authentication, key establishment, and data encryption. The authentication procedure provides common keying material for the Base Stations and Remote Stations and facilitates the secure exchange of data encryption keys that ensure the confidentiality of FullMax data communications.

Security Associations

A security association (SA) is a shared set of security parameters that a Base Station and its Remotes use to facilitate secure communications. Similar in concept to Internet Protocol Security (IPsec), an SA defines the security parameters of a connection, i.e., encryption keys and algorithms. SA's fall into one of two categories: authorization and data. A distinct SA is established for each service offered by the Base Station.

Authorization SA's facilitate authentication and key establishment to configure data SA's. Authorization SA's contain the following attributes:

- **X.509 certificates.** X.509 digital certificates allow FullMAX communication components to validate one another. The FullMax manufacturer certificate is used for informational purposes and the Base Station and Remote Station certificates contain the respective devices' public keys. The certificates are signed by Full Spectrum or may be signed by a third-party certification authority.
- **Authorization key (AK).** AK's are exchanged between the Base Station and its Remote Stations to authenticate one another prior to the traffic encryption key (TEK) exchange. The authorization SA includes an identifier and a key lifetime value for each AK.
- **Key encryption key (KEK).** Derived from the AK, the KEK is used to encrypt TEKs during the TEK exchange, as discussed later in this chapter.
- **Message authentication keys.** Derived from the AK, the message authentication keys

validate the authenticity of key distribution messages during key establishment. These keys are also used to sign management messages to validate message authenticity.

- **Authorized data SA list.** The authorized data SA list provided to the Remote Stations by the Base Station an indication of which data encryption SAs the Remote Stations are authorized to access.

Data SA's establish the parameters used to protect data messages between Base Stations and Remote Stations. A data SA contains the following security attributes:

- **SA identifier (SAID).** This unique value identifies the SA to distinguish it from other SA's.
- **Encryption cipher to be employed.** The connection will use this encryption cipher definition to provide wireless link confidentiality.
- **Traffic encryption key (TEK).** TEK's are randomly generated by the Base Station and are used to encrypt FullMAX data messages. Two TEKs are issued to prevent communications disruption during TEK rekeying; the first TEK is used for active communications, while the second TEK remains dormant.
- **Data encryption SA type indicator.** This indicator identifies the type of data SA. There are three types:

Primary SA. This SA is established as a unique connection for each Remote Station upon initialization with the Base Station. There is only one primary SA per Remote Station.

Static SA. This SA secures the data messages and is generated for each service defined by the Base Station.

Dynamic SA. This SA is created and eliminated in response to the initiation and termination of specific service flows.

Authentication and Authorization

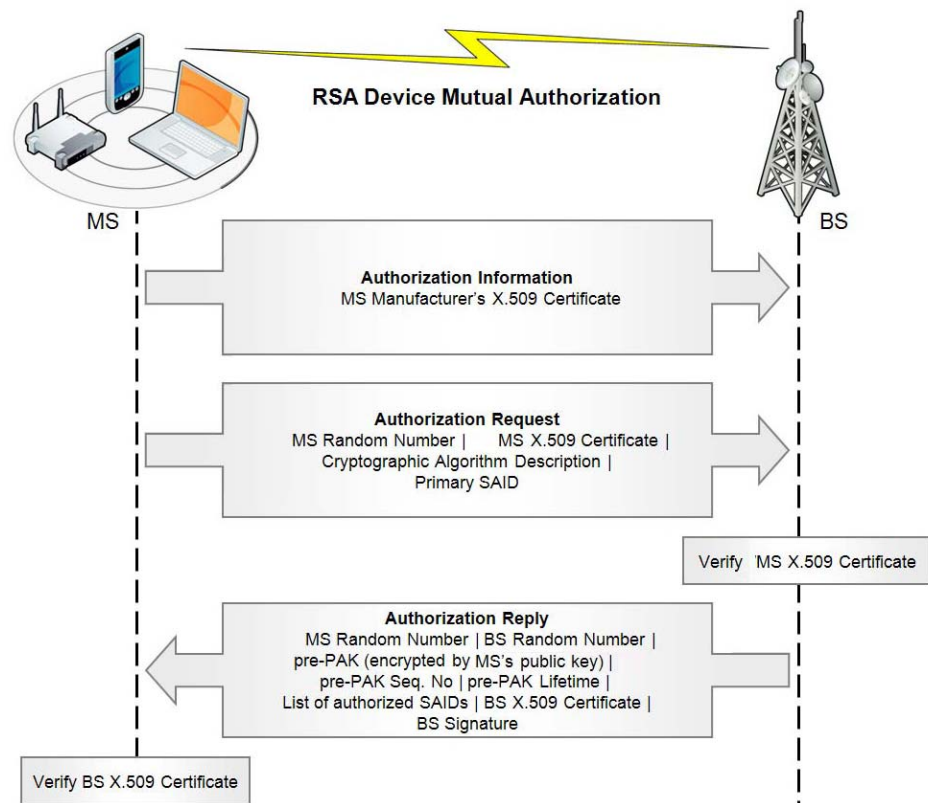
FullMax security generally refers to authorization as the process of authenticating FullMAX nodes and granting them access to the network. The authorization processes implicitly include authentication. The FullMAX system implements the Privacy Key Management Version (PKMV2) protocol as the set of rules responsible for authentication and authorization to facilitate secure key distribution in FullMAX. PKM uses authorization SA's to authenticate system entities so that data encryption SA's can be established. PKM's authentication enforcement function provides the Remote Stations and Base Stations with

identical AK's; each AK is then used to derive the message authentication keys and KEKs that facilitate the secure exchange of the TEK's. FullMax devices derive the AK using PKMv2.

PKMv2 requires mutual authentication between the Base Station and the Remote Station. PKMv2 starts with what is known as RSA device mutual authentication. The figure below illustrates its challenge-response verification scheme. It facilitates the exchange of a pre-Primary AK (pre-PAK) to ultimately derive a common AK. The exchange begins with the Remote Station sending an authorization information message containing the manufacturer X.509 certificate to the Base Station. The message is strictly for informational purposes.

The authorization information message is followed by an authorization request message sent from the Remote Station to the Base Station. It contains the following information:

- A 64-bit random number generated by the Remote Station
- The Remote Station FullMax-issued unique X.509 certificate
- A description of the Remote Station supported cryptographic algorithms
- The primary SAID

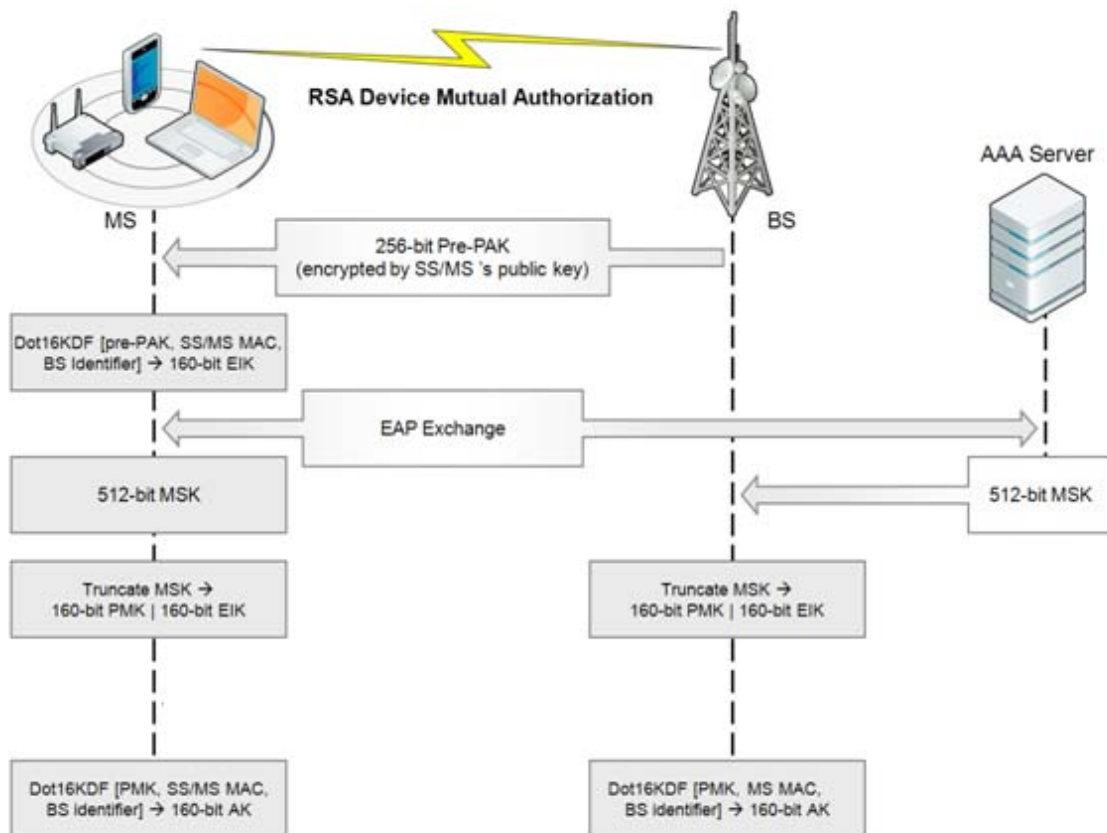


Upon receipt of the authorization request message, the Base Station verifies the Remote Station X.509 certificate. If the certificate is valid, the Base Station sends an authorization reply message to the Remote Station containing the following:

- The 64-bit Remote Station generated random number sent in the authorization request message and another 64-bit random number generated by the Base Station.
- The 256-bit pre-PAK encrypted using the Remote Station's public key
- The Pre-PAK sequence number used to differentiate between successive generations of pre-PAKs
- The Pre-PAK lifetime
- A list of SAIDs that the Remote Station is authorized to access and their associated properties
- The Base Station's FullMax-issued X.509 certificate
- The Base Station's signature provided by the Base Station's private key.

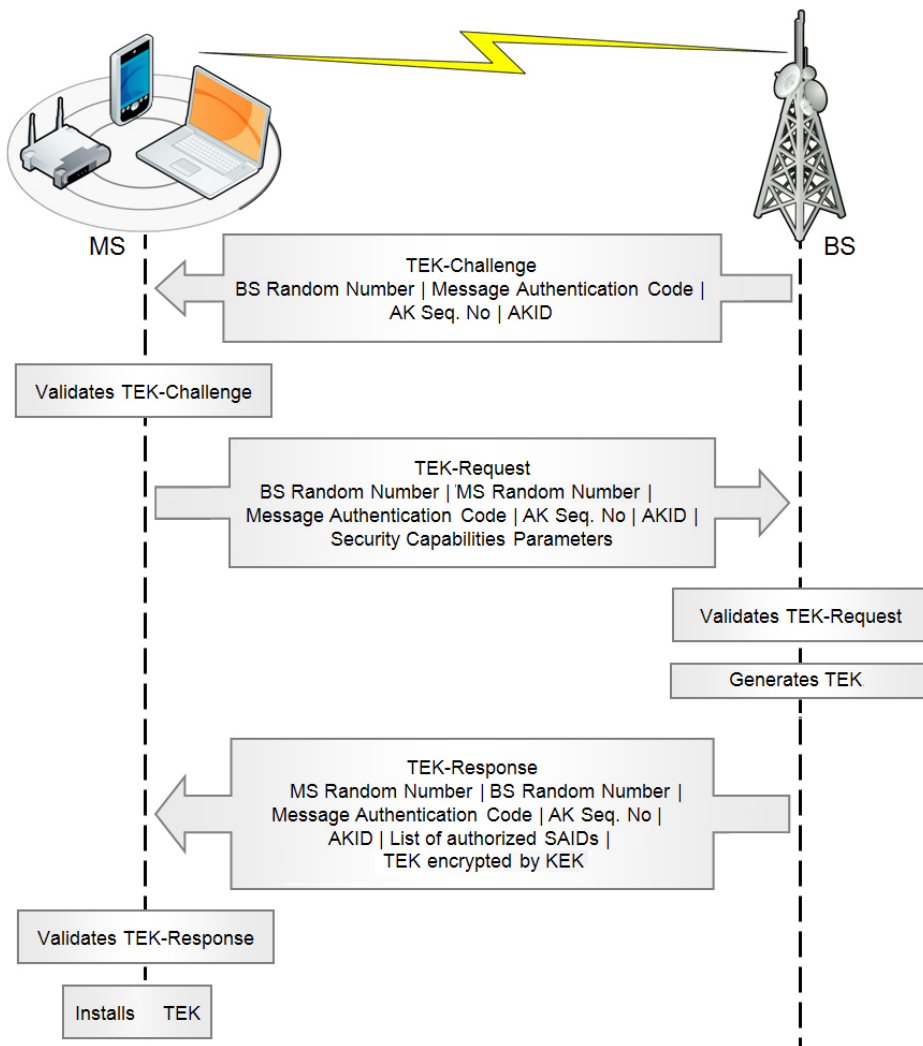
The Remote Station verifies the Base Station's X.509 certificate. If the certificate is valid, the Base Station and Remote Station proceed to the next authentication procedure to derive the AK.

After RSA device mutual authentication occurs, there is a process of *EAP after the RSA device mutual authorization* procedure. The process is depicted in the figure below. The pre-PAK is delivered to the Remote Station and then used to derive the EAP integrity key (EIK) to secure the first EAP exchange. The first EAP exchange results in the production of a 512-bit master session key (MSK) that is disclosed to the authentication, authorization, and accounting (AAA) server, the Base Station and the Remote Station. The Base Station and the Remote Station truncate the MSK to 320 bits—160 bits for the pair wise master key (PMK) and 160 bits to create another EIK. The PMK, the Remote Station MAC address, and the Base Station identifier are then used to derive the AK. Device mutual authentication only takes place during initial network entry. For network reentry or re-authentication, only EAP authentication is required.



Encryption Key Establishment

Once authentication is complete, the Base Station and the Remote Station share an activated AK. PKM then uses the 160-bit AK to derive the 128-bit KEK and the 160-bit message authentication keys, which are used to facilitate a secure exchange of TEKs. The secure TEK exchange uses a three-way handshake between the Base Station and the Remote Station, as illustrated in the figure below.



The first step in this procedure is the TEK-Challenge sent from the Base Station to the Remote Station. The TEK-Challenge is sent during initial network entry or during reauthorization.

The TEK-Challenge includes the following attributes:

- **Base Station random number.** This number is attached to the TEK-Challenge to prevent replay attacks by validating message freshness.
- **Message authentication code.** These validate data authenticity of the key distribution messages sent from the Base Station to the Remote Station.
- **AK sequence number and AK identifier (AKID).** These attributes identify which AK is used for the TEK exchange.

Upon receipt of the TEK-Challenge, the Remote Station validates the authenticity of the TEK-Challenge using the message authentication keys. After the TEK-Challenge has been validated, the Remote Station sends the TEK-Request to the Base Station , which contains the following attributes:

- **Base Station and the Remote Stations random numbers.** In addition to sending back the Base Station random number from the TEK-Challenge, the Remote Station attaches its own random value.
- **Message authentication code.** These validate data authenticity of the key distribution messages sent from the Remote Station to the Base Station.
- **AK sequence number and AKID.** These identify which AK is used for the TEK exchange.
- **Security capabilities parameters.** These describe the security capabilities of the Remote Station, including supported cryptographic suites. During initial network entry, the TEK-Request will also include a request for SA descriptors to identify the primary, static, and dynamic SAs that the Remote Station is authorized to access. FullMax Base Station and the Remote Station support the EAS-128 cryptographic suite.

Upon receipt of the TEK-Request, the Base Station verifies that the Base Station random number matches the number sent in the TEK-Challenge and validates the message authentication keys. The Base Station next confirms that the AKID refers to an available AK and that the security capabilities parameters provided by the Remote Stations are supported. Once the TEK-Request is validated, the Base Station will generate two TEKs. The Base Station then sends the TEK-Response to the Remote Stations, which contains the following attributes:

- **Base Station and the Remote Stations random number.** The Base Station attaches its random number generated in the TEK-Challenge and the Remote Stations random number generated in the TEK-Request.

- **Message authentication code.** These validate data authenticity for the key distribution messages sent from the Base Station to the Remote Stations.
- **AK sequence number and AKID.** These attributes identify which AK is used for the TEK exchange.
- **List of authorized SAIDs.** This is the list of primary, static, and dynamic SAs that the Remote Station is authorized to access.
- **TEKs.** Using the KEK derived from the AK, the Base Station encrypts the two TEKs. These keys include all of the required keying material needed to facilitate secure communications between the Base Station and the Remote Stations.

Upon receipt of the TEK-Response, the Remote Station ensures the Base Station random number matches the value given in the TEK-Challenge and that the Remote Stations random number matches the value delivered in the TEK-Request. The Remote Stations then validates the message authentication keys. Once validation is complete, the Remote Station installs the appropriate TEKs and secure communications can begin.

Data Confidentiality

The completion of the TEK exchange provides the Base Station and the Remote Station with the TEKs required to encrypt FullMAX data communications. The type of encryption employed by the TEK is 128 bits AES.

Network Management Security

The NMS server is a user role-based web application centric. It uses role-based authorization to manage access. Access permissions are granted to an abstract entity called a security role, and access is allowed only to users or groups of users who have that role.

NMS client-server traffic is over HTTPS (HTTP over SSL). HTTPS (HTTP over SSL) allows web browsers and the web server to communicate over a secured connection. It also provides authentication: during the initial attempt to communicate with the web server, that server will present the web browser with a set of credentials, in the form of a Certificate, as proof the site is who and what it claims to be. The Certificate can be purchased from a well-known Certificate Authority (CA) such as VeriSign, or can be manually generated by the FullMax customer.

Users and Roles

Access to the NMS requires user name and password based authentication. The NMS provides an interface for defining users and roles. The following roles are supported:

- **Administrator** can change the NMS configuration.
- **Advanced user** can perform actions on managed elements, but cannot change the NMS configuration.
- **Viewer** can view all information, but cannot perform any action

Only a user with an Administrator role can add, delete or edit users' properties. To add, delete or edit users' properties use the menu to go to Admin > Users Accounts. A list of all existing users is displayed.

Home Network Map View Events Reports Admin Support

You are logged in as admin , [Log out](#)

User accounts:

Full name	User name	E-mail	Edit
admin	admin	admin@admin.com	user options
John	john	john@fullspectrumnet.com	user options
Alice	alice	alice@fullspectrumnet.com	user options
Bob	bob	bob@fullspectrumnet.com	user options
Chris	chris	chris@fullspectrumnet.com	user options
Daniel	daniel	daniel@fullspectrumnet.com	user options

Add

To add a new user, click the Add button on the bottom of the list.

To delete a user or to change the user password or other property, click the link on the right column. The NMS will display the following screen:

The screenshot shows a web interface for editing user account data. At the top, there is a navigation bar with links: Home, Network, Map View, Events, Reports, Admin, and Support. On the right side of the navigation bar, it says "You are logged in as admin" with a "Log out" link. Below the navigation bar, the main content area is titled "Edit user account data:". The form contains the following fields and options:

- Full name:** A text input field containing "John".
- User name:** A text input field containing "john".
- Password:** A text input field with masked characters "*****".
- Retype password:** An empty text input field.
- Role:** A group of three radio buttons: "Admin" (unselected), "Advanced" (selected), and "Viewer" (unselected).
- E-mail:** A text input field containing "johnd@fullspectrumnet.com".

At the bottom of the form, there are two buttons: "Save" and "Delete".

Click the delete button to remove the user.

Edit the relevant fields and click the save button to keep the changes.

Secured Device CLI

The CLI on FullMax devices are password protected. The devices provide two levels of CLIs for two different users: administrator and operator. Each has its own password.

Secured Remote Software Upgrade

FullMax supports secure remote SW download to the Base Station and the Remote Station as follows:

The flash memory in the Base Station and the Remote Stations have two partitions. Each of these partitions accommodates one full load.

The downloaded file has a checksum code used at the Base Station and the Remote Station to verify its integrity.

The new load does not override the current operational load in the non-volatile memory before its integrity is verified by means of a checksum. If an error is detected, the new load is discarded.

ANNEX A: FULLMAX SPECIFICATIONS

RF Specifications

Duplexing mode	Time Division Duplexing (TDD)
Spectrum allocation	Either paired or unpaired
Operational Frequency range	Configurable from 40 MHz to 958 MHz
Frequency Resolution	3 Hz
Frequency Accuracy	± 1 ppm Max (1 ppb if GPS synchronized external clock is used)
IF Frequency	1,220 MHz
RF Front End Phase Noise	-97dBc / Hz @ 10 kHz offset
Channel Bandwidth	Programmable from 200 kHz to 5 MHz, including: 200 kHz, 400 kHz, 500 kHz, 1 MHz.
Multicarrier Scheme	128 FFT
Permutations	Downlink: PUSC, AMC 2X3; Uplink: PUSC, AMC 2X3
Support of Multiple Zones	Yes
Sub-channelization	PUSC: 3 downlink sub-channels and 4 uplink sub-channels; AMC 2X3: 6 downlink and uplink sub-channels
Cyclic Prefix	1/8
TDD downlink/uplink ratio	Programmable. For a reverse symmetrical application (e.g. SCADA), more bandwidth can be allocated to the uplink.
TTG, RTG	Programmable
Distance	Determined by path loss only.
Max Effective TX Power	Base Station: Upto 40 dBm with default PA, upto 43 dBm with high power PA Remote Station: Upto 40 dBm with default PA, upto 43 dBm with high power PA
TX Power Range	79 dB (-43 dBm to +36 dBm)
TX Power Resolution	0.5 dB
Noise Figure	5 dB

CINR for AWGN channel	QPSK	1/2	:	5	dB	
	QPSK	3/4	:	8	dB	
	16QAM	1/2	:	11	dB	
	16QAM	3/4	:	14	dB	
	64QAM	1/2	:	16	dB	
	64QAM	2/3	:	18	dB	
	64QAM	3/4	:	20	dB	
RX Sensitivity @ 500 kHz channel bandwidth	QPSK	1/2	:	-107	dBm	The receiver sensitivity can be further improved with the use of subchannels and ARQ / HARQ
	QPSK	3/4	:	104	dBm	
	16QAM	1/2	:	100	dBm	
	16QAM	3/4	:	98	dBm	
	64QAM	1/2	:	98	dBm	
	64QAM	2/3	:	94	dBm	
	64QAM	3/4	:	92	dBm	

PHY Specifications

Protocol	ieee802.16e-2005 with extensions.
Type	Multi Carrier
Number of Subcarriers	128, 512, 1024, 2048 depending on channel bandwidth
Modulation Schemes	BPSK, QPSK, 16QAM, 64QAM
FEC	Convolutional Coding (CC) with rates: 1/2, 2/3, 3/4
Adaptive Modulation and Coding (AMC)	FullMax supports AMC on an individual Mobile and Fixed Subscriber Station basis for both the downlink and uplink (i.e., each MS and FS is allocated the highest AMC scheme dynamically depending on its CINR in any point in time. The Link Adaptation and Power Control algorithm is designed for maximum throughput and not for minimum power.
Retransmissions	ARQ

MAC Specifications

Multiple Access Method	Two dimensional TDMA and OFDMA
Standard	ieee802.16e-2005
Scheduling Methods	Best effort (BE), Non Real Time Polling (nrTPS), Real Time Polling (rtPS), Extended Real time Polling (ErtPS), Unsolicited Grant Service (UGS)
QoS Parameters	Priority, minimum rate, maximum rate, maximum burst size, jitter, latency
QoS Priorities	7
QoS Classifiers	- Up to 16 classifiers per subscriber station - Classifier fields: Ethernet, IP, UDP/TCP header fields
Compression	Payload Header Suppression (PHS).

Up to 256 bytes of layer two, layer three and higher header fields.

Security

Air Link Encryption	128 bits AES
Key Management Protocol	PKMv2
Authentication	EAP-TLS after RSA X.509 certificates

Remote Management and Control

Architecture	Web based
Management Protocol	SNMP v2, CLI
MIB	Standard WiMAX MIBs + FullMax private MIB
Fault Management	Traps, events and audit logs. Real-time remote diagnostic tool
Configuration	Profile based configuration.
Security	https
Remote SW download	Yes, Over the Air

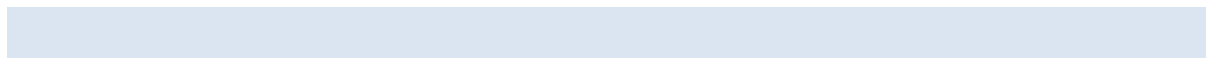
Interface

LAN	RJ45, 100 BaseT
RF	N-Connector, 50 ohm
RS232	DB-9 (indoor) or RJ45 (outdoor) FullMax RS232 interface supports all RS232 control function for legacy SCADA interface
GPS	TNC GPS is used for time synchronization (external clock and 1 PPS). It is mandatory at the Base Station and optional at the Remote Station
Power	The Base Station and the Remote Station are designed for DC power source between 9 VDC and 36 VDC.

Mechanical Environment

Base Station	Rack mount 19" ,1 U Enclosure <i>Indoor unit</i>
Fixed Station	Length = 27.8 mm (1.1 ") Width = 19.8 mm (0.8 ") Height = 7.2 mm (0.283 ") Wall Mount (indoor) or Pole Mount (outdoor)

Temperature	Indoor Base Station and Fixed Remote Station: -40°C to +70°C Outdoor Remote Station: - 30°C to +75°C
Humidity	95%



FCC compliance statement (United States)

FCC CLASS B PART 15

This device complies with Part 15 of the Federal Communications Commission (FCC) Rules. The FCC ID for this device is X27-FS-218. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

CAUTION:

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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 in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instructions, may cause interference harmful to radio communications.

There is no guarantee, however, that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer for help