Documentation Code	ALB-M-135001en

ARBA135 BS Series User Guide

MAC Release: **3.3**

Doc. Rev. **A1**, September 2010

albentia Systems

C/ Margarita Salas, 22
Parque Tecnológico de Leganés
28918 Leganés (Madrid)
SPAIN

Tel.: +34 91 440 02 13
Fax: +34 91 440 05 69
www.albentia.com

Copyright and confidentiality information

PUBLICATION HISTORY

The publication history for this document is given in Table 1.

Rev.	Author	Date	Description
A1	C. Sánchez	*September 2010*	First version

Table 1 - Publication History

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF TERMS AND DEFINITIONS

Table 2 summarizes abbreviations and terms used in this document.

Term	Description
3DES	*Triple-DES*
AA	*Authentication and Authorization*
AAA	*Authentication, Authorization and Accounting*
AES	*Advanced Encryption Standard*
AGC	*Automatic Gain Control*
AK	*Authorization Key*
ARP	*Address Resolution Protocol*
ARQ	*Automatic Repeat reQuest*
ASCII	*American Standard Code for Information Interchange*
AST	*Allocation Start Time*
ATM	*Asynchronous Transfer Mode*
BE	*Best Effort*
BPDU	*Bridge Protocol Data Unit*
BPSK	*Binary PSK*
BS	*Base Station*
BW	*Bandwidth*
CA	*Certification Authority*
CID	*Connection Identifier*
CINR	*Carrier to Interference and Noise Ratio*
CLI	*Command-line interface*
SS	*Costumer Premise Equipment*
CE	*Conformité Européenne*
CPS	*Common Part Sublayer*
CRC	*Cyclic Redundancy Check*
CS	*Convergence Sublayer*
CSL	*Convergence SubLayer*
CSV	*Comma Separated Values*
DC	*Diffserv Codepoint*
DCD	*Downlink Channel Descriptor*
DCE	*Data Communication Equipment*
DES	*Data Encryption Standard*

DFS	*Dynamic Frequency Selection*
DHCP	*Dynamic Host Configuration Protocol*
DiffServ	*Differentiated Services*
DL	*DownLink*
DLFP	*DownLink Frame Prefix*
DoC	*Declaration of Conformity*
DNS	*Domain Name System*
DSA-ACK	*Dynamic Service Addition Acknowledge*
DSA-REQ	*Dynamic Service Addition Request*
DSA-RSP	*Dynamic Service Addition Response*
DSAP	*Destination Service Access Point*
DSCP	*Differentiated Services Code Point*
DTE	*Data Terminal Equipment*
ECN	*Explicit Congestion Notification*
EEA	*European Economic Area*
EFTA	*European Free Trade Association*
EIRP	*Equivalent Isotropically Radiated Power*
ERTPS	*Extended Real Time Polling Service*
ETSI	*European Telecommunications Standards Institute*
EU	*European Union*
FCC	*Federal Communications Commission*
FDD	*Frequency Division Duplex*
FEC	*Forward Error Correction*
FCH	*Frame Control Header*
FSN	*Fragment Sequence Number*
FTP	*File Transfer Protocol*
FTP	*Foiled Twisted Pair*
GPS	*Global Positioning System*
GSM	*Global System for Mobile communications*
HTTPS	*Hypertext Transfer Protocol over Secure Socket Layer*
HW	*Hardware*
IANA	*Internet Assigned Numbers Authority*
ICMP	*Internet Control Message Protocol*
IDU	*Indoor Units*
IE	*Information Element*
IEEE	*Institute of Electrical and Electronics Engineers*

IGMP	*Internet Group Management Protocol*
IP	*Internet Protocol*
IPTV	*Internet Protocol Television*
ISM	*band industrial, scientific and medical band*
LAN	*Local Area Network*
LED	*Light-emitting Diode*
LI	*Leap Indicator*
LDAP	*Lightweight Directory Access Protocol*
MAC	*Medium Access Control*
MAN	*Metropolitan Area Networks*
MPEG	*Moving Pictures Experts Group*
NAT	*Network Address Translation*
NLOS	*Non Line of Sight*
NRTPS	*Non-Real Time Polling Service*
NTP	*Network Time Protocol*
OCXO	*Oven-Controlled Crystal Oscillator*
ODU	*Outdoor Unit*
OFDM	*Orthogonal Frequency Division Multiplexing*
PDU	*Protocol Data Unit*
PHY	*Physical Layer*
PM	*Poll-Me*
PoE	*Power Over Ethernet*
PPS	*Pulse-per-second*
PS	*Physical Slot*
PSE	*Power Supply Equipment*
PSK	*Phase-Shift Keying*
PtMP	*Point to Multi-Point*
PtP	*Point to Point*
QAM	*Quadrature Amplitude Modulation*
QoS	*Quality Of Service*
QPSK	*Quadrature PSK*
RADIUS	*Remote Authentication Dial In User Service*
REG-REQ	*Registration Request*
REG-RSP	*Registration Response*
RF	*Radio Frequency*
RFC	*Request For Comments*

RNG-REQ	*Ranging Request*
RNG-RSP	*Ranging Response*
RSA	*Rivest, Shamir, Adleman*
RSSI	*Received Signal Strength Indication*
RTC	*Real Time Clock*
RTPS	*Real Time Polling Service*
RTT	*Round-Trip Delay time or Round-Trip Time*
RX	*Reception*
R&D	*Research and Development*
SA	*Spectrum Analizer*
SAP	*Service Address Point*
SBC-REQ	*SS Basic Capability Request*
SBC-RSP	*SS Basic Capability Response*
SCP	*Secure Copy*
SCU	*Sector Control Unit*
SDU	*Service Data Unit*
SF	*Service Flows*
SFID	*Service Flow Identifier*
SI	*Slip Indicator*
SL	*System Losses*
SMC	*Secondary Management Connection*
SNR	*Signal to Noise Ratio*
SNMP	*Simple Network Management Protocol*
SPC	*Space Time Coding*
SS	*Subscriber Station*
SSAP	*Source Service Access Point*
SSH	*Secure Shell*
SSL	*Secure Socket Layer*
STP	*Shielded Twisted Pair*
STP	*Spanning Tree Protocol*
SW	*Software*
TCP	*Transmission Control Protocol*
TEK	*Traffic Encryption Key*
TOS	*Type of Service*
TDD	*Time Division Duplex*
TDM	*Time Division Multiplexing*

TFTP	*Trivial File Transfer Protocol*
TX	*Transmission*
UCD	*Uplink Channel Descriptor*
UDP	*User Datagram Protocol*
UGS	*Unsolicited Grant Service*
UTC	*Universal Time Coordinated*
UTP	*Unshielded Twisted Pair*
UL	*UpLink*
UMTS	*Universal Mobile Telecommunications System*
UPS	*Uninterruptible Power Supply*
VLAN	*Virtual LAN*
VNF	*Virtual Noise Floor*
VoIP	*Voice over Internet Protocol*
WiMAX	*Worldwide Interoperability for Microwave Access*
XML	*Extensible Markup Language*
XML-RPC	*XML Remote Procedure Call*

Table 2 - List of Terms

1. INTRODUCTION

1.1. About this document

Albentia Systems proudly introduces the **ARBA135** series, the first truly WiMAX interoperable Base Station system operating in the 3.5 GHz licensed ETSI/FCC bands. This document is a User Guide that includes all the required information to install and configure this unit in a simple and quick way. This manual is intended to show a complete overview of the unit, giving the reader the necessary knowledge to deploy correctly an entire WiMAX network.

In the following points information about the standard *IEEE 802-16-2009* is presented, together with the connection schemes of the unit, the configuration parameters and all the information needed to make a first approach to the technology. Later, both Web and CLI user interfaces will be explained more in detail.

In addition, the new local provisioning system will be described in detail. Very deep and important changes can be found in the new software version, and this document tries to cover all of them, including the new provisioning philosophy and its procedures. This system is a method in which users and services are provisioned in a local database saved in the storage memory of the BS equipment. This innovative operation mode leaves nearly all the network's functionalities and management on the BS, offering a secure and centralized solution to operators.

NOTE

All the pictures shown in this document are referred to the software version called "Fwood 3.3". Screenshots and contents may change in new releases of the system, as Albentia Systems ARBA135 family is always being improved.

1.2. First approach to the WiMAX standard

This unit is fully based on the *IEEE 802.16-2009* standard, comprising a high number of specifications for radio communications equipment for microwave bands. *WiMAX* (*Worldwide Interoperability for Microwave Access*) is a wireless technology included in this standard which offers broadband connectivity both for Access and Backhauling applications.

The *WiMAX* Forum is an organization that defines a profile about *IEEE 802.16-2009* standard as a subset of functionalities and specifications that units marked as *WiMAX Certified* must fulfil. It also defines the interoperability test and it selects the official certifier organizations. In this way, the proper way to define this device is saying that it is based on *IEEE 802.16-2009* standard.

The following points are intended to be a first approach to this technology, so only the more basic points will be explained. However, for a more extended knowledge around this technology it is advisable to look up directly in the *IEEE 802.16-2009* standard.

1.2.1. Basic operation

WiMAX is completely different from other technologies such as *Ethernet* or *Wi-Fi*; its concept is closer to GSM or UMTS technologies. *WiMAX* is in fact conceived for

Metropolitan Area Networks (MAN), rather than to the Local Area Network (LAN) orientation of *Wi-Fi*.

This system conception assigns all the control over the radio medium to the Base Station, which is responsible of managing the *WiMAX* frame. This method guarantees a total control over transmissions and ensures QoS.

Almost any digital communication protocol can be carried over *WiMAX* protocol, as it will be seen later in this guide. The *IEEE 802.16-2009* standard defines adaptive layers for cell-oriented protocols (ATM) for packet-oriented protocols (Ethernet or IP), and also specifies mechanisms to transmit TDM-circuit protocols (such as E1/T1). However, it does not specify them, letting the final implementation to vendors.

Although it is a packet transmission protocol (PDUs), it is connection-oriented philosophy allows reserving resources and guaranteeing QoS.

1.2.2. System topology

WiMAX is based on a star-topology with a master station and several slave stations. The master node is the base station (*BS*) and the slaves are the subscriber stations *(SS)*, which can also be known as CPEs *(Costumer Premise Equipment)*. Nearly all the network intelligence is on the BS, which controls many parameters and provides service to every SS.

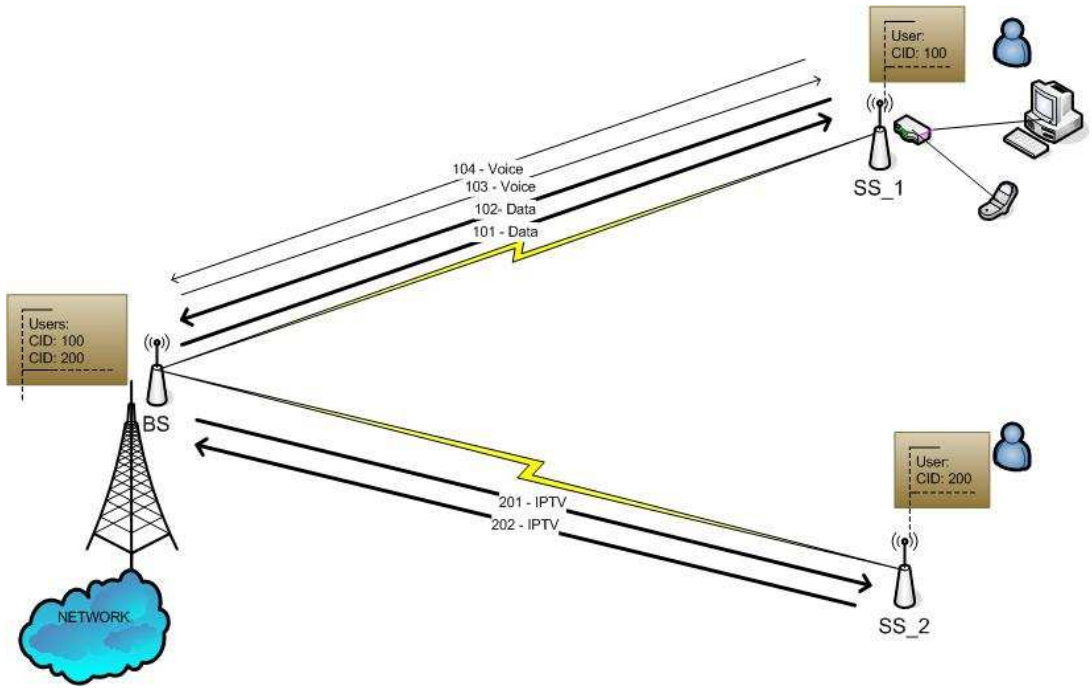


Figure 1 - Basic operation scheme

Figure 1 shows a basic operation scheme which can help to understand better the "*User*" and "*Service flow*" concepts. It represents a PtMP scenario formed by a BS and two SS units. Using the same radio channel for both stations, the BS is provisioning two different users (*User CID* 100 and *User CID* 200 in the example) and a total amount of six unidirectional *Service Flows* (SF): two pairs of SFs for *User CID* 100 and one pair of SFs for *User CID* 200. Each par of flows is designed to carry different types of application services. This is a great advantage in WiMAX: although the physical medium is the same for every station connected to the BS, the Service Flow architecture allows applying different QoS features to every final service, so the customer gains total control over the communications.

1.2.3. WiMAX terms: Frame, Burst, User and Connection

From a physical-layer point of view, *WiMAX* is a completely framed system where time slots are reserved for each connection, so end-to-end QoS parameters can be guaranteed for each service even with a variable physical medium. The frame duration (as many other parameters) is controlled by the BS, which broadcasts it periodically together with other network parameters by a specific control message. The standard defines different frame durations from 2.5 ms to 20 ms.

Depending on the system configuration type, there are two types of frame multiplexing: **FDD** (*Frequency Division Duplex*) and **TDD** (*Time Division Duplex*). In FDD configuration (typically used in licensed bands) there are two independent radio channels for UL and DL, so the 100% of the frame duration is always used in both directions, each one with an independent radio channel. On the other hand, TDD performs time multiplexing: the BS decides how much of the frame duration will be reserved for the Downlink (DL) and how for the Uplink (UL), so there is a unique radio channel to transmit and receive alternatively. TDD is the typical configuration **ARBA135** will operate in this mode.

- **TDD frame description**

  In TDD, every frame will be divided in two parts: the part dedicated for the Uplink will be the *UL subframe*, and the part dedicated for the Downlink will be the *DL subframe*. The *DL subframe* consists of only one downlink PHY PDU. The *UL subframe* consists of contention intervals scheduled for initial ranging and bandwidth request purposes and one or multiple uplink PHY PDUs, each transmitted from a different SS. The detailed structure of a frame is shown in Figure 2.

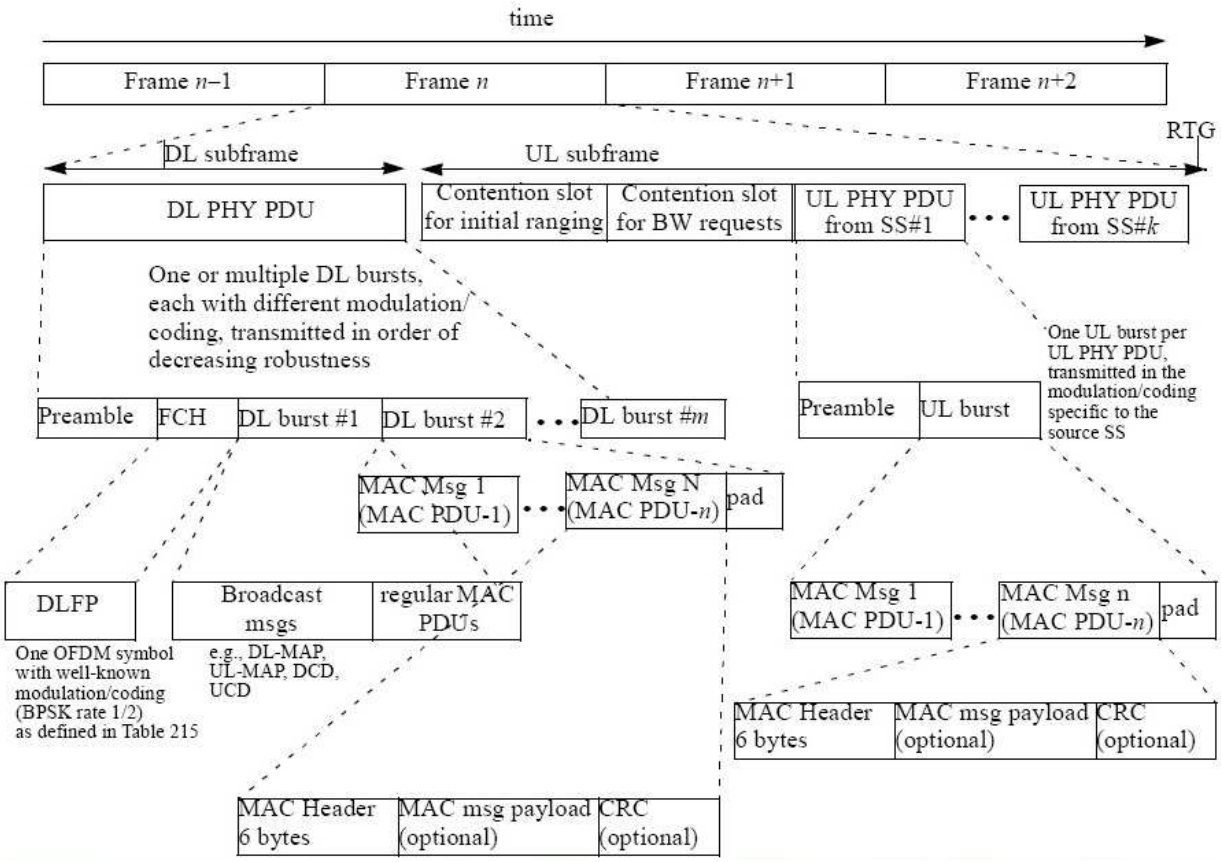


Figure 2 - OFDM frame structure, in TDD

A downlink PHY PDU starts with a long preamble, which is used for PHY synchronization. The preamble is followed by a FCH burst (*Frame Control Header*), one OFDM symbol long and transmitted using BPSK-½ rate with the mandatory coding scheme. The FCH contains a DLFP (*DL Frame Prefix*) to specify burst profile and length of one or several downlink bursts immediately following the FCH. A DL-MAP message, if transmitted in the current frame, shall be the first MAC PDU in the burst following the FCH. An UL-MAP message shall immediately follow either the DL-MAP message (if one is transmitted) or the DLFP. If UCD (*Uplink Channel Descriptor*) and DCD (*Downlink Channel Descriptor*) messages are transmitted in the frame, they shall immediately follow the DL-MAP and UL-MAP messages.

The FCH is followed by one or multiple downlink bursts, each transmitted with different burst profile. Each downlink burst consists of an integer number of OFDM symbols. Location and profile of the first downlink burst is specified in the DLFP. The location and profile of the maximum possible number of subsequent bursts shall also be specified in the DLFP. At least one full DL-MAP must be broadcast in burst #1 within a fixed interval. Location and profile of other bursts are specified in DL-MAP. Profile is specified either by a 4-bit Rate_ID (for the first DL burst) or by DIUC. The DIUC encoding is defined in the DCD messages.

With the OFDM PHY, a PHY burst, either a downlink PHY burst or an uplink PHY burst, consists of an integer number of OFDM symbols, carrying MAC messages, i.e., MAC PDUs. Then the payload should be randomized, encoded, and modulated using the burst PHY parameters specified by this standard. If an SS does not have any data to be transmitted in an UL allocation, the SS shall

transmit an UL PHY burst containing a "*Bandwidth Request*" header with its basic CID. An SS shall transmit during the entirety of all of its UL allocations, using the standard padding mechanism to fill allocations if necessary.

- **User and connection management**

A base station is responsible of managing all the connected users. Each user that connects correctly to a BS has a unique identifier (also called basic CID). Using this CID, the BS and SS exchange high priority control information. The base station is in charge of dividing each subframe (UL and DL) in time slots that will be allocated for different users. In that sense, *WiMAX* is basically a dynamic TDM system. Thus, the slots' length, position and codification are selected dynamically by the BS taking into account the current configuration, QoS parameters and bandwidth requirements for each user, as long as the link state in that moment.

In general, and mainly for the UL, there is a direct relation between the slot assigned to a user and the *burst* term. A *burst* is a set of consecutive symbols assigned to one user, having all these symbols the same modulation and codification. For example, it can be said that the UL has 3 burst assigned to users SS0, SS1 and SS3. Each burst may have different modulation, because users with good SNR will be able to use better modulations with higher throughputs than those modulations in worse link conditions. Besides the basic CID explained previously, the users connected to the BS must establish connections or services (*Service Flows*) in order to be able to transmit information. Each connection has a unique identifier or CID. For example, a user with CID 100 could have 3 connections: 101, 102, and 103 for data transmission.

It is very important to note that these service flows are unidirectional, so CIDs will be unidirectional too. There must be at least a downlink service and an uplink service in order to establish a bidirectional communication between a BS and a SS. The basic CIDs that are required to provide service to a user are bidirectional, so they take up the two UL and DL possibilities.

1.2.4. Control over the radio parameters

The *IEEE 802.16-2009* standard uses an OFDM digital modulation (*Orthogonal Frequency Division Multiplexing*) with 256 subcarriers that allows optimum communications in the most severe channel conditions. Besides, adaptive modulation for each subcarrier is also used depending on the SNR of the radio link. There are 7 available modulations: BPSK-1/2, QPSK-1/2, QPSK-3/4, 16QAM-1/2, 16QAM-3/4, 64QAM-2/3 and 64QAM-3/4, which will be selected by the BS depending on the existing link conditions. BPSK provides the higher robustness at expense of reducing the throughput, but is easier to demodulate so the receiver's sensibility is lower and in conclusion longer distances can be covered. On the other hand, 64QAM is optimum for links with low interference allowing the highest bitrates. These adaptive techniques allow a high use of the available bandwidth and a high spectral efficiency.

Regarding the transmitted power, the SSs usually perform AGC (*Automatic Gain Control*). The main goal of this technique is to be able to transmit every moment with the power that the BS asks for, which implies a reduction of the power consumption and the interferences between SSs.

On the other hand, at the BS the power control should be done manually by the operator. As explained before, the BS controls and selects a lot of communication aspects: modulation, frame duration, channel bandwidth… and so does it happen with the SS transmission power. It is only possible to manually adjust transmission power at

the BS; as long as the transmission power of the SS will be automatically adjusted following the orders received from the BS. When a SS is powered on, it begins to perform a power scanning: it increases power slowly and cyclically until it is detected by a BS. When the BS notices that there is a SS performing this scan, it indicates to this unit the optimum transmission power that should use in order to establish a correct communication.

1.2.5. MAC Layer

The MAC Layer definition is probably the more powerful advantage of this standard, and it is the main difference between WiMAX and other competing technologies. Extremely efficient, it is designed to obtain the best performance of the radio channel.

Other technologies use statistic MAC-Layer with contention access and burst-transmission. This means that all users compete for using the channel. If two or more users transmit at the same time, collisions are produced and the overall throughput gets reduced. In these conditions, it is impossible to guarantee QoS, as the performance of a user depends directly on the other users' behaviour. In addition, this algorithm establishes many "no-transmission" times, so the medium is not used on an efficient way, reducing the achievable throughput.

On the other hand, WiMAX uses a deterministic MAC-Layer where the communication is performed using predefined frames. In addition, this system is contention free: users do not compete for the channel (they only compete once, in the initial entry to the network. Once inside, there is no more contention). There is a master node which decides who transmits, for how long, and even with which modulation. The allocation of the frame slots is described by the master station in the frame map at the beginning of each frame. The Slave unit simply follows the instructions from the master unit and transmits only during the symbols allocated to the uplink.

This intelligent unit is the BS, which can control the QoS parameters by balancing the *Time Slots'* assignments, as it knows the needs of all units every moment. In addition, as the slave units are only allowed to transmit when the BS decides it, there are not collisions or unused slots, so the channel can be used in a much more efficient way, increasing dramatically the overall performance and aggregated throughput.

1.2.6. Convergence layers

The reference model associated to the *IEEE 802.16-2009* standard is shown in Figure 3, where it can be seen the MAC layer over the physical layer. The MAC layer is divided in three sublayers: Convergence, Common Part and Security.

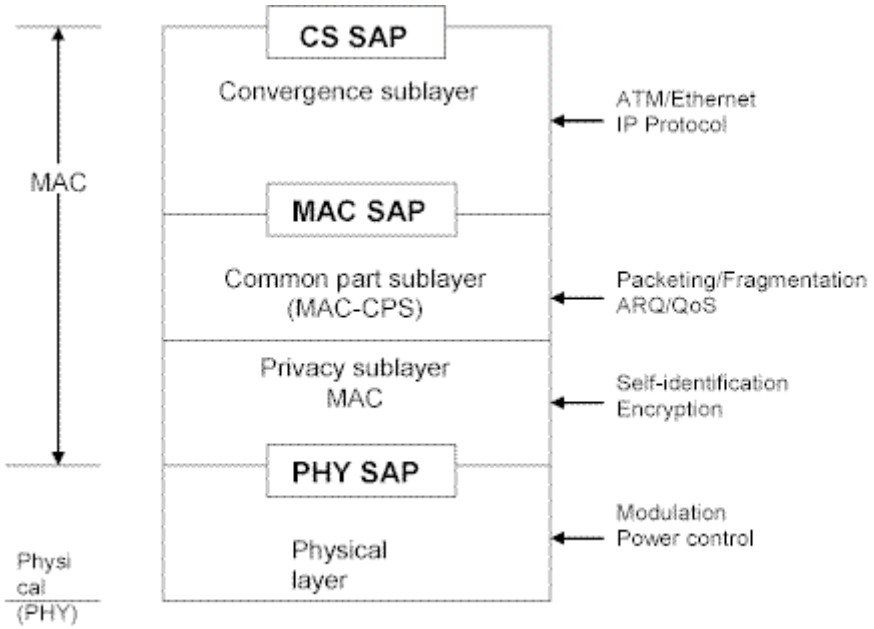


Figure 3 - *IEEE Std. 802.16-2009* protocol layering

Convergence SubLayer (CSL) is responsible of adapting the data units from high level protocols to the MAC-SDU format, and vice versa. Regarding to the QoS control, it is in charge of classifying the incoming SDUs following the established criteria, and it sends differentiated data flows to the lower sublayer.

The main sublayer is the *Common Part Sublayer* (CPS), which comprises the system accessibility functionalities, the bandwidth managing, connections' establishment, and connections' maintenance. It takes the different data flows (already classified) from the above sublayer and performs the resource allocation. The *Scheduler* is the responsible of this allocation, and allows the deterministic resource allocation in accordance with the QoS agreement for each service. This sublayer is strongly related with the Security sublayer.

The MAC layer has an additional Security sublayer that allows providing authentication, key exchanging, and encryption. When defined, this layer performs the PDUs exchange between the MAC and the physical layer.

1.2.7. Network entry and initialization

The *IEEE 802.16-2009* standard establishes the applicable procedures for entering and registering a new SS or a new node to the network. The SS initialization procedure of an SS is shown in Figure 4. This figure shows the overall flow between the stages of initialization in an SS. This shows no error paths and is shown simply to provide an overview of the process.

The procedure is divided in different phases, while the implementation of some phases (i.e. "*Establish Time of the Day*" or "*Establish IP Connectivity*") at the SS is optional. In the following some of the main phases will be explained briefly:

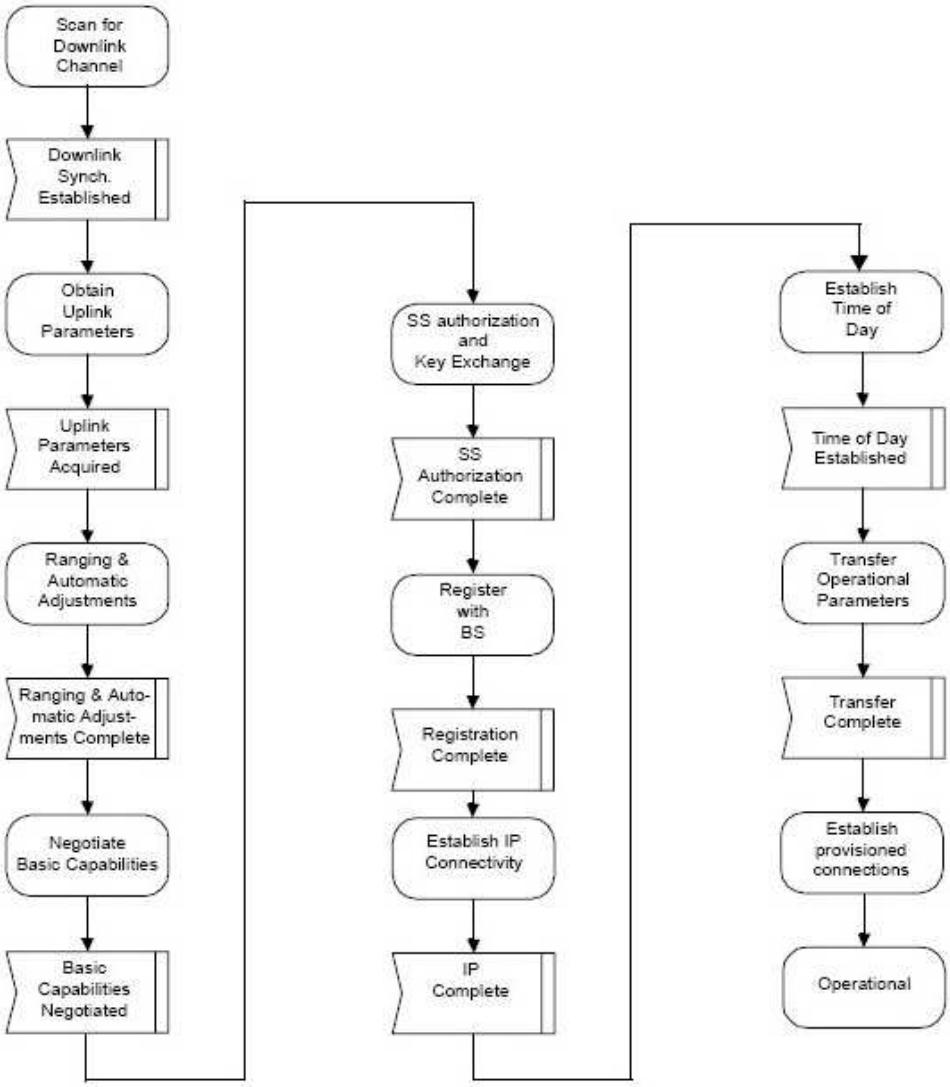


Figure 4 - SS initialization overview

a) **Scanning and synchronization to the downlink**: on initialization or after signal loss, the SS shall acquire a downlink channel. The SS shall have non-volatile storage in which the last operational parameters are stored and shall first try to reacquire this downlink channel. If this fails, it shall begin to continuously scan the possible channels of the downlink frequency band of operation until it finds a valid downlink signal. Once the PHY has achieved synchronization, as given by a PHY Indication, the MAC shall attempt to acquire the channel control parameters for the DL and then the UL.

b) **Obtaining downlink parameters**: The MAC shall search for the DL-MAP MAC management messages. The SS achieves MAC synchronization once it has received at least one DL-MAP message. An SS MAC remains in synchronization as long as it continues to successfully receive the DL-MAP and DCD messages for its Channel. If a certain time is elapsed without receiving DL-MAP messages, the SS shall try to re-establish synchronization.

c) **Obtaining uplink parameters**: After synchronization, the SS shall wait for a UCD message from the BS in order to retrieve a set of transmission parameters for a possible uplink channel. These messages are transmitted periodically from

the BS for all available uplink channels and are addressed to the MAC broadcast address. If no uplink channel can be found after a suitable timeout period, then the SS shall continue scanning to find another downlink channel. The SS shall determine from the channel description parameters whether it can use the uplink channel. If the channel is not suitable, then the SS shall continue scanning to find another downlink channel. If the channel is suitable, the SS shall extract the parameters for this uplink from the UCD. It then shall wait for the next DL-MAP message and extract the time synchronization from this message. Then, the SS shall wait for a bandwidth allocation map for the selected channel. It may begin transmitting uplink in accordance with the MAC operation and the bandwidth allocation mechanism.

d) **Initial ranging and automatic adjustments**: Ranging is the process of acquiring the correct timing offset and power adjustments such that the SS's transmissions are aligned with the BS receive frame, and received within the appropriate reception thresholds. Ranging Request (RNG-REQ) message shall be transmitted by the SS during the *Initial Ranging* phase and periodically to determine network delay and to request power and/or downlink burst profile change. Ranging Response (RNG-RSP) message shall be transmitted by the BS in response to a received RNG-REQ. In addition, it may also be transmitted asynchronously to send corrections based on measurements that have been made on other received data or MAC messages. As a result, the SS shall be prepared to receive an RNG-RSP at any time. If initial ranging is not successful, the procedure is restarted from scanning to find another downlink channel.

e) **Negotiating basic capabilities:** Immediately after completion of ranging, the SS informs the BS of its basic capabilities by transmitting a SBC-REQ message. The BS responds with an SBC-RSP message.

f) **SS authorization and key exchange**: The BS and SS shall perform authorization and public key exchange using X.509 digital certificates.

g) **Registration**: Registration is the process by which the SS is allowed entry into the network and a managed SS receives its Secondary Management CID and thus becomes manageable. To register with a BS, the SS shall send a Registration Request (REG-REQ) message to the BS. The BS shall respond with a Registration Response (REG-RSP) message. For an SS that has indicated being a managed SS in the REG-REQ message, the REG-RSP message shall include the Secondary Management CID. Once the SS has sent a REG-REQ to the BS, it shall wait for a REG-RSP to authorize it to forward traffic to the network.

h) **Establishing provisioned connections:** After the transfer of operational parameters (for managed SS) or after registration (for unmanaged SS), the BS shall send DSA-REQ messages to the SS to set up connections for pre-provisioned service flows belonging to the SS. The SS responds with DSA-RSP messages. Once the service flows are added, the SS has successfully entered the network and may start transmitting.

NOTE

RNG-REQ, RNG-RSP, REG-REQ, REG-RESP and all the messages mentioned above are MAC management messages, carried in the payload of the MAC PDU.

1.2.8. QoS control

QoS can be defined as a set of mechanisms that can guarantee the transmission of a certain amount of data in a maximum specified time, or that can control the resource allocation between nodes in order to perform a communication. The guarantee of QoS is a very desirable parameter for operators and providers because it allows them to guarantee certain minimum conditions to their clients, like a minimum bandwidth or a maximum end-to-end delay. It can also provide priorities to different users or data flows. Guarantying a minimum service levels is critic in certain applications like VoIP, IPTV or real time video, especially with limited network capacity or high number of users. In these scenarios the QoS plays a basic role. QoS mechanisms also allow offering Differentiated Services (*DiffServ*).

A device that implements mechanisms for guaranteeing QoS should perform at least two differentiated processes: classification and resource allocation. This is shown schematically in Figure 5. In the first phase packets are classified into different data flows using the available criteria: DSCP/TOS, VLAN tags, IP or MAC addresses, source or destination port… Once these flows are created and data is classified, the device will route the packets in a deterministic way, sending first the higher priority ones. In conclusion, this structure of differentiated data flows allows implementing QoS mechanisms that can guarantee some minimum parameters.

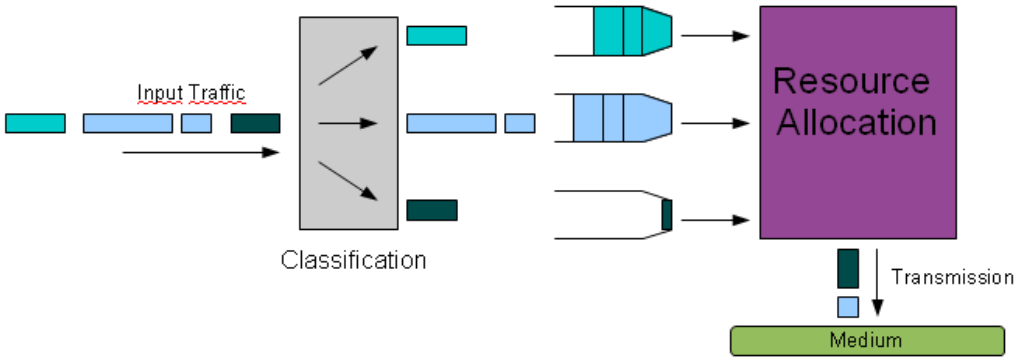


Figure 5 - Simple block diagram of a QoS mechanism

WiMAX technology implements up to level 2 QoS mechanisms, and supports 5 different types of service: BE (*Best Effort*), RTPS (*Real Time Polling Service*), ERTPS (*Extended Real Time Polling Service*), NRTPS (*Non-Real Time Polling Service*) and UGS (*Unsolicited Grant Service*).

1.3. Interoperability

Many manufacturers design and distribute proprietary solutions to offer wireless broadband solutions in the 3.5 GHz licensed band. In many cases these products are wrongly called “Pre-WiMAX”, a confuse term as they are technologies far away from the *IEEE 802.16-2009* standard (WiMAX), and more similar to other technologies such as *IEEE 802.11a (Wi-Fi).*

Thus, it is very important to realise that the acquired unit is 100% WiMAX: completely interoperable *IEEE 802.16-2009* standard compliant equipment working in the 3.5GHz licensed band, with all the proved advantages of this technology: OFDM with 256 subcarriers, framed and deterministic MAC, great spectral efficiency, real guarantees of QoS… *Albentia Systems* is proud of being the first manufacturer in the

world to present this kind of equipment, which offers an awesome performance comparing to other proprietary solutions.

Why is so important to be compliant with a standard? First of all, because the standard is supposed to work pretty well: the *IEEE* is a leading professional organization where hundreds of engineers have worked for years to define an innovative and efficient technology, defining all the specifications and every detail in WiMAX. All these human resources are supposed to guarantee a nearly unbeatable technology, at least up to now, so the equipment's total compliance with the standard should be a clear guarantee of success.

But probably the main advantage when following a standard is that it offers the possibility to achieve the *Interoperability*. Speaking about interoperability in WiMAX means that the BS is able to register, communicate with and interchange information with SSs of other vendors. Besides, this is probably the easiest way to certify that a WiMAX BS is fully compliant with the standard: checking its interoperability with other vendor's equipment.

The **ARBA135** can work successfully with many SS units from other manufacturers, and the number keeps growing. Interoperability is a powerful advantage which gives the operator more flexibility when acquiring SS units, increasing the possibilities to find the most appropriate solution and in conclusion reducing the total deployment costs.

1.4. System specifications

Radio parameters			
Frequency Band		3400-3600MHz. 3.3 and 3.6GHz optional	
Modulation		OFDM IEEE 802.16-2009 - 256 subcarriers, cyclic prefix 1/4, 1/8, 1/16 or 1/32	
Supported channel bandwidth		3.5, 7 MHz	
Adaptive modulation		BPSK, QPSK, 16QAM and 64QAM	
FEC code rate		1/2, 2/3 and 3/4 concatenated Reed-Solomon and *Viterbi*	
Maximum output power		+20 dBm	
Frame duration		2.5, 5, 10 & 20ms	
Duplexing method		TDD (Time Division Duplexing)	
Uplink/Downlink allocation		Programmable from 4:1 to 1:4	
Dynamic Frequency Selection		Yes	
Antenna connector		N-type, 50 ohms	
RF parameters	**Modulation**	**Sensitivity (3.5 MHz)**	**Sensitivity (7 MHz)**
	BPSK-1/2	-95 dBm	-92 dBm
	QPSK-1/2	-93 dBm	-90 dBm
	QPSK-3/4	-89.5 dBm	-86.5 dBm
	16QAM-1/2	-86.5 dBm	-83.5 dBm
	16QAM-3/4	-83 dBm	-80 dBm
	64QAM-2/3	-79 dBm	-75 dBm
	64QAM-3/4	-77 dBm	-74 dBm
Data traffic and Throughput			
Maximum over-the-air data rate		26.2Mbps (64QAM-3/4, 7 MHz BW)	
ARQ support		Yes, per IEEE 802.16-2009 standard - Selectable per service flow	
Simultaneous registered users	Basic	30	
	Advanced (2)	Unlimited	
Encryption		AES and 3DES	
Quality of Service (QoS)			
Supported QoS types		UGS, RTPS, nRTPS and BE (IEEE 802.16-2009 standard)	
Service differentiation	Layer-2	MAC source/destination address, EtherType, VLAN tag	
	Layer-3	DSCP ToS, IP source/destination address and subnet, Protocol type	
	Layer-4	TCP, UDP source/destination port range	
Differentiated service flows		Unlimited differentiated services per user	
Management and Provisioning			
Management local interfaces		Web, Command-Line Interface, RS232	
Management remote interfaces		SNMP, XML-RPC	
User and services local provisioning		XML local database	
User and services centralized provisioning		AAA Radius, LDAP, XML-RPC	
Network functionality			
Layer-2 Network functionality		Bridging (IEEE 802.1), VLAN (IEEE 802.1q)	
Layer-3 Network functionality		Static/Dynamic routing, NAT, DHCP server/client	
Supported CS		Ethernet, IPv4oEthernet, VLAN, IPv4oVLAN	
Networking modes		Bridge mode, IP routing	
Data interface		10/100 Base-T Ethernet RJ45	
Physical, Mechanical and Electrical			
Size		233 x 233 x 40 mm	
Outdoor Unit Weight		3 kg	
Power Supply	Basic	48V or 220VAC (802.3af compliant (PoE))	
Power Consumption		<18 Watts (full traffic conditions)	
Standards Compliance			
WiMAX		IEEE 802.16-2009 + Corrigendum IEEE 802.16-2005	
Radio		ETSI EN 301 893	
Environmental		ETSI EN 300 019-1-4 C4.1E (ODU), ETSI EN 300 019-1-3 C3.2 (IDU)	

1.5. CE Marking

The **CE marking** (also known as CE mark) is a mandatory conformance mark on many products placed on the single market in the **European Economic Area** (**EEA**). The CE marking certifies that a product has met EU consumer safety, health or environmental requirements. CE stands for *Conformité Européenne*, "European conformity" in French. The term initially used was "EC Mark" and it was officially replaced by "CE Marking" in the Directive 93/68/EEC in 1993. "*CE Marking*" is now used in all EU official documents.

CE Marking on a product indicates to governmental officials that the product may be legally placed on the market in their country, ensures the free movement of the product within the European Union (EU) and the European Free Trade Association (EFTA) single market (total 30 countries), and permits the withdrawal of the non-conforming products by customs and enforcement/vigilance authorities.

Albentia Systems declares that this equipment complies with the essential requirements and other relevant demands established in the *Directive 1995/5/EC*. A copy of the "***Declaration of Conformity (DoC)***" document may be obtained in this link:

http://www.albentia.com/Docs/CEcompliance.pdf (english version)

http://www.albentia.com/Docs/ConformidadCE.pdf (spanish version)

Figure 6- CE Marking logo

The European Economic Area (EEA) includes the 27 EU-Member States:

1. Austria (AT)
2. Belgium (BE)
3. Bulgaria (BG)
4. Cyprus (Greec part) (CY)
5. Czech Republic (CZ)
6. Denmark (DK)
7. Estonia (EE)
8. Finland (FI)
9. France (FR)
10. Germany (DE)
11. Greece (GR)
12. Hungary (HU)
13. Ireland (IE)
14. Italy (IT)
15. Latvia (LV)
16. Lithuania (LT)
17. Luxembourg (LU)
18. Malta (MT)
19. Netherlands (NL)
20. Poland (PL)
21. Portugal (PT)
22. Romania (RO)
23. Slovakia (SK)
24. Slovenia (SI)
25. Spain (ES)
26. Sweden (SE)
27. United Kingdom (GB)

)

as well as the 3 EFTA Member States:

28. Iceland (IS)

29. Liechtenstein (LI)
30. Norway (NO)

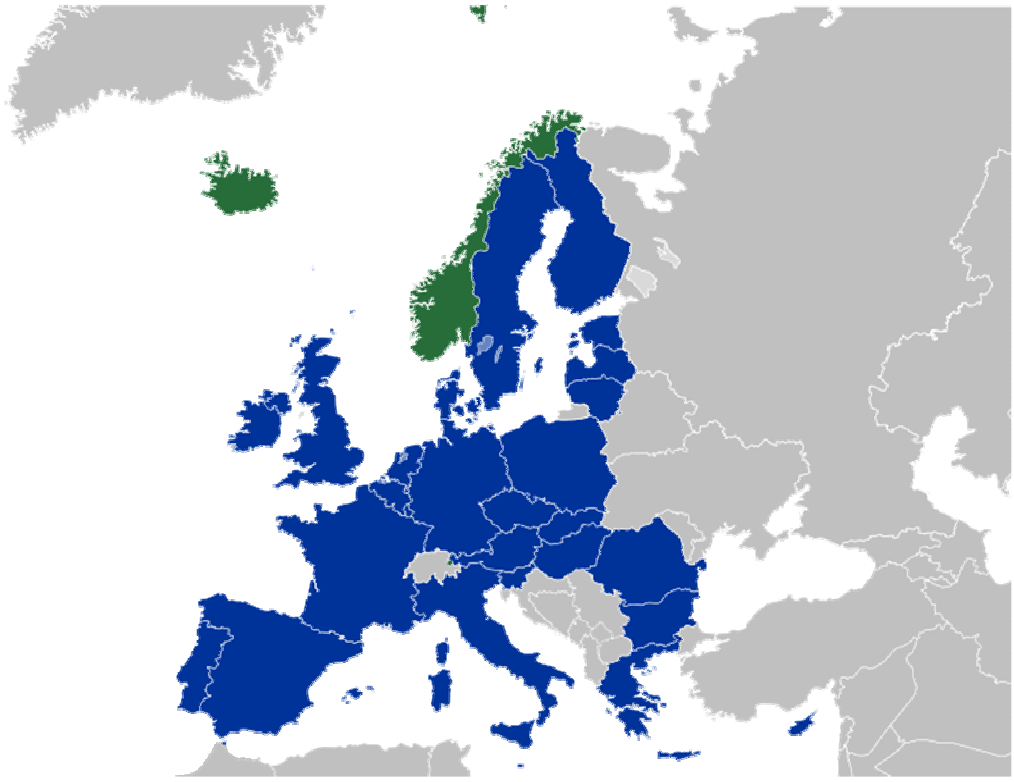


Figure 7 – European Economic Area map (2010)

1.6. About *Albentia Systems*

Albentia Systems is the Spanish leading provider of Broadband Wireless solutions. Founded in 2009 and headquartered in Madrid (Spain), *Albentia Systems* leverages its strong IP and systems expertise on a significant R&D effort to develop WiMAX-based innovative solutions for Access and Backhauling applications.

Albentia Systems' R&D teams benefit from a confirmed experience in some of the world's most renowned and challenging research labs. This dynamic group of engineers paves the way for our customers in the deployment of the industry's most advanced communications systems.

- **Our values**

  Albentia Systems' philosophy is sustained on two main values: **quality** and **transparency**.

  We are aware of the excellence of our products. And yet we want to go farther in the relationships with our customers. All our planning and organization processes are customer-oriented, in order for us to meet our customers' requirements and satisfy their needs in the most optimized manner. Furthermore, our customer management policy is based on proximity, communication, interaction and reactivity.

- **Our products**

Albentia Systems leverages on the most advanced technological innovations to offer products with an outstanding quality, capable of satisfying our customers' increasingly demanding needs.

The whole range of *Albentia Systems'* product lines implement the physical and access layers as defined in the *IEEE 802.16-2009* standard. Additionally, and as a member of the WiMAX Forum, *Albentia Systems* is fully committed to the development of Broadband Wireless industry, and to the interoperability of different communication systems.

2. FUNCTIONAL DESCRIPTION

This unit belongs to the high performing and well proven **ARBA135** family of single-sector and multiple-sector WiMAX Base Stations, which provide up to **26** Mbps Ethernet aggregated throughput per sector. In the following, some of the main features of the unit will be explained briefly.

- **Multi-purpose broadband wireless Access solution**

  ARBA135 is designed to give cellular coverage to Subscriber Stations in Point-to-Multipoint application scenarios, making it ideal for multi-user and multi-service networks. This family has been specifically designed for applications where broadband connectivity, QoS, security and privacy are critical requirements, thus making it the perfect solution in many different scenarios:
  - Provide Triple-Play services (Voice, Video, Data) in low-density areas where technical and economic factors inhibit DSL deployments.
  - Provide cost-effective last mile Access in rural or remote areas.
  - Make a fast roll-out and service delivery possible, thanks to its *Plug-and-Play approach.*
  - Usage as Metropolitan hotspot for broadband wireless internet Access.
  - And many more...

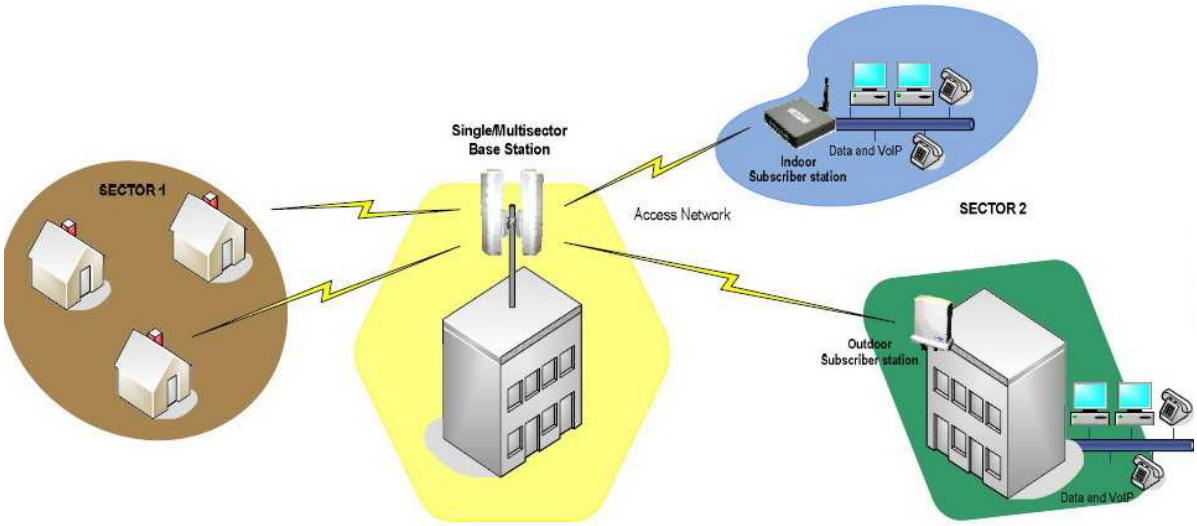


Figure 8 - Application scenarios

- **IEEE 802.16-2009 (WiMAX) standard compliance**

  ARBA-135 is the first *IEEE 802.16-2009* standard-compliant BS operating in the 3.5GHz licensed band, and has proved interoperability with many professional and low cost SSs manufactured by multiple vendors, enabling CAPEX optimization based on the customer's particular needs. This family is based on a *WiMAX Forum Certified™* design to ensure seamless interoperability with all a *WiMAX Forum Certified™* Subscriber Stations.

- **Advanced physical layer control**

  ARBA135 allows controlling the most relevant physical transmission parameters: transmission power, cyclic prefix, frame duration, channel bandwidth… This control may be used to establish the right balance between capacity and several specific performance parameters like latency, sensitivity, achievable link distance, immunity against multipath and Bit Error Rate.

  In addition, adaptive OFDM modulation with **256** subcarriers is used for an optimum performance even in NLOS scenarios characterized by strong multipath propagation. The transmission rate will be automatically adapted depending on the radio link budget, ranging from BPSK to 64QAM modulations.

  Thanks to the use of wide channel bandwidths of up to **7 MHz**, this solution is able to provide an outstanding throughput-coverage performance comparable to expensive licensed band high power base stations. Besides, *Automatic Transmit Power Control* allows for optimal network deployment, tight frequency reuse and interference avoidance.

- **Advanced contention-free MAC layer, obtaining a great spectral efficiency and higher distance coverage**

  The **ARBA135** family applies advanced physical and MAC layer techniques to achieve unprecedented spectral efficiency (higher than 3bps/Hz). This highly efficient use of the spectrum allows more robust modulation schemes with lower Signal-to-Noise ratio requirements, enabling the use of smaller and less expensive antennas. A net Layer-2 capacity of 26Mbps can be achieved using a 7MHz channel with 64QAM-3/4 modulation, with a gross physical layer throughput of approximately 26Mbps. This net capacity is obtained thanks to the use of techniques for deterministic access to the radio resources and the avoidance of statistical access techniques like in most 802.11-based wireless equipment.

  This is achieved by means of a framed transmission protocol where *time slots* are allocated to each connection, so end-to-end QoS parameters (net capacity, latency and jitter) can be guaranteed for each connection even in time-varying wireless physical channels. Throughput and latency are kept constant thanks to the use of this frame-based deterministic MAC layer. The use of a contention-free MAC layer maximizes the net spectral efficiency by avoiding packet collisions and unused idle time.

  This well defined frame structure with continuous use of the spectrum and absence of contention slots is the way **ARBA135** is able to guarantee outstanding Layer-2 net capacity, which can go beyond 90% of the physical layer gross capacity.

- **Advanced functionalities**

  ARBA135 family implements the most advanced functionalities of the *IEEE 802.16-2009* standard, such as ARQ (*Automatic Repeat Request*) mechanism for zero packet-losses, FEC (*Forward Error Correction*), full QoS Support (BE, RTPS, nRTPS, eRTPS, UGS), multiple convergence sublayers, data encryption or differentiated service flows per user. All these functionalities are explained more in detail in 3.16.

- **Single/multiple sector configurations**

The **ARBA135** is designed with a highly scalable architecture in order to meet costumer requirements in different applications, making it a cost-effective solution for wireless deployments. Thanks to the use of the multi-sector configuration, the operator can easily increase the system capacity to support network growth.

A *Single-sector* configuration comprises an outdoor radio unit connected to an indoor power supply injector via a standard Cat5-Ethernet cable which carries data and power. *Multiple-sector* Base Stations can be configured by connecting several outdoor units to a single rack-mount IDU, which synchronizes all sectors in order to cancel TDD inter-sector interferences.

On a multisector configuration every sector must be synchronized someway. Synchronism may be external (i.e. using a GPS signal) or internal, using an extremely accurate high frequency synchronism generator (OCXO). In both cases this synchronism in the IDU will be transmitted to all sectors through the default Ethernet cable, so additional infrastructure it's not required in the installation. It is important to take into account that when using several sectors with synchronism, one sector will function as *Master* and the rest of sectors that will function as *Slave*.

WiMAX in the licensed band uses the TDD mechanism, which is based on differentiating transmission and reception. Due of this, inter-sector interference will be minimal on a synchronized multi-sector configuration, because all sectors transmit or receive at the same time. When a sector is receiving, adjacent sectors are transmitting nothing, so it does not receive any signal that could interfere with its reception.

- **Complete management solutions**

The **ARBA135** family offers a wide range of options for remote management and software upgrade, providing the operator a powerful and intuitive management system based in industry standard protocols.

- Web: a user-friendly interface which allows to fully configure the unit and to control many aspects of the system. The operator will only need a web navigator to access this interface. HTTPS protocol is used for a more secure communication.
- CLI: all the operations that can be performed by the Web Interface are also available in this Command Line Interface. In order to use this interface, it is necessary to establish a SSH (*Secure Shell*) connection towards the IP address of the unit. The encryption used by SSH provides confidentiality and data integrity as it uses public-key cryptography to authenticate the remote computer.
- SNMP: it is supported to manage user status, alarms, and to provide with a general overview of the system, allowing fully integration with networking management systems.
- XML-RPC: *Albentia Systems* offers this innovative open-source protocol which may be used and modified by the final user. It works with files based on the popular XML standard, making the communication with the unit simpler. Communications are as robust and safe as in SSH, because it is transported over an SSL layer similarly to HTTPS. Any customer could develop its own management tool to make the translation of SNMP commands into XML-RPC commands.
- AMS (*Albentia Management Solution*): This more advanced interface provides a comprehensive management solution for equipments and allows working with the last SNMP versions.

- **Advanced networking functionality:**

  ARBA135 is prepared to support many network modes Bridging, Routing, Multicast, NAT, Net-Hooks, Local Network, VLANs, DHCP,... In the following some of the are mentioned

  - Routing mode: this is defined as the classic working mode where units have some routing tables defined and they redirect packets through one interface or another following these previously established rules.
  - Bridging mode: the BS allows performing transparent Layer-2 *Bridging* between different sub-networks. The main advantage is its simplicity an its *Plug-and-Play* feature, since it will not be necessary to add manually any route to the WiMAX units and neither to any other network equipment in the network.
  - IP Multicast: this mode is very interesting for broadcast or multicast transmissions.
  - NAT: the Base Station may also make IP address translations for the Subscriber Stations in the system.

  Much more detailed information about networking possibilities will be found in Paragraph 3.17.

- **Outdoor easy installation and low power consumption**

  ARBA135 is an easy to install and low power consumption solution, perfectly suited for rural WiMAX deployments, supporting solar-based power supply. It uses a very simple architecture characterized by an indoor Power over Ethernet (PoE) supply injector and a weather-proof outdoor enclosure which contains the electronics and radio.

3. WEB MANAGING INTERFACE

ARBA135 includes a powerful web interface, which is probably the simplest way to fully configure the unit and to control many aspects of the system. The customer will only need a web navigator such as *Mozilla Firefox* or *Internet Explorer* to access this interface. HTTPS (port 443) is the default used protocol for a more secure communication. The following paragraphs give more detail about the different sections in this web interface.

3.1. Accessing the Web Interface

To enter the web interface, just open a web browser and make an HTTPS connection using the IP address of the ARBA135 unit. (i.e.: **https//10.11.12.2**). If everything is correct, a login window similar to the one in Figure 10 will be shown, asking for user name and password. There are two possible modes of authenticating:

- **"*INSTALLER*" PROFILE**

  This profile has fewer privileges than the Administrator profile. It is intended to be a reduced version of the complete *web interface*, including status information about the BS and about the connected users, but only for monitoring purposes. The modification of any parameter is not allowed for this profile. The web interface will present just a few subsections, as shown in Figure 9, and it has been specially designed for CPE installers that need to know the radio status when pointing the antenna to the BS.

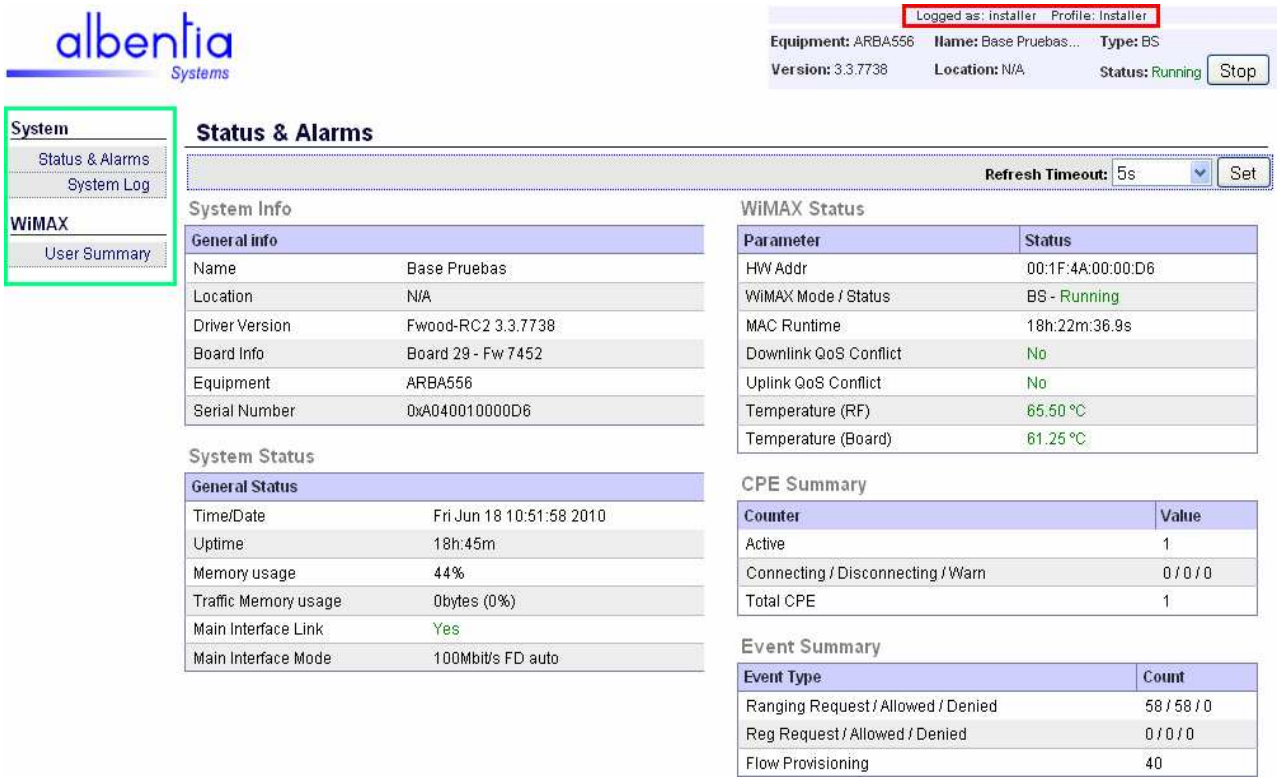


Figure 9 - Web Interface, "*Installer*" profile

The login is performed with the following data:

- User: **installer**
- Password: **wmax**

► **"*WIMAX USER*" PROFILE**

This profile allows the user to operate as Administrator in the web Interface, so all the sections and the configuration options will be enabled. The login is performed with the following data:

- User: **wmax**
- Password: **wmax**

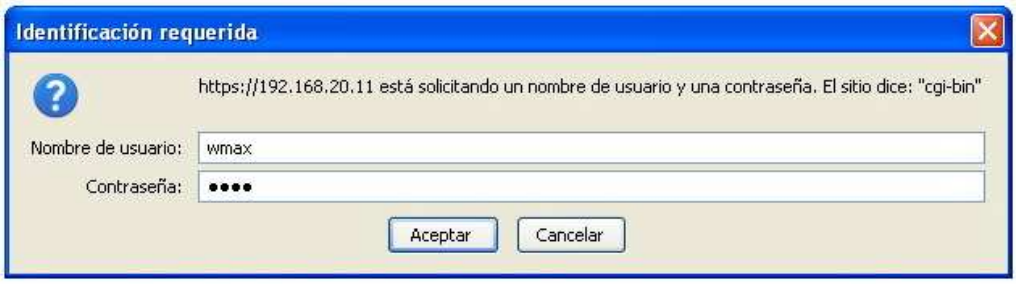


Figure 10 - Login window

NOTE

It has been detected that some web browsers may ask for login and password three times, one for each area of the web interface.

If this information is introduced correctly, the *Status & Alarms* menu of the unit will be shown. From this, all the sections of the web interface may be accessed using the lateral menu.

The web interface is divided in four different areas: a main area in the centre (**Main View**), a selection menu in the left side (**User Menu**), an upper-right information bar (**System Connection**), and a refresh control bar (**Refresh bar**), as shown in Figure 11.

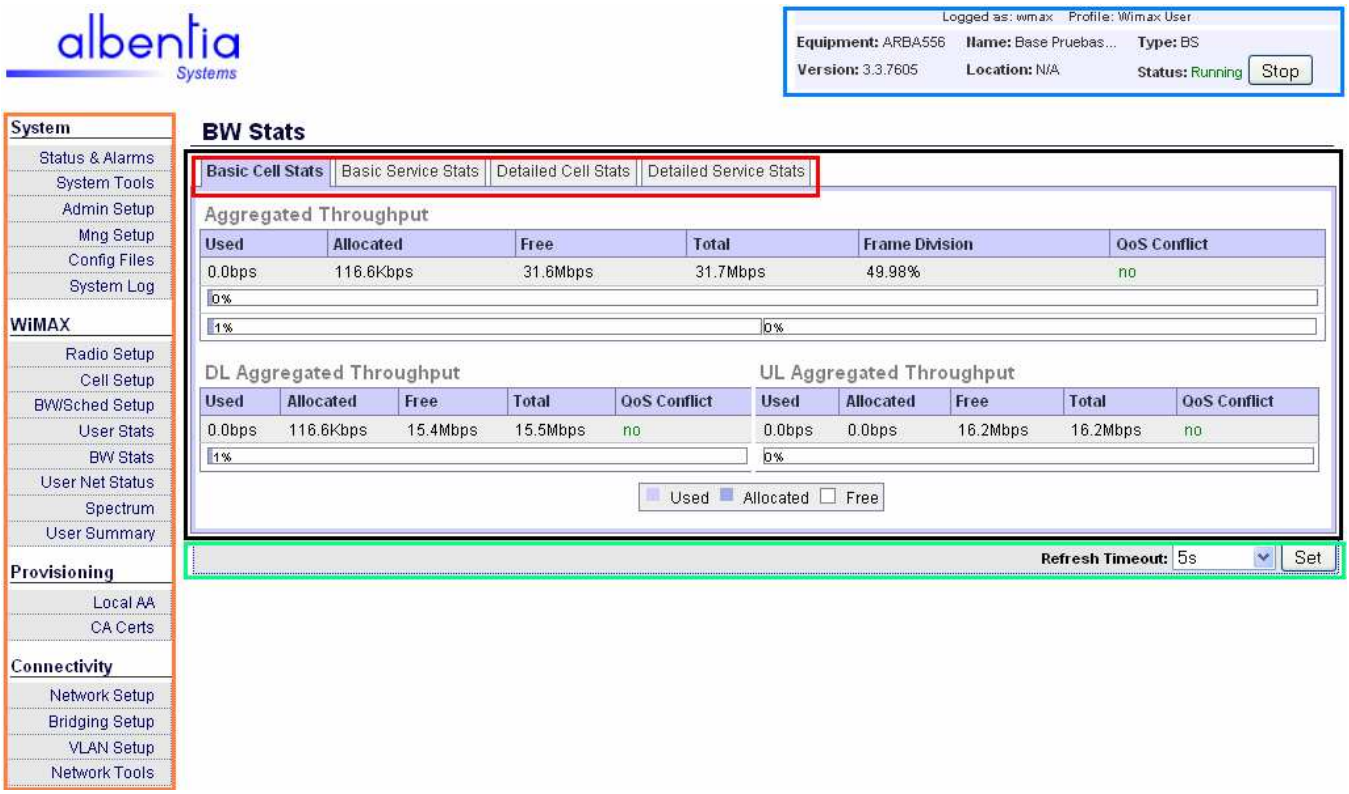


Figure 11 - Structure of the Web interface

3.1.1. Main View

The main area is called the **Main View** (central side, squared in black in Figure 11), and it shows the contents the menu that has been selected from the User Menu Area. Some menus include too much information to be displayed in one unique screen, so these sections will include a **Tabs Area** (squared in red inside the Main View area) to select different sections of the current menu.

3.1.2. User Menu Area

The **User Menu** is located in the left side of the screen (squared in orange in Figure 11), and it offers a list of all the available menus, allowing the user to jump into the different parts of the web interface. This area is divided into different blocks:

- **SYSTEM**: This block refers to the internal information and operation with the BS: status information, log, configuration slots… It contains the following sections: "*Status & Alarms*", "*System Tools*", "*Administration Setup*", "*Management Setup",* "*Configuration Files*", and "*System Log*".
- **WIMAX:** This block refers to all the WiMAX aspects: radio link, cell parameters, traffic statistics… It contains the following sections: "*Radio Setup*", "*Cell Setup*", "*Bandwidth & Scheduler Setup*", "*User Stats*", "*Bandwidth Stats*", "*User Net Stats*", "*Spectrum Analyzer*" and "*User Summary*".
- **PROVISIONING**: This block refers to the BS provisioning database, where the admitted SS units will be defined and the service flows and QoS options will be selected. It contains the sections "*Local AA*" and "*CA Certificates*"

- **CONNECTIVITY**: This block refers to the all networking possibilities: routing, bridging, multicast, DHCP, NAT… It contains the following sections: "*Network Setup*", "*Bridging Setup*", "*VLAN Setup*" and "*Network Tools*".

NOTE

The title of every these four blocks is preceded by a + or – symbol which may be used to contract or expand the contained section labels.

3.1.3. System Connection Area

This area, located in the upper-right side of the screen (squared in blue in Figure 11), provides some status information about the unit, and is shown every time in the web interface (regardless the active menu). The shown parameters are the following:

- **Equipment** it shows unit's commercial name (i.e. ARBA 135).
- **Version**: it shows the software release number of the unit.
- **Name:** it shows the alias of the unit, which may be defined in the "*Admin Setup*" section.
- **Location:** it shows the location of the unit, which may be defined in the "*Admin Setup*" section.
- **Type**: it shows the nature of the unit (BS, SS…).
- **Status**: it shows the status of the WiMAX system (Running, Stopped, Scanning…)
- ***"Stop/Start button***: it stops the unit's WiMAX driver when it is running, and starts it when it is stopped.
- **Profile**: it shows the current user profile that is logged on.

3.1.4. Refresh Timeout Bar

The presented screen of some in the web interface will be automatically refreshed, to show updated information in every precise moment. The default refreshing time is 5 seconds. This time can be configured using the "Refresh Timeout Bar", which will be located in the top or in the bottom of the screen. The sections where the "*Refresh Timeout* Bar" is available are the following: "*Status and Alarms*", "*System Log*", "*User Stats*" and "*BW Stats*". Figure 11 shows this bar in a green-coloured square.

NOTE

All along the website some help "tooltips" may be found. They are represented by the "[?]" symbol, and they will display help information when the mouse pointer is located over them.

3.2. Status & Alarms

This section is the welcoming screen of the unit when the web interface is opened, and shows important information such as the system general status and some alarms. A snapshot is shown in Figure 12.

Figure 12 - *"System Status & Alarms"* menu

The information is divided in five different subsections. In the following every indicator will be explained:

► SYSTEM INFO

- **Name:** it shows the alias of the unit, which may be defined in the "*Admin Setup*" section.
- **Location:** it shows the location of the unit, which may be defined in the "*Admin Setup*" section.
- **Driver version:** it shows the software release of the unit and its associated alias.
- **Board info:** it shows information about the board of the unit and about the current Firmware version.
- **Equipment:** it shows unit's commercial name (i.e. ARBA 135).
- **Serial Number:** it shows the serial number that has been assigned to the unit.

► SYSTEM STATUS

- **Time/Date**: it shows the current time and date. This value may be adjusted in "*Admin Setup*".
- **Uptime:** it shows the time of operation since the unit was powered on.

- **Memory Usage**: it refers to the percentage of internal memory that is currently being used.
- **Traffic Memory usage**: it refers to the percentage of packets that are queued in the internal memory.
- **Main Interface Link**. It shows whether there is connectivity in the Ethernet interface or not.
- **Main Interface Mode**: it shows the current operation mode of the Ethernet interface: speed (10 or 100 Mbps), negotiation (auto or forced), and transmission mode (full/half duplex). This mode can be set in the "*Network Setup*" section. If the "*Main Interface Link*" parameter is set to "*No*", the "*Main Interface Mode*" will show "*BAD Value…*".

► WIMAX STATUS

- **HW Address:** it shows BS's MAC address.
- **WiMAX Mode/Status:** it shows the nature of the unit (BS, SS…) as long as the current status of the WiMAX system (*Running, Stopped…*).
- **MAC Runtime:** it shows the time that the unit has been working until this moment. It is shown in a format *hh:mm:ss*.
- **Downlink QoS Conflict:** it shows if the unit is having any problem on provisioning the configured services, in the downlink. This could happen when the BS is not able to guarantee certain QoS services, for example because there is not enough aggregated throughput for all. When this happens, a counter will appear after the "*Yes*" or "*No*" indication, showing the number of frames with exceeded bandwidth requests.
- **Uplink QoS Conflict:** it shows if the unit is having any problem on provisioning the configured services, in the uplink. When this happens, a counter will appear after the "**Yes**" or "**No**" indication, showing the number of frames with exceeded bandwidth requests.
- **Temperature (RF):** it shows the radiofrequency board temperature, expressed in ºC.
- **Temperature (Board):** it shows the internal temperature of the unit, expressed in ºC. This unit is designed to work properly with up to 75 ºC internal hardware temperature.

► CPE SUMMARY

- **Active**: it shows the number of users that are connected to the BS at this precise moment.
- **Connecting/Disconnecting/Warn**: it shows the number of users that are currently connecting or disconnecting to the BS at this precise moment, as long as those ones in a "*warning*" state, such as users that have failed in the negotiation with the BS or users with bad link conditions which cannot complete all the connection phases.
- **Total CPE**: it shows the total number of users in the systems (*Active, Connecting, Disconnecting and Warning)*. It will be the total amount of the previous fields.

► EVENT SUMMARY

- **Ranging Request/Allowed/Denied**: it represents the total amount of *Ranging Request* (RNG-REQ) messages that the BS has received since the last time it was powered on, as well as how many of them have been successfully accepted and how many have been denied. As it has been commented previously in point 1.2.7, *Initial Ranging* is the process of acquiring the correct timing offset and power aligned in the WiMAX adjustments such as the SS's transmissions are perfectly synchronized.
- **Reg Request/Allowed/Denied**: it represents the total amount of *Registering Reques*t (REG-REQ) messages that the BS has received since the last time it was powered on, as well as how many of them have been successfully accepted and how many have been denied.
- **Flow Provisioning**: it indicates the total amount of service flows that the BS has provisioned to all users since the last time it was powered on.

3.3. System Tools

This section performs five important operations for the unit: (1) updating the internal firmware, (2) changing the system password, (3) rebooting the unit, (4) rebooting the unit after a specified reboot timeout and (5) returning the unit to the factory values. This menu is shown in Figure 13.

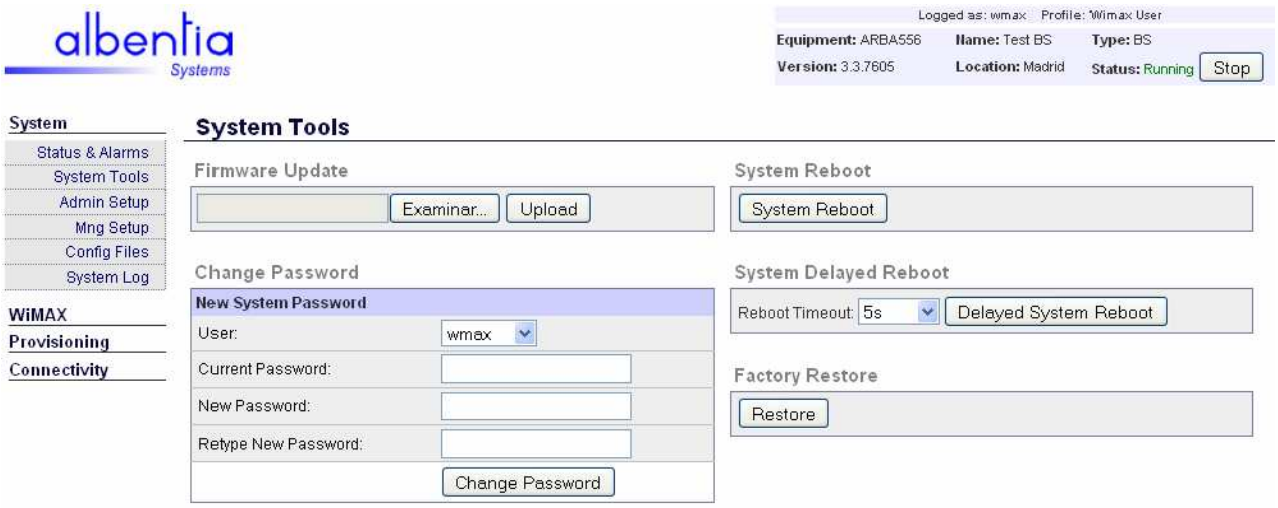


Figure 13 - "*System Tools*" menu

► FIRMWARE UPDATE

When a new unit is manufactured, it is loaded with the most up-to-date software release, but as times goes it is recommended to periodically update the unit since new functionalities are added to the system. Therefore *Albentia Systems* always recommends working with the last version of software, which will offer the best achievable performance.

The updating process is fast and simple, but must be performed carefully, because data is overwritten in memory and this process should not be interrupted. This process consists of uploading a **.bin** file to the unit and letting it be installed. This upgrading file should be provided by *Albentia Systems*.

Firstly, the user must select the **.bin** file and press the "*Upload*" button. Once the file has been uploaded (this operation takes some seconds and shows an animated moving bar), a new screenshot will ask for confirmation to continue or not, as shown in Figure 14. If the process is stopped at this point, the file will be discarded and the SW of the unit will remain unalterable.

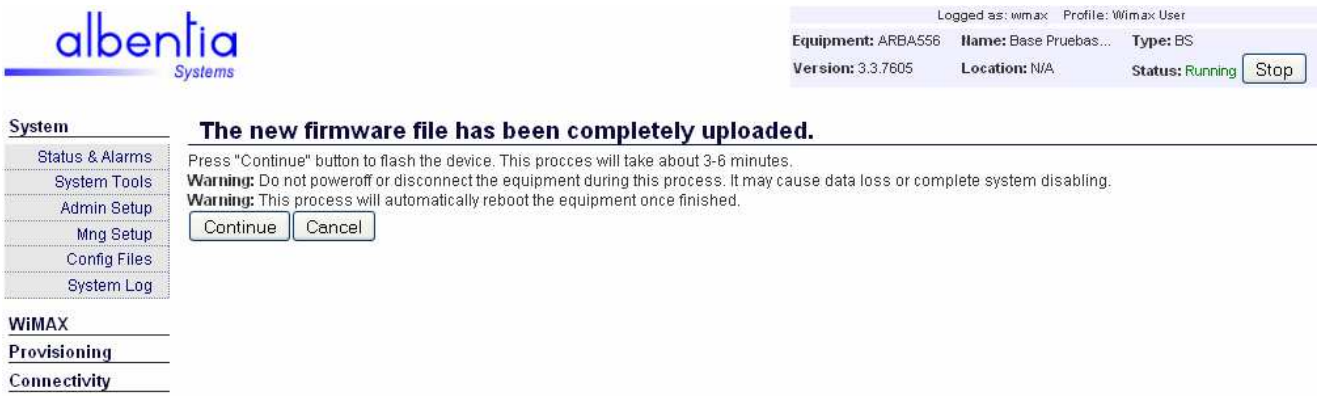


Figure 14 - "*Upgrade confirmation*" screenshot

On the other hand, if "*Continue*" is pressed, the software will be completely installed in the unit. This process takes about 5-7 minutes, and during it some messages will be displayed in this screen informing about the different phases of the upgrade. When the process finishes the unit will be automatically rebooted, and when it comes up again the web interface will show the new version number in the upper-right side of the screen: that means that the updating operation has finished successfully.

⚠ ATENTION!

Updating is a process that must be performed carefully. Make sure the power supply is not interrupted during the upgrade; otherwise the unit could become unusable!

⚠ ATENTION!

If the update is performed from a Firmware version 3.0 or earlier, the automatic reboot that is performed after the upgrade process will not leave the unit fully operational. In this case, an additional manual reboot is required.

NOTE

Every *Albentia Systems*' unit working together should use the same software release.

NOTE

Updating a unit will reboot the unit when finishing. As the configuration files are not modified in this process, the unit will be recovered with the configuration specified in the default XML file. See chapter 3.3 for more information about configuration files.

► PASSWORD MODIFICATION

Changing the password for accessing the web interface is an easy operation: user should go to "*Change Password*" block and type the current password and the desired new one into the appropriate fields. Then press the "*Change Password*" button and the operation would be performed. The new password must be formed by five or more ASCII characters.

SYSTEM REBOOT

This unit may be remotely rebooted by the operator using the web interface. This reboot operation can be considered as a "*hard reboot*" as long as the unit will be switched off and on automatically, so the final result will be the same as rebooting the unit manually in the real location.

To perform a reboot, just click into the "*System Reboot*" button. A message asking for confirmation will be shown. After rebooting, the unit will restart with the configuration stored in the *default* configuration file. Note that changes that have not been saved in this file will be lost.

SYSTEM DELAYED REBOOT

This is another interesting functionality, which allows performing a delayed reboot to the unit. This could be useful, for example, when accessing to the web interface via wireless. In this case, if any configuration parameter is changed wrongly or if the BS is stopped and the wireless link fails, the BS may become unreachable from its wireless interface. To avoid this, a delayed reboot may be programmed. The operator could configure the unit (without saving the changes in the default configuration file), and if something gets wrong, the BS will be rebooted with the previous configuration.

To perform a delayed reboot, first set the time before rebooting the BS, which is selectable from 5 seconds to 10 minutes. Then, click into the "*Delayed System Reboot*" button. A message asking for confirmation will appear, as shown in Figure 15. After rebooting, the unit will restart with the configuration stored in the *default* configuration file. Note that changes that have not been saved in this file will be lost.

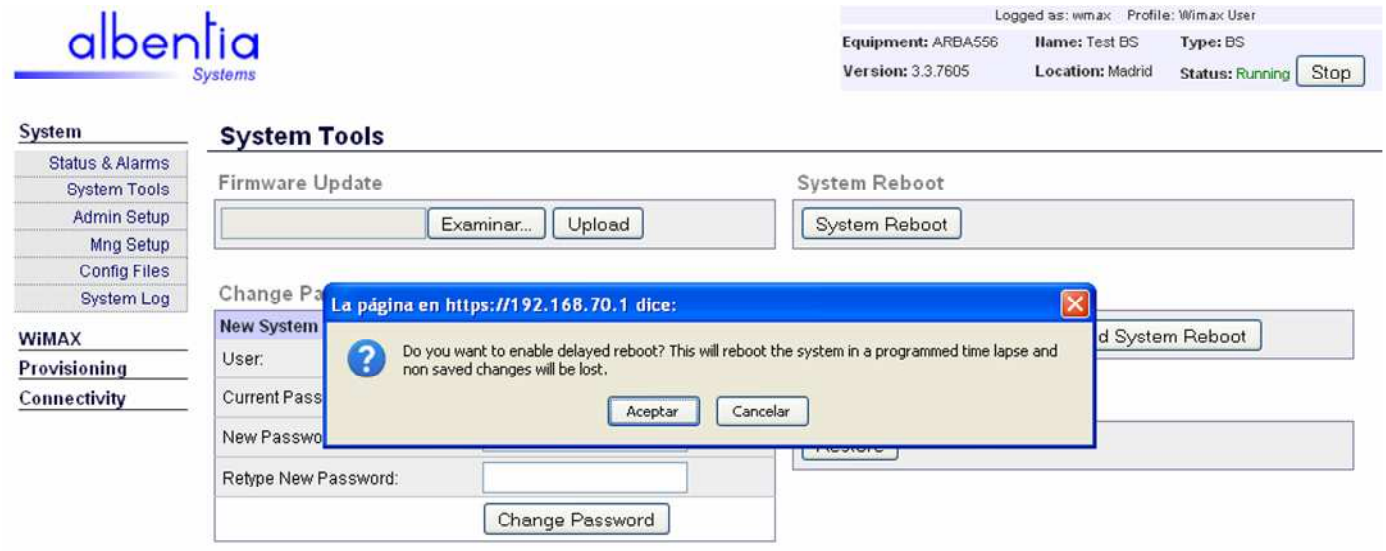


Figure 15 - Delayed Reboot (confirmation)

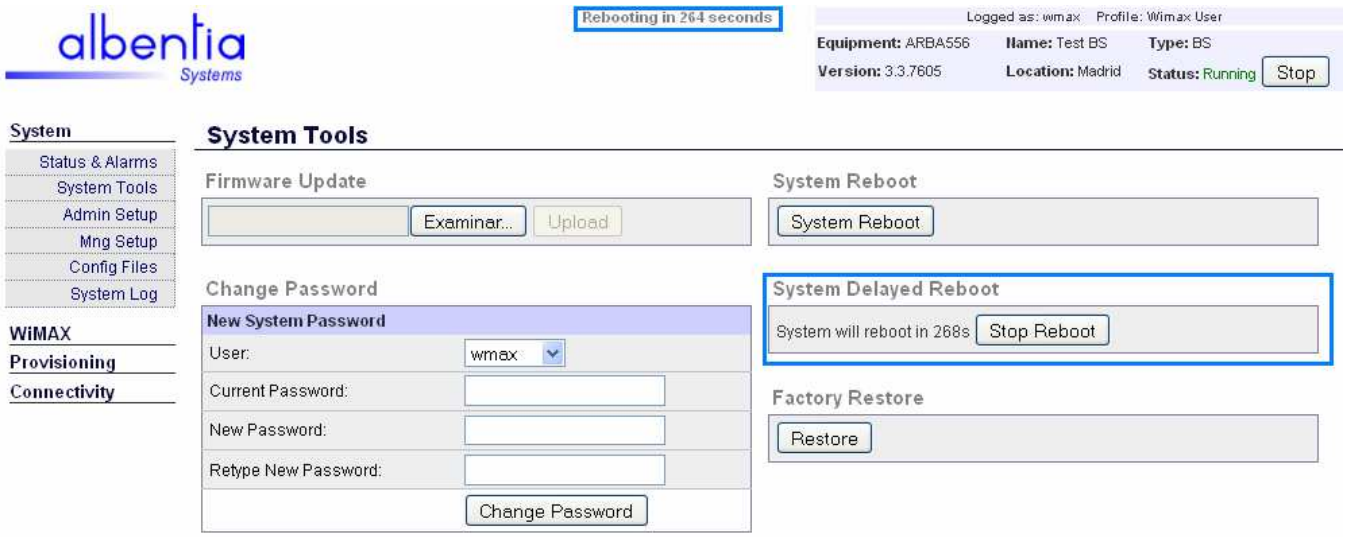


Figure 16 - Delayed Reboot (countdown)

Once the *Delayed Reboot* is applied, the countdown of the remaining time to reboot will be shown in the screen, measured in seconds. Note the countdown will be also shown in the top of the screen while using the web interface. This reboot may be cancelled any time pressing the "*Stop Reboot*" button.

► FACTORY RESTORE

ARBA135 includes the possibility to return the unit to its factory configuration, pressing the "*Restore*" button included in the *Factory Restore* section. This operation will delete all the current state, configuration files, network configuration and provisioning database, so a warning screenshot informing about the consequences will be displayed before performing the reset, as shown in Figure 17. If the user still wants to reset the unit, the "*Restore*" button in this screenshot should be pressed.

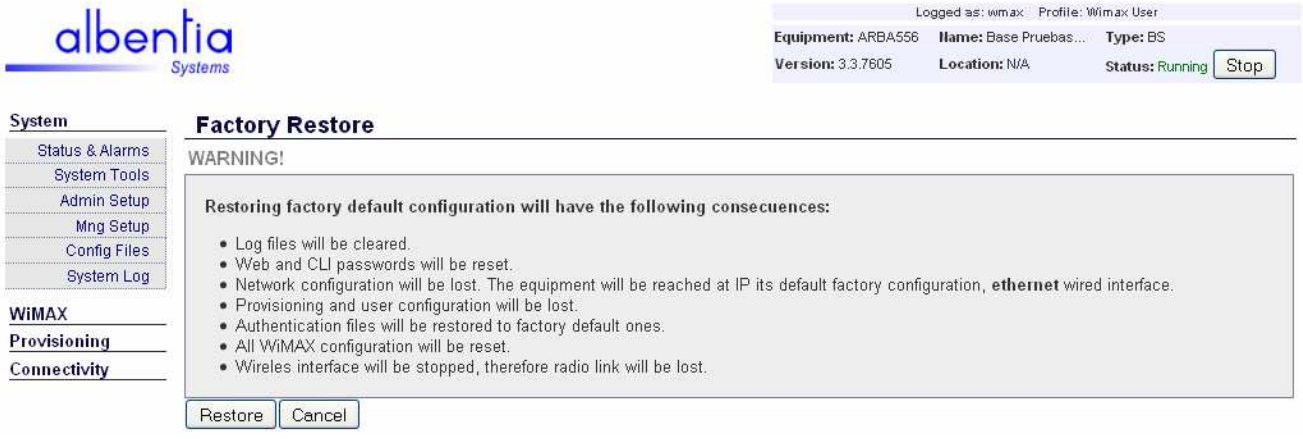


Figure 17 - Factory Restore (confirmation)

3.4. Admin Setup

This section allows to introduce administrative information of the unit and to configure its local time. This screen is shown in Figure 18.

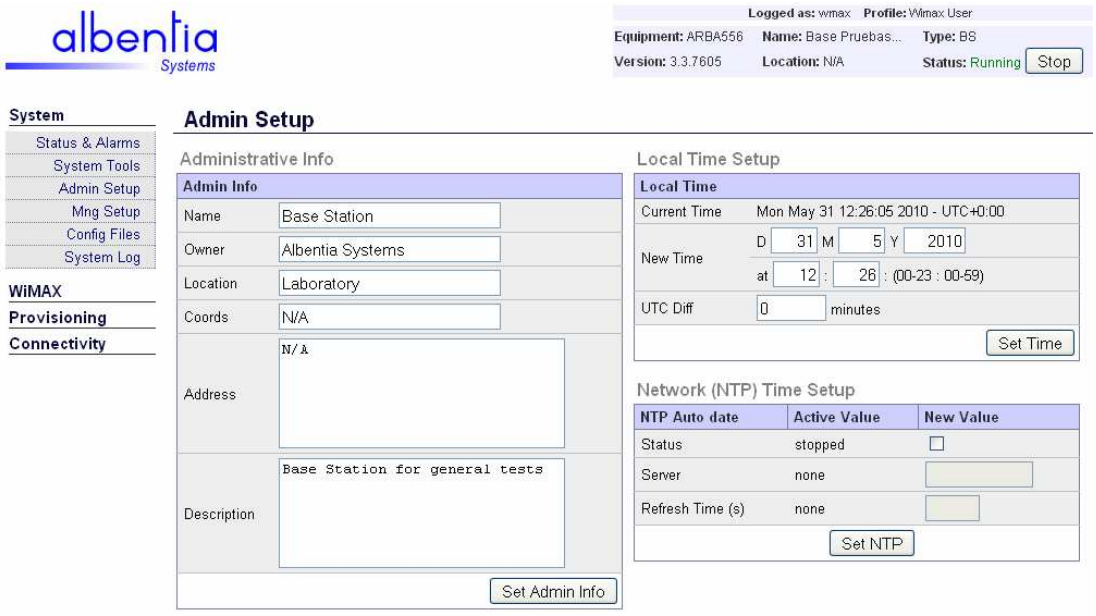


Figure 18 - "*Admin Setup*" menu

► ADMINISTRATIVE INFORMATION

This block allows the operator to specify some administrative information to identify better every unit. The fields are the following: "*Name*", "*Owner*", "*Location*", "*Coordinates*", "*Address*" and "*Description*". Note "*Name*" and "*Location*" fields will be shown every time in the upper side of the screen, in the *System Connection Area*.

► LOCAL TIME

The unit, when is first powered on, starts counting with its internal clock from this date: 01 *January 1970, 00:00:00*. This date may be modified by filling in the appropriate spaces (day, month, year and time-24h) and pressing the *"Set Time"* button. The new date will be updated and all the new information displayed in the "*System Log*" will refer to the new date. ARBA units include RTC (*Real Time Clock*) support, so this time configuration will be maintained although the unit is powered off, due to an internal battery. In addition, the "*UTC Diff*" field allows inserting a time difference respect to the *Universal Time Coordinated*, useful when synchronizing from a foreign time server.

ARBA135 also supports NTP (*Network Time Protocol*), a time synchronization system through the Internet that provides automatic and accurate timing. If the unit can access the Internet, the user may activate de "*Status"* field and introduce one of the many available public NTP servers available, as long as the refresh time in seconds (one example of NTP Public server may be 163.117.131.239, *es.pool.ntp.org*). Then click in the "*Set NTP*" button. The unit will periodically and automatically refresh the current time querying the specified NTP server.

"**Relaxed mode**": when the NTP Client receives the time information from the Server, there is a field in the NTP header of the received packet which indicates if the Server is correctly synchronized or not. When this field, called LI (Leap Indication), is set to 3, it indicates that the Server may not be synchronized, what means that the received time may be wrong.

The *RFC-4330* recommends that the NTP Client should always verify the received time-packet, and if those verifications fail, the time information should be discarded. When the "**Relaxed Mode**" tag is activated, the NTP Client will not perform any verification, enabling the BS to accept time-information form not-synchronized Servers. For more information, please refer to the *RFC-4330* document.

NOTE

In order to use the NTP system, the BS must be able to reach the server IP address. If the NTP server field is filled in with the server host name instead of its IP address, the unit should also have defined one DNS server in the "*Network Setup*" section. Otherwise, the NTP service would not be shown as enabled.

3.5. Management Setup

This section allows to define the management interfaces and to configure the management protocols (SNMP and XML-RPC). It is structured in two tabs, *Interfaces* and *SNMP*, which are explained bellow.

► **REMOTE MANAGEMENT BLOCK**

This block only appears when the BS is being controlled by an XML-RPC based system, such as the AMS (*Albentia Management System*). Together with this section, an information message will appear at the top of the page when the BS is being configured through its XML-RPC interface. This message will display "*Remote Management Mode*".

Changes in the BS can only be made through one management interface at the same time. Before performing a modification in the BS, the XML-RPC system blocks the *Web* interface ability for making changes. The "*Force Local Management*" button allows the user to recover the BS control from the *Web* interface.

3.5.1. "*Interfaces*" tab

This section includes 3 different functionalities: (1) to configure the input management policy, (2) to configure the XML-RPC protocol, and (3) to enable or disable de HTTPS mode. A screenshot of this tab is shown in Figure 19.

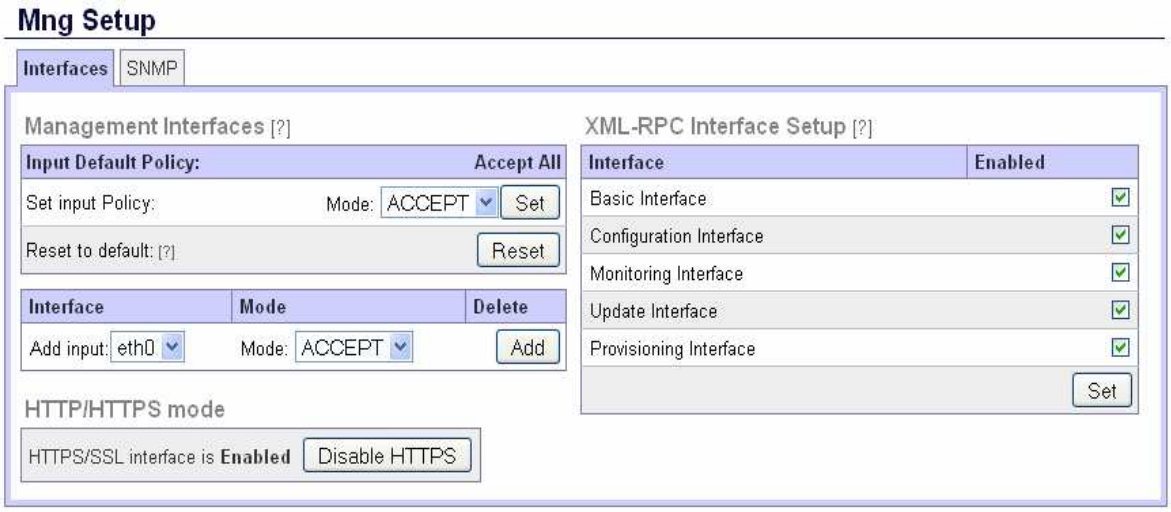


Figure 19 - "*Management Setup*", Interfaces tab

► **MANAGEMENT INTERFACES**

This section allows controlling the input management policy, applied to the **Input Management traffic** (that management traffic whose final destination is the BS). It may be applied to all the existing interfaces in the unit: *eth0*, *wethx wireless interfaces*, "*lanx*" *bridges* or *VLANs*.

All the Input Traffic may be treated with an **ACCEPT** or **DROP** policy. When ACCEPT is selected in one interface, Input Traffic coming from this interface will be allowed, and when DROP is selected, Input Traffic from that interface will be discarded. A DROP policy will only be selectable one there is art list one interface with an ACCEPT policy, in order to always keep the unit reachable.

Section is divided into two blocks: the first one defines the Default Input Policy that will be applied to all interfaces. The units start working with the "ACCEPT ALL" default filtering policy, but the operator could change it to the "DROP ALL" mode. On the other hand, the second block is able to create individual input policy rules to the defined interfaces. That means that the BS will apply the Default Policy to all interfaces except to that ones with defined specific input policies. An individual policy takes precedence to the default policy.

As the https connection to the web interface of the BS is a type of Input Traffic, this functionality may be used for example to avoid the CPEs entering the BS configuration page, or to limit the access to the BS to hosts belonging to a specific VLAN, for example.

NOTE

Setting "DROP" mode as the input policy must be performed carefully, as the unit could remain unreachable from the selected interface.

- **HTTP/HTTPS MODE**

  This button allows selecting the protocol used to access the BS through *Web* interface. On the one hand HTTPS is securer than HTTP. On the other hand HTTPS uses more resources, so it could be interesting changing into HTTP when having a very slow remote connectivity to the BS, for example. By default the unit will use HTTPS protocol in order to assure a secure communication, but this section allows the user to change to the HTTP protocol.

- **XML-RPC INTERFACE CONTROL**

  This section gives the opportunity to select the interfaces that will be controlled using XML-RPC protocol.

3.5.2. "*SNMP*" tab

As shown in Figure 20, a SNMP Interface control can be enabled. ARBA135 unit supports the SNMP protocol on versions 1, 2 and 3. This block allows setting all the parameters related to SNMP.

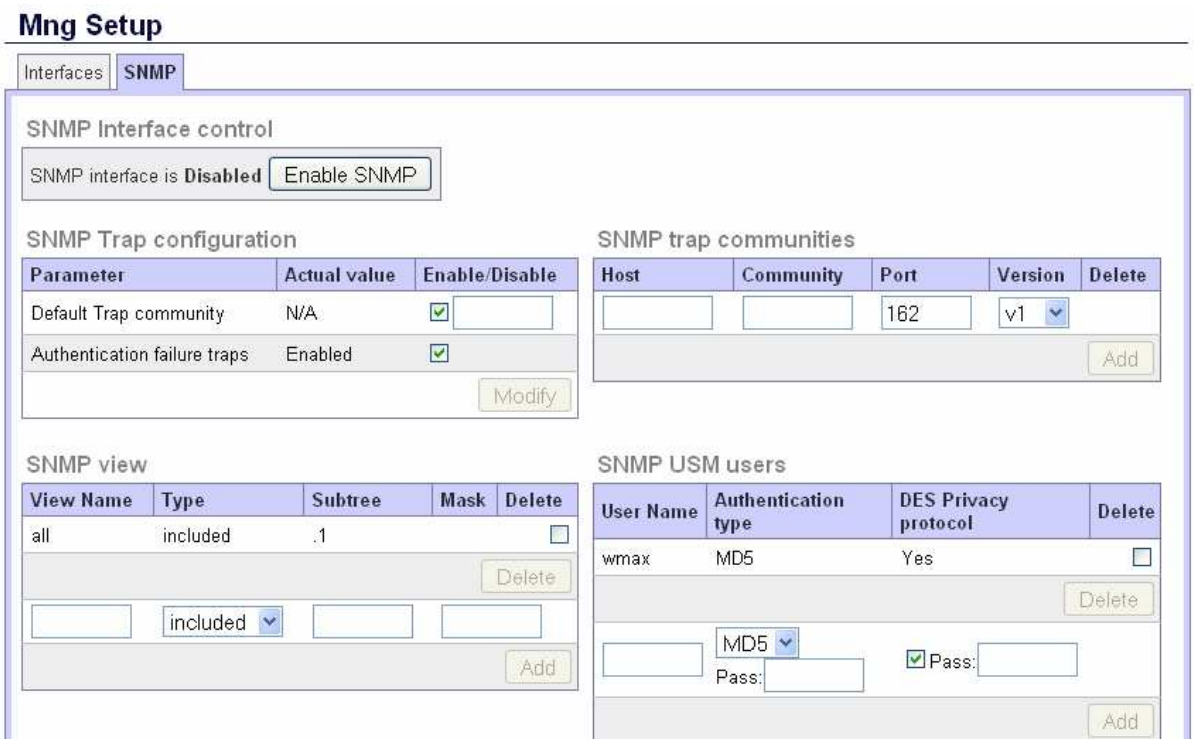


Figure 20 - "*Management Setup*", SNMP tab

The 3rd version of SNMP protocol introduced a whole slew of new security related features that have been missing from the previous versions. In SNMPv1 and SNMPv2c, a simple community string was put in clear text into the packet to authenticate the request, which is highly insecure.

SNMPv3 introduces advanced security which splits the authentication and the authorization into two pieces:

- The USM is the default Security Module. The U stands for *User-based*, as it is contains a list of users and their attributes. The USM is described by *RFC 2574*.
- The VACM is the *View-based Access Control Module* and controls which users (and SNMPv1/v2c communities as well) are allowed to access and how they can access sections of the MIB tree. The VACM is described by *RFC 2575*.

Default configuration includes a community called "**public**" for SNMP v1 and v2. The user and password defined for SNMP v3 are "**wmax**" and "**wmaxsnmp**" respectively.

SNMP settings are stored into an XML configuration file which will be explained later. After configuring SNMP parameters it is important to save the whole configuration in order to avoid losing changes. It is also required to disable and enable SNMP by click on the "*Disable/Enable SNMP*" button in order to apply the modifications.

3.6. Configuration Files

The current configuration of the unit can be saved in XML format files. When selecting the "*Configuration Files"* menu in the left-side of the screen, ten XML files are listed as shown in Figure 21. The user may save up to 10 different configurations into these slots, which will be stored in the internal memory of the unit. If the slot is used, it will be dark coloured, and if it is empty the name of the file will be shown in bright grey.

The first file in the list, called "**default.xml**", will be the default configuration file of the unit. This means that when the unit is powered on the configuration saved in this file will be automatically loaded. Due to this, it is highly recommended to keep saved in this file the desired configuration of the unit, so the unit could recover properly from a punctual power fail, for example.

Remember that when any parameter of the unit is changed, this change takes effect immediately but it is not saved into any configuration file. The user should take care of saving the configuration manually when a configuration change has been made.

XML is a very versatile format which can keep the configuration options perfectly structured. The user may easily view and understand these files, and even create his ones. The system offers the possibility to download these files, modify them or upload user-made ones.

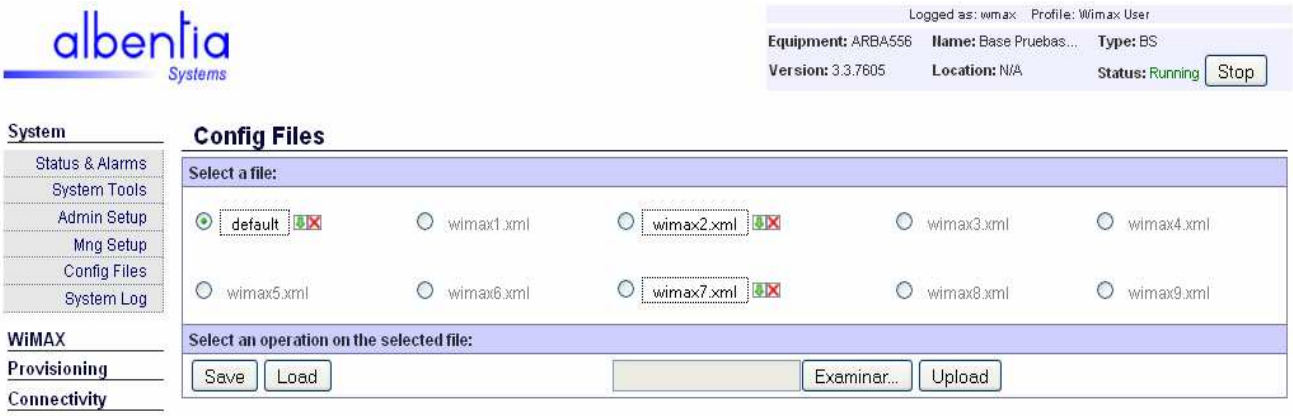


Figure 21 - "*Configuration Files"* menu

Operating with these configuration files is very simple:

- **Saving**: to save the current configuration into a configuration slot, just select the destination file and press the "*Save*" button.
- **Loading**: to load a stored configuration, just select the desired source file and press the "*Load*" button.
- **Clearing a slot**: to delete the configuration of an XML file, simply select it and press the "*Delete*" button or the "*Delete*" icon .
- **Downloading**: when pushing the "*Download*" button, or the "*Download*" icon , the selected file will be downloaded into the computer. This allows storing many different configurations into other storage units. The stored files can also be modified with a simple text editor, for example, and can be uploaded again to the unit with the new modified configuration. The Downloading process can be viewed in Figure 22.

- **Uploading**. It is also possible to upload a configuration XML file into the unit: just click into the "*Browse*" button, select the desired file, and press the "*Upload*" button. The system will check first if the XML file is grammatically correct, and if so the new configuration may be applied or saved. This sequence is shown in the following screenshots.

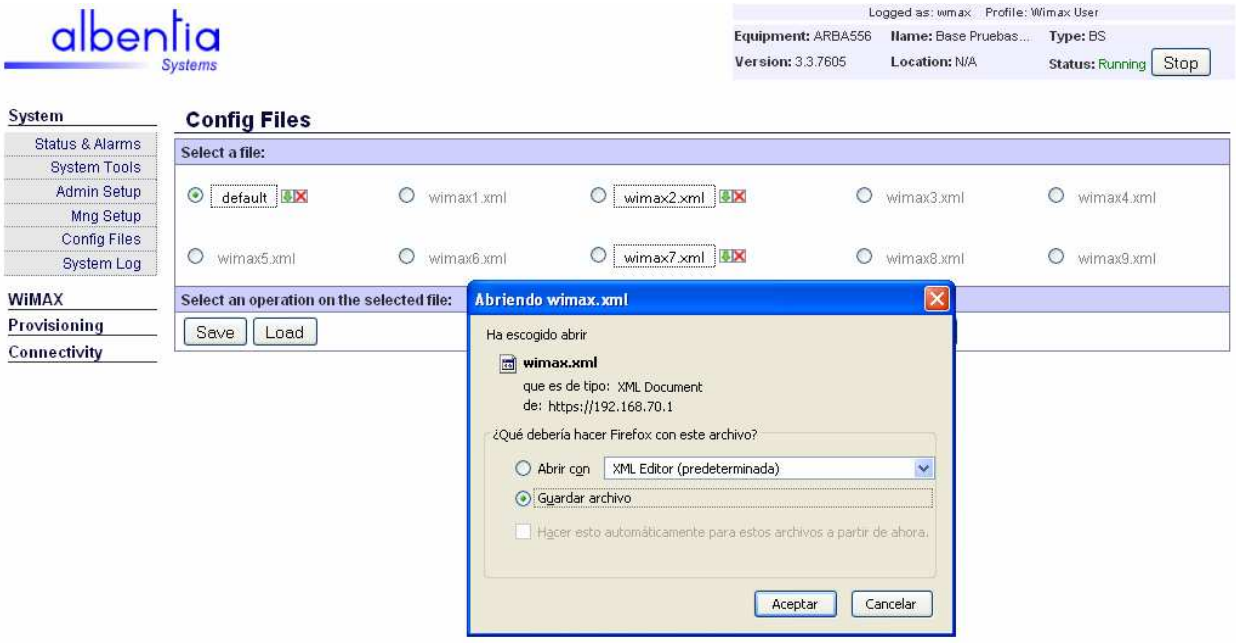


Figure 22 - Opening or saving a file

Figure 23 - Sample XML configuration file

3.7. System Log

The System Log is a powerful tool to visualize every action the BS is performing in order to keep stored the BS operation sequence, which could be helpful if the unit suffers any problem or simply to have a detailed historic file about what happens inside the BS. The unit always saves this log into a .**log** file, so in case of malfunction the customer may examine this file and try to detect the problem.

Every relevant operation in the BS will be represented as a line of this log, describing the type of the event and the time when happened (referred to the *Local Time Setup* explained in point 3.4). In case the event is related to a SS, the MAC address of the SS will also be showed. There are many different operations that will be shown in the log, such as: *MAC stop/start*, *Initial Ranging operation*, *Negotiating*, *Authenticating*, *Registering*, *Flows added*... Some relevant messages will be explained in the following.

The log is automatically filled and refreshed periodically, as specified in its "*Refresh Timeout*" control bar. However, if the log gets too long only the most recent entries will be shown, as long as the original and complete **.log** file keeps stored in the unit even if it is powered off. The most recent entries will be added in the first lines of the log, as shown in Figure 24.

The "*Clear Log*" icon cleans the screen in the web interface, although the complete log will remain unalterable in the unit. The "*Download Log*" icon allows downloading the complete log in a **wimax.log** called file, which can be opened with a standard text editor, for example.

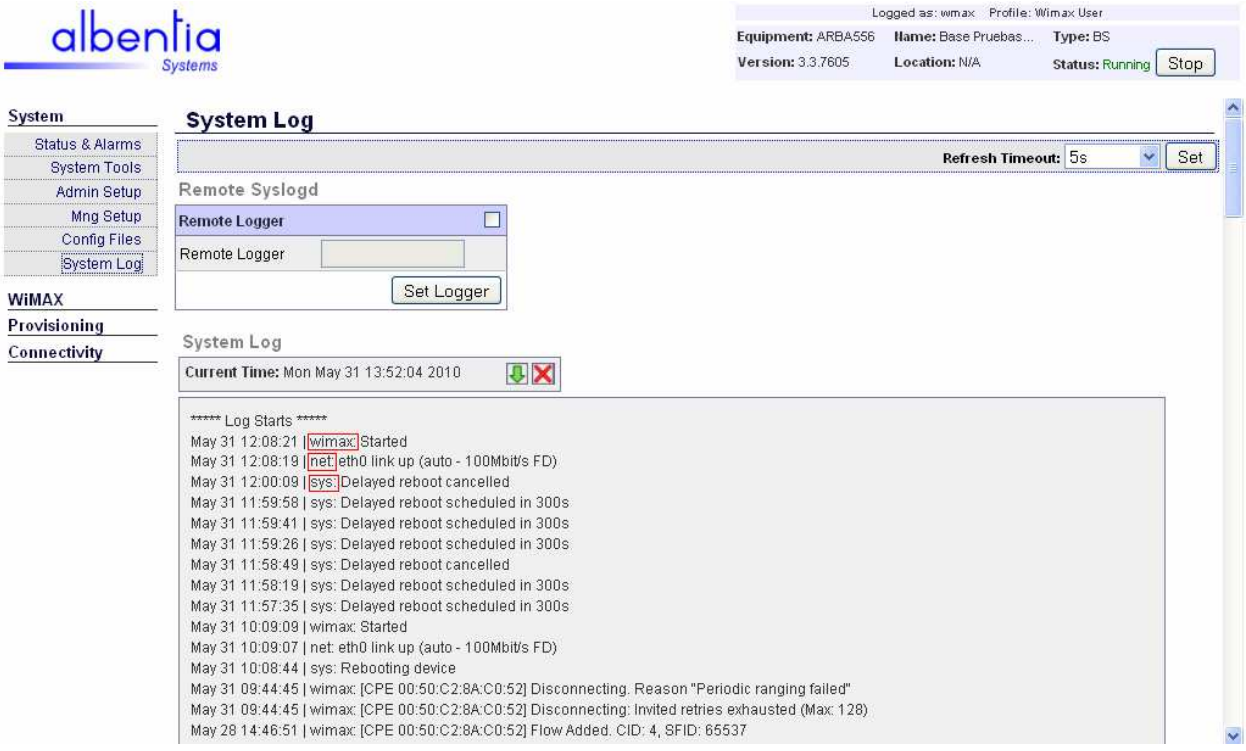


Figure 24 - "*System Log*" menu

► REMOTE SYSLOGD

Syslog is a Client-Server protocol that is used for forwarding log messages in an IP network. This BS includes a Syslog Client which will send the generated log

messages to a Syslog server (for example, "*syslogd"* in Linux or "*Kiwi Syslog Server*" in *Microsoft Windows™*).

The Client is simply configured setting the IP address of the destination Syslog server in the "*Remote Syslogd*" block. The BS will send automatically and periodically the new log messages to the specified destination Syslog server.

► LOG MESSAGES

There are three types of log events: "***wimax***", "***system***", and "***network***" messages. The type of every message will be included in the message, just after the timestamp, as it is shown red-squared in Figure 24.

"W*imax*" messages show information about *WiMAX* transactions and will be usually related to a certain CPE (the MAC will be shown in the message). "*System*" messages show general and status information about the BS, and "network" messages show information about the networking in the BS. In the following some of the most common log-messages that may appear in the log of the BS will be listed.

A) WiMAX MESSAGES

- **SS initialization and Network entry**: when a new SS is detected by the BS, the network entry and initialization process that is defined in WiMAX starts: *Authentication*, *Registration*… if all the phases are successful, the SS becomes *Active*, the provisioned flows are added and the networking is configured. The sequence that will appear in the log looks like this:

  Initial Ranging, starting cell entry process
  ACTIVE, RSSI: -59dBm, CINR: 26dB, Managed: No, Auth: MAC Addr
  2 provisioned flows
  Net config: Bridged dev weth1 in bridge lan0
  Flow Added. CID: 6, SFID: 262144
  Flow Added. CID: 8, SFID: 262145

  If this sequence is not finished completely, the log will show in a message which phase has failed. For example, when the registering timeout has been exceeded the message will be:

  Disconnecting. Reason "Registration timeout"

  When the authenticating process has failed the messages will be:

  Initial Ranging, starting cell entry process
  Initial ranging MAC unauthorized

  When the user is active, the BS will try to create the provisioned flows, using DSA (*Dynamic Service Addition*) WiMAX messages. If certain number of DSA retries (configurable in *Cell Setup* menu) is exceeded without getting any response from the SS, there are two possibilities, according to the *LocalAA* configuration; if the "*Disc on DSA Fail*" field is not active, the SS will remain active but some of the provisioned flows will not be added. On the other side, if the "*Disc on DSA Fail*" field is active, the SS will be dropped from the BS instead of being added without service flows. After being dropped, the following log messages will be shown. After dropping the SS, the BS will start again the registering process.

Flow Added. CID: 15, SFID: 65536
Flow Failed. CID: 16, SFID: 65537
Disconnecting. Reason "DSA Transactions failed and required to disconnect"

- **Disconnecting causes**: an active SS may be dropped from the BS for different reasons. One possible cause of dropping a user may be when the maximum allowed signal correction retries sent by the BS to the SS is exceeded. The BS sets a desired "*Uplink RSSI*" value with the "*Target RSSI*" parameter, and continuously corrects the transmitted power of the SS to achieve this value. The BS has a maximum/minimum allowed RSSI error, selectable in the "*Cell Setup*" menu, to maintain a user connected to the cell. If this dB margin is exceeded after certain number of corrections, the user will be dropped from the cell. The log message will be the following:

  Initial Ranging, starting cell entry process
  InitRng Correction retries exhausted (Max: 16 -Time err: 0 smpl - RSSI Err: 11dB)
  Disconnecting. Reason "Init ranging failed"

  After completion of ranging, the SS informs the BS of its basic capabilities. Another possible cause of dropping a user may be that time slot reserved for that negotiation is over.

  Disconnecting. Reason "Capabilities negotiation timeout"

  Another possible cause of dropping a user may be that the BS is not receiving any response from it, commonly due to bad radio signal levels. If the BS offers a time slot to the SS and it does not get any response, the SS will be dropped after a certain number of opportunities.

  Disconnecting: Invited retries exhausted (Max: 128)"
  Disconnecting. Reason "Periodic ranging failed"

  During the Authentication process, if the "*RSA Auth Required*" mode is enabled, the CPE must support this option, otherwise next message will appear:

  Disconnecting. Reason "Authentication required but CPE does not support it"

  After the "*Disconnecting*" alert and the reason explanation, the SS dropping process will continue deleting the associated network interfaces. When all the process is finished, the SS will be shown as "*Disconnected*". The following messages show the elimination of the network interfaces for a SS in Local Network mode:

  Removing Local Network for device weth82: Public IP:188.119.197.137, Private IP: 192.168.101.100 Bridge: lan99
  Removing hook for device weth82 from hidden ip 192.168.101.151 to private ip 192.168.101.100

- **Local Network**: the following log messages represent the typical transactions for a SS using Local Network mode with DHCP and a Net-Hook.

  DHCPDISCOVER dev "weth0" via "lan0"
  DHCPOFFER on 188.119.197.84/23 received for weth0
  Net config: Local Network dev weth0: Public IP: 188.119.197.84, Private IP: 192.168.101.128 Bridge: lan99

Setting hook for device weth0 from hidden ip 192.168.101.151 to public ip 192.168.101.128

- **Other messages**

a) When a certain user is provisioned with more flows than the *maximum-flow-number-per-user* parameter of the BS, the BS will not create the exceeding flows, and the log will show this:
Error creating Flow. Max Num Flows Rx reached

b) There is also a log message when exceeded the maximum allowed number of active users :
Aborting initial ranging, max total users exceeded

c) During the SS initialization and Network entry process, when in AUTO mode, if a SS is assigned to a bridge without IP direction, a warning message will appear. It is necessary to configure the lan0 with an IP direction.
Warning: Private IP not configured for weth0 in AUTO mode. Please, check bridge ID 1 configuration

d) Stopping and starting the radio:
Stopped
Started

e) Spectrum Analyzer operation:
Spectrum Analyzer mode enabled
Spectrum Analyzer mode disabled

f) DFS operation:
Starting DFS
DFS finished. Selected frequency 5525 MHz

B) SYSTEM

These messages show status information about the BS after performing some operations.

- **Software Update:**
Updating system software versions. From "Fwood- EngSmpl" 3.3.7605 To "Fwood-EngSmpl" 3.3.7611
System software updated
Rebooting device

- **Reboot:**
System Reboot

- **Delayed Reboot:**
Delayed reboot cancelled
Delayed reboot scheduled in 300s

- **Syslogd configuration:**
syslog running (remote logger: 192.168.70.11)

- **Syslogd configuration:**
syslog running (remote logger: 192.168.70.11)

- **System time configuration:**

Setting new time – 17/06/2010 – 16:15 – TZ: 0

C) NETWORK

These messages give information about the physical interfaces, such as the status, the mode (Auto/Manual), and the speed:

eth0 no link
eth0 is down
eth0 is auto - 100Mbit/s FD
eth0 link up (auto - 100Mbit/s FD)

3.8. Radio Parameters

This section allows to view and to modify the unit's radio configuration. A snapshot of this menu is shown in Figure 25. This is a very important section, because in order to establish a WiMAX communication the first thing that should be done is to configure properly the physical part of the link, which can be done in this section.

In the tables, every parameter is shown with the active selected value. In the right side the "*New Value*" column can be found, which allows modifying the active value of every parameter, just by selecting the new value and clicking the "*Modify*" button. This button is able to modify several parameters at the same time.

The "*Radio parameters*" section can help to optimize the performance of the link, since some parameters have a direct impact into the communication's maximum throughput, minimum latency/jitter, or robustness against multipath, for example. This will be explained thoroughly in the next paragraphs.

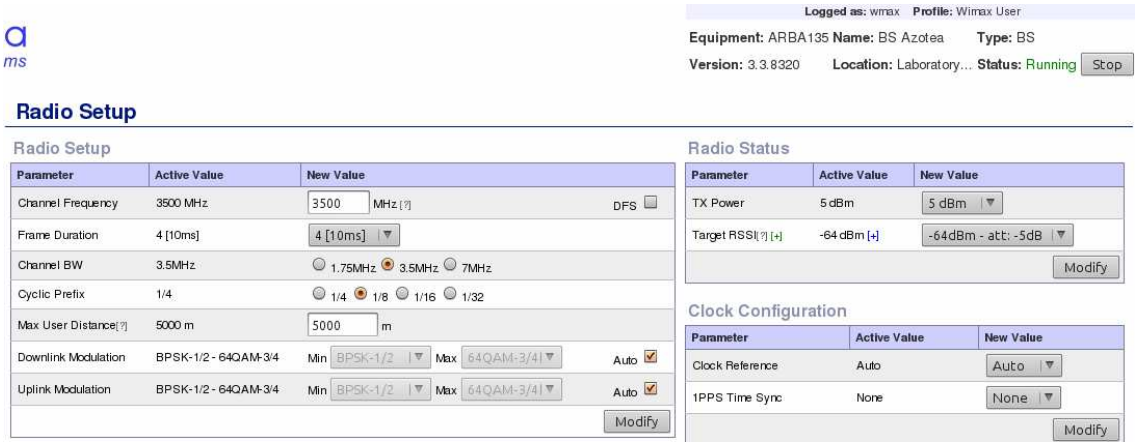


Figure 25 - "*Radio Setup*" menu

3.8.1. Parameter list

ARBA135 allows controlling the most relevant physical transmission to establish the right balance between capacity and several specific performance parameters like latency, sensitivity, achievable link distance, immunity against multipath and Bit Error Rate. The physical parameters are listed below, with some configuration recommendations:

Parameter	Description
Channel Frequency	It is the operation frequency, expressed in MHz. *Albentia Systems*' ARBA family is designed to work in 3400-3600MHz **Important note:** frequencies are selectable for allowing the enhancement of the usable radio range, but the user should notice that these frequencies will suffer some degradation (up to 6dB) due to the nature of the radio filters. In this row there is a **DFS** checkbox, which enables the *Dynamic Frequency Selection* functionality. This checkbox activates a new table, which will be explained later. Selection: **Every frequency** in the valid range, in steps of **1MHZ**
Frame	It refers to the WiMAX frame's duration, expressed in milliseconds.

Duration	This parameter is strongly related with system's latency, and also with the overall throughput. Short frames help reducing the round-trip latency of the system, and larger ones optimize the overall throughput of the system, due to the shorter overhead. Selection: **2.5**, **5**, **10** and **20 msg.**
Channel Bandwidth	It refers to the channel width, expressed in MHz. This parameter can be used to control the throughput and sensibility in the system. Overall net throughput (at Ethernet level) is near 3bps/Hz. Using a large bandwidth maximizes the capacity, whereas a narrower one optimizes the sensibility and so increases the link budget. Selection: **3.5**, **7 MHz.**
Cyclic Prefix	The OFDM cyclic prefix is expressed as a fraction of the current frame duration, and represents the guard time slot allocated before the data frame in order to be able to receive delayed symbols, for example those proceeding from the reflected rays (multipath). Thus, this is a useful parameter that controls the immunity against multipath: a short cyclic prefix maximizes the link capacity as it reduces the guard time, and a larger cyclic prefix increases robustness against multipath propagation. (NOTE: symbol durations are 32 and 64 microseconds for 7MHz and 3.5MHz bandwidth, respectively). Selection: **1/4, 1/8, 1/16 y 1/32** of the OFDM symbol time.
Maximum User Distance	This parameter specifies the maximum link range measured in metres. Be careful with this parameter because it has different meaning in a BS or in a SS. In the BS this parameter represents the distance in which the farthest SS may be located. It is highly recommended that this parameter is set to a value slightly higher than the real maximum distance in order to have a certain margin. However, this margin should not be too wide because this distance is directly related to the time spent by the BS while listening to new SSs (*Ranging mode*), so if "Max. User Distance" is too high that will mean many time waited for inexistent users, therefore decreasing spectral efficiency and total net capacity. Selection: **Any** (consequent with the real scenario).
DL/UL Modulation	*Albentia Systems'* equipment supports different modulations, from the more robust ones to the ones that provide a higher *throughput*. Using the "*DL/UL Modulation*" fields it is possible to limit the minimum and the maximum codifications that can be used in both UL and DL. The available modulations are the following ones: BPSK ½, QPSK ½, QPSK ¾, 16QAM ½, 16QAM ¾, 64QAM 2/3 and 64QAM ¾. First ones offer more robustness and can reach longer distances, while last ones can provide higher *throughput* if the link conditions are optimum. Although modulation may be limited between a lowest and a highest scheme, the modulation used at each time will be automatically selected by the BS depending on the available SNR at that moment. There are also two "*Auto*" labelled checkboxes, which may be activated if no modulation limitation is intended. (NOTE: Each provisioned user may also restrict its own modulation, but this condition will be less restrictive than the "*DL/UL Codification"* parameter). Selection: minimum and maximum modulation (**7 different schemes**).
Tx Power	This parameter selects the transmission power at the output of the radio stage of

	the device and is measured in dBm. It refers to the transmission power that the unit leaves at the N connector. The BS works with a fixed Transmission Power for communicating with all CPE units. In real deployments, *Albentia Systems* usually recommends to set this parameter on a fixed **+20dBm** value. It is the maximum selectable transmission power with no distortion, so all the modulations would be available and long distances would be covered. Selection: between **-20 dBm** and +2**0dBm** (in steps of 1 dBm). **IMPORTANT NOTE**: There are national organizations that may legally limit the EIRP (*Equivalent Isotropically Radiated Power*) of the unit. In Spain, for instance this is controlled by the CNAF (*Cuadro Nacional de Atribución de Frecuencias*), which sets the following maximum EIRP levels: When configuring the *Transmission Power* in the ARBA station, the user should take care about the EIRP limitations established by the competent organization. *In order to calculate the EIRP of the unit it will be necessary to sum up the current antenna gain to this parameter.*
Target RSSI	This parameter specifies the expected received signal (RSSI) at the BS from every connected CPE, so it indirectly controls the transmission power of the CPEs. If a fixed *Target RSSI* is requested for all the connected CPEs, the farther ones will be requested to transmit higher power levels than the closer ones, so everyone is received at the BS with similar RSSI. This parameter may change slightly from one BS to another, and it is related to another parameter: "*Rx Attenuation*" (in dB). In most cases it is not necessary to modify this parameter (RX Attenuation = 0 dB). However, in some scenarios it may be necessary to adjust this parameter in order to adapt the equipment to the channel conditions. When decreasing the *Target RSSI* (negative attenuations), the BS will demand less power. This could be an option when the current "*Target RSSI*" is not achievable (CPEs transmitting at their highest Transmission Power which are not able to achieve the fixed "*Target RSSI*" at the BS, for instance). This adjustment is typically made when there are CPEs far enough from the BS. On the other hand, it may be necessary to increase the *Target RSSI* (positive attenuations) in situations where higher RSSI levels can be reached (scenarios with very low attenuation, CPEs very close to the BS, antennas with high gain,…). In these situations, a low Target RSSI may not be achievable. Setting this parameter to 10dB, for example, increases in 10dB the desired reception RSSI level at BS antenna connector, thus allowing those very near SSs to get in. Be careful because if this reception attenuation is too high, far-away users could be left out of the cell coverage. **[+] Indicator**: *Target RSSI Range* In the "*Active Value*" column, there is a **[+]** tooltip which shows the current "*Target RSSI Range*". This range is calculated from the current "*Target RSSI*" value and the "*RSSI maintenance error*" value, which is configured in the **Cell Setup** section. CPEs with received RSSI levels out of this range will be dropped from the cell. **[+] Indicator**: *RSSI Range Error* In the "*Parameter*" column, there is a **[+]** tooltip which shows if the current "*Target RSSI*" value is not in the optimal RSSI range. ▪ *Warning State*: The symbol is shown in orange (**[+]**) when the averaged received RSSI differs slightly (3-6 dB) from the selected "*Target RSSI*" value. ▪ *ERROR State*: The symbol is shown in orange (**[+]**) when the averaged

	received RSSI differs from the selected "*Target RSSI*" value more than 6 dB. Selection: Target RSSI values for a RX attenuation between **-20 dB** and **35dB** (in 1 dB steps).

Table 3 - Radio parameters

NOTE

If any physical parameter is modified, it is strongly recommended to save the configuration to avoid losing this configuration. In order to do this, the menu *Configuration Files* allows saving the current state of the equipment (parameters, users, flows...) in a XML configuration file that can be restored later. (This is explained in section 3.3).

NOTE

Some modifications may require stopping and starting the system to make effect. When this happens, the system will show a notification page asking for confirmation. By pressing *Accept* the system will continue with the modification. The WiMAX module will restart in a process that takes 2 or 3 seconds approximately. So if some service is being provided to final users, the impact of this short unavailability should be taken into account.

DYNAMIC FREQUENCY SELECTION (DFS)

When DFS is activated, the BS will scan the spectrum and will choose the cleanest working frequency, selecting the channel **with the minimum received RSSI**. Every time the radio of the BS is started, the DFS will perform a new same spectrum analysis, and will move to the best scanned frequency.

This functionality is activated checking the "**DFS**" checkbox located in the "*Channel Frequency Parameter*" in the Radio Setup Table. When the checkbox is activated, a new table will appear in the bottom of the page, as shown in Figure 26.

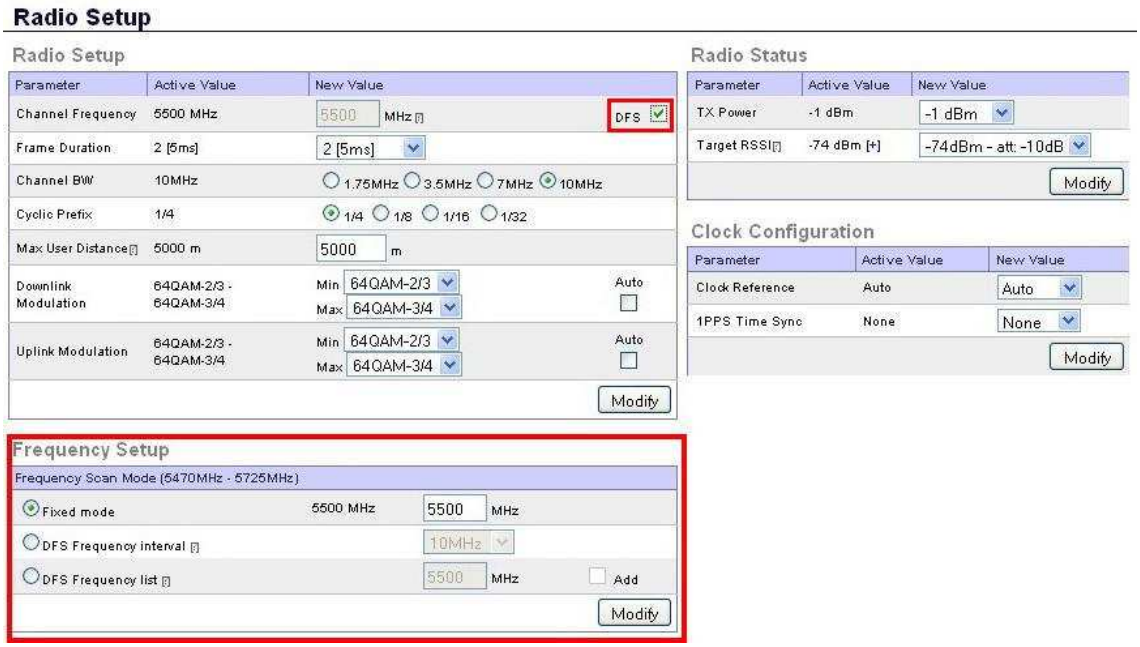


Figure 26 - DFS section

DFS includes three operating modes:

- **Fixed Mode**: this mode sets the BS to a fixed frequency, so the BS will not jump to another channel. When this option is selected, the DFS functionality is disabled and the DFS table will disappear.
- **DFS Frequency Interval**: when this option is activated, the unit will work in DFS mode, scanning the entire band with the selected stepping (from 1 MHz to 10 MHz). The scanning will take longer with a smaller stepping, so this issue must be taken into consideration.
- **DFS Frequency List:** when this option is activated, the unit will work in DFS mode, scanning only in the selected frequencies. These frequencies are added by the user one by one, filling in the frequency field (in MHZ), enabling the "*Add*" tag, and pressing the "Modify" button. This option is considered more reliable than the previous one, as the DFS will only change into some known frequencies. Figure 27 shows the DFS table after the analysis performed in five different frequencies. The table shows the RSSI obtained in each one as long as the selected frequency.

Figure 27 - DFS (measured results)

DFS performs a Spectrum Analysis for detecting the best frequency, and the results of the scan are displayed live in the "*Spectrum*" section (see paragraph 3.14 for more details about this menu). When DFS is scanning, the Status indicator in the top-right side of the page will show ***"DFS [Scanning]"*** in orange (see Figure 28).

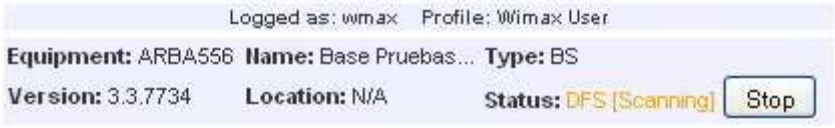


Figure 28 - DFS (Scanning)

⚠ ATENTION!

Using DFS implies that the BS may change the channel unexpectedly every time the radio is started. Therefore, it is necessary that the connected CPEs are configured to be able to change to the new frequency, so they do not get unreachable.

⚠ ATENTION!

While DFS is scanning the active users will disconnect from the cell until the analysis finishes. Therefore, the faster the analysis is performed, the faster the CPEs will re-connect to the cell.

► CLOCK CONFIGURATION

This section is useful when the BS works in a multi-sector configuration (many BS units operating in the same location). With this architecture, it is strongly recommended to synchronize all the units for the best radio performance.

TDD mechanism to transmit is based on separating transmission and reception in *time slots*. Due to this, inter-sector interference will be minimal on a synchronized multi-sector configuration, because all sectors transmit and receive at the same time. When a sector is receiving, adjacent sectors are transmitting nothing (are

receiving, too), so units do not receive signal from adjacent units that could interfere with their reception.

In the standard configuration (one sector), the BS auto generates its own clock, while in a multisector configuration, all the BSs will get the same clock signal (also known as the synchronism signal) from an Indoor Unit, which will generate the signal and will transfer it to all the units using the not-used pairs of the Ethernet cables (so additional cabling is not needed).

This section includes two parameters:

- **Clock Reference**: two different values may be selected:
  - **Auto**: the BS will auto-generate its own clock signal. This is the configuration mode for monosector architectures.
  - **Ext. Ref.**: in multisector architectures where the clock signal is obtained from an external Indoor Unit, this value must be set.
- **1PPS Time Sync**: three different values may be selected:
  - **None**: this is de default value for monosector configurations.
  - **Slave**: this is the default value for multisector configurations.
  - **Master**: there is an additional multi-sector scenario, where one of the units acts as the synchronism-generator, and the rest of the units get this signal from it. In this case, the BS which generates and transmits the signal to the rest of the units must be configured as *Master*.

3.8.2. Adjusting the link balance

For a good communication between BS and SSs, it is necessary to balance correctly the link, and for this, it is mandatory to understand how WiMAX performs the power control. As it has been explained previously, all the network intelligence in WiMAX is assigned to the BS, and this also applies to the radio link control. As explained before, the BS controls and selects a lot of communication aspects: modulation, frame duration, channel bandwidth… and so does it happen with these power parameters, which should be adjusted manually by the operator.

The radio parameters that mainly refer to the link balance are the "*Transmission Power*" and the "*Target RSSI*". With the *first one*, the BS sets the transmitted signal level, and with the second one, the BS sets the signal level that it expects to receive from all SSs.

Regarding SSs, they usually perform AGC (*Automatic Gain Control*). The main goal of this technique is to be able to transmit with the power that the BS asks for, which implies a reduction of the power consumption and the interferences between SSs.

In conclusion, the transmission and reception signal levels of the BS will be adjusted manually in the "*Radio Setup*" menu, as long as in the SSs these levels will be automatically adjusted following the orders received from the BS. When a SS is powered on, it begins to perform a power scanning: it increases power slowly and cyclically until it is detected by a BS. When the BS notices that there is a SS performing this scan, it indicates to this unit the optimum transmission power that should use in order to establish a correct communication.

The "*User Stats*" menu offers a complete overview of the link state towards every active SS, showing valuable link status information such as **CINR** or **RSSI**. This menu gives a good idea about the power balance both in UL and DL, allowing adjusting the BS's radio parameters to their optimum values for the current scenario. The main goal of the operator should be to configure these parameters in the BS so the UL and DL CINR values are maximized. This will allow to use the higher modulations and

consequently to obtain higher throughputs.

NOTE

The radio configuration system of SSs is managed in different ways depending on the SS vendor. Thus, some SSs are able to autodetect some radio parameters such as the cyclic prefix or even channel frequency, whereas in others these parameters should be adjusted manually to match up with the BS's configuration. So be sure that SSs are properly configured to operate with the BS

Regarding the RSSI, a high value means that the received signal level is high, so in general this should be traduced to a good CINR measure. However, if there is noise and interference in the operating channel, with a high value of RSSI a poor CINR measurement may be obtained. In this case, it is recommended to look for other operation radio channel to try to reduce the noise that is affecting the communication.

The following points should also be attended:

- In the Downlink (BS-->SS), when modifying the *Transmission Power* in the BS, the *RSSI* in the SS units will vary.
- In the Uplink (SS --> BS), when modifying the *Target RSSI* in the BS, the *Transmission Power* in the SS will be automatically adjusted.
- This phase of the configuration depends mainly on the environment's conditions: distance between units, antenna gains, alignment, interferences, climatic conditions… so it is impossible to establish some default values which could adapt to every scenario. The customer should adapt these radio parameters to its particular situation.
- The distance between BS and SSs has a lot of influence in this configuration phase, and it is a very important data to configure the power parameters correctly. Thus, for long distances is usually convenient to set a higher transmission power and lower reception attenuation in the BS. On the other hand, for short distances it is usually convenient to set a lower transmission power and higher reception attenuation.
- If the BS and a SS are too close to each other and directly pointed, the reception could be saturated even at minimal BS transmission power. In this case, it is recommended to move slightly the SS so the alignment gets worse and the received signal is lower, avoiding the saturation.
- In the case that the power balancing and adjustment is not successful, it is important to identify on what sense is failing (UL or DL).

More information and tips about the radio parameters may be found in Table 3, and the complete explanation about the "*User Stats*" menu may be found in section 3.11.

3.8.3. WiMAX Physical Layer

ARBA135 implements advanced physical layer control mechanisms to perform the use of the wireless medium. Below some useful information will be displayed.

IEEE 802.16-2009 physical layer uses adaptive OFDM modulation with **256** subcarriers, where only 200 will be used (192 for data and 8 for control). Subcarriers are separated 45 kHz from each other. Each carrier will be modulated in BPSK, QPSK, 16QAM or 64QAM using an adaptive modulation. Higher modulations will be able to transmit more info, as displayed in Table 4.

Modulation	Information bits/ carrier	Information subcarriers	Information bits/ OFDM_symbol
BPSK-1/2	**0.5**	**192**	96
QPSK-1/2	**1**	**192**	192
QPSK-3/4	**1.5**	**192**	288
16QAM-1/2	**2**	**192**	384
16QAM-3/4	**3**	**192**	576
64QAM-2/3	**4**	**192**	768
64QAM-3/4	**4.5**	**192**	864

Table 4 - Modulation schemes

Symbol durations (T_S) are 32, 64 and 128 microseconds for 7MHz, 3.5MHz and 1.75MHz of bandwidth, respectively, plus a guard time slot called "*Cyclic Prefix*" (T_{CP}) which will be allocated before in the data frame in order to be able to receive delayed symbols. This time will be expressed as a fraction of the current symbol time. Therefore, the complete duration of the symbol (T_T) will be expressed as $\mathbf{T_T = T_S + T_{CP}}$, and will vary with the duration of the cyclic prefix, as shown in Table 5.

Channel BW (MHz)	Ts (ms)	Ts + Tcp [1/4] (ms)	Ts + Tcp [1/8] (ms)	Ts + Tcp [1/16] (ms)	Ts + Tcp [1/32] (ms)
3.5	**64**	80	72	68	66
7	**32**	40	36	34	33

Table 5 - Symbol durations

With the complete symbol duration (T_T) and the information bits for each modulation, the achievable physical rates can be easily calculated for each Cyclic Prefix (CP). All the information is shown in Table 6, Table 7, Table 8 and Table 9.

Modulation	Information bits/ OFDM symbol	3,5 MHz (Mbps)	7 MHz (Mbps)
BPSK-1/2	96	1,2	2,4
QPSK-1/2	192	2,4	4,8
QPSK-3/4	288	3,6	7,2
16QAM-1/2	384	4,8	9,6
16QAM-3/4	576	7,2	14,4
64QAM-2/3	768	9,6	19,2
64QAM-3/4	864	10,8	21,6

Table 6 - Maximum physical rates (CP=1/4)

Modulation	Information bits/ OFDM symbol	3,5 MHz (Mbps)	7 MHz (Mbps)
BPSK-1/2	96	1,33	2,67
QPSK-1/2	192	2,67	5,33
QPSK-3/4	288	4	8
16QAM-1/2	384	5,33	10,67
16QAM-3/4	576	8	16
64QAM-2/3	768	10,67	21,33
64QAM-3/4	864	12	24

Table 7 - Maximum physical rates (CP=1/8)

Modulation	Information bits/ OFDM symbol	3,5 MHz (Mbps)	7 MHz (Mbps)
BPSK-1/2	96	1,41	2,82
QPSK-1/2	192	2,82	5,65
QPSK-3/4	288	4,24	8,47
16QAM-1/2	384	5,65	11,29
16QAM-3/4	576	8,47	16,94
64QAM-2/3	768	11,29	22,59
64QAM-3/4	864	12,71	25,41

Table 8 - Maximum physical rates (CP=1/16)

Modulation	Information bits/ OFDM symbol	3,5 MHz (Mbps)	7 MHz (Mbps)
BPSK-1/2	96	1,45	2,91
QPSK-1/2	192	2,91	5,82
QPSK-3/4	288	4,36	8,73
16QAM-1/2	384	5,82	11,64
16QAM-3/4	576	8,73	17,45
64QAM-2/3	768	11,64	23,27
64QAM-3/4	864	13,09	26,18

Table 9 - Maximum physical rates (CP=1/32)

The receiver sensitivity is also an interesting parameter when calculating the system link budget. Higher modulations will require a better SNR for being correctly demodulated, so the sensitivity will depend on the current modulation and bandwidth. Table 10 is filled with the sensitivity values for 3 and 7 MHz.

Modulation	SNR (dB)	Sensitivity for 3.5 MHz (dBm)	Sensitivity for 7 MHz (dBm)
BPSK-1/2	3	-95	-92
QPSK-1/2	6	-93	-90
QPSK-3/4	9	-89.5	-86.5
16QAM-1/2	12	-86.5	-83.5
16QAM-3/4	15	-83	-80
64QAM-2/3	18	-79	-75
64QAM-3/4	21	-77	-74

Table 10 - Receiver Sensitivity

Albentia Systems' equipment supports different modulations, from the more robust ones to the ones that provide a higher throughput. The available modulations are the following ones: BPSK ½, QPSK ½, QPSK ¾, 16QAM ½, 16QAM ¾, 64QAM 2/3 and 64QAM ¾. First ones offer more robustness and can reach longer distances, while last ones can provide higher throughput if the link conditions are optimum.

Although modulation may be limited between a lowest and a highest scheme, generally the modulation used at each time will be automatically selected by the BS depending on the available SNR at that moment.

3.9. Cell Setup

In this section the WiMAX cell parameters may be observed and modified within the allowed limits in each case. The coverage area of a BS may be considered as a **cell**, so these parameters will be applied to all CPES located in this area.

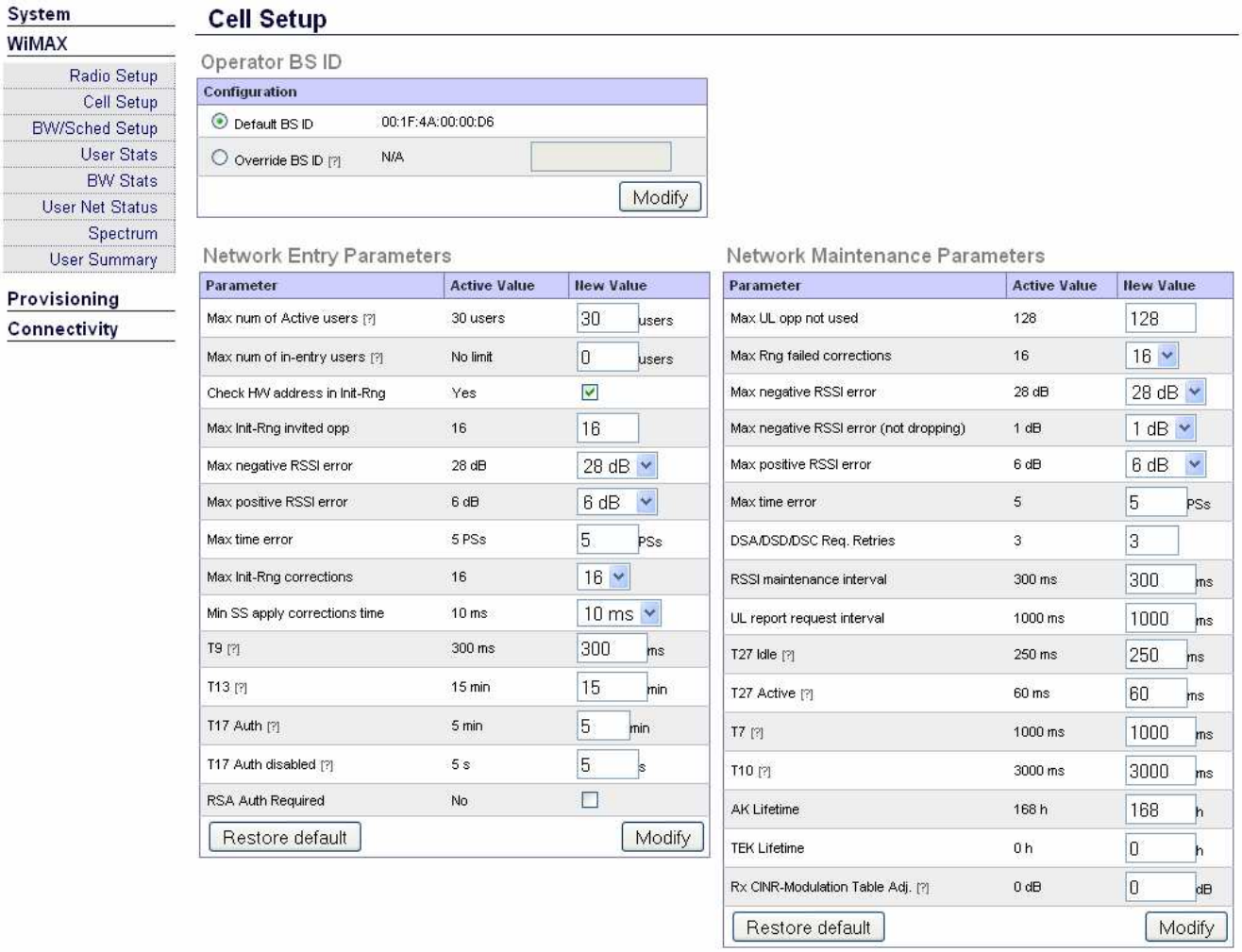


Figure 29 - "*Cell Setup*" menu

A capture of this section can be observed in Figure 29. This section includes very technical and precise parameters which are specified and completely described in the *IEEE 802.16-2009* standard. The default values are supposed to be the most suitable ones for many scenarios, so the general recommendation is to keep these default settings if the modification is not strictly necessary or if the user is not familiarized with these terms, because a wrong modification could make the cell operate worse (there are two "*Restore Default*" buttons to return to the original configuration). However, in some specific cases it might be necessary to make little modifications for a better performance. In the following these parameters are going to be explained briefly. A more detailed view can be obtained in the IEEE 802.16-2009 standard.

- **OPERATOR BS ID**

This block allows changing the Base Station Identifier (Hardware Address). By default, the BS will broadcast its real MAC Address (the one showed in the "*Default BS ID*" field) to all CPEs in the cell. It is possible to change the MAC address that the BS broadcasts to its cell by selecting the *"Override BS ID"* option and filling in the field with a new "*Virtual MAC Address*". This may be useful in an scenario where the CPEs are forced to connect always to the same BS. If this BS is replaced by a new one (which will have a different MAC address), it is possible to configure this one so it broadcasts the MAC address of the previous one, and therefore CPEs do not have to be configured individually to connect to the new MAC address.

NOTE

This section changes the MAC address that the BS broadcasts to the CPEs, although the BS will keep its real MAC address. Only the information messages sent to the CPEs change, but the real MAC keeps unmodified.

► NETWORK ENTRY PARAMETERS

The network entrance parameters are listed and explained below in Table 11, with some configuration recommendations.

Parameter	Description
Max num of Active users	It specifies the maximum amount of active SS units that the BS is allowed to accept in the cell. Selection: the minimum and maximum values of this field may vary depending on the particular features of the BS. "0" value will establish no limit.
Max. number of in-entry users	The "*in-entry*" phase is situated between the "*Initial ranging*" phase and just before activating the user. A non-authorized user will always be located in this state, trying to enter the network. With this parameter the overall number of users in this "*in-entry*" phase may be limited. Selection: at user's choice. "0" value will establish no limit.
Check HW address in Init-Rng	When this field is activated, the BS will only give access to the network to those SS units whose MAC address is specified in the provisioning database. This condition will be checked during the *Initial Ranging* phase, and those units that are not allowed will be dropped. The "*System Log*" will show the MAC address of these unauthorized stations, if any. On the other hand, it this field is not activated, all the SS units in the operation range of the BS will be added to the cell: the ones that are provisioned in the provisioning data base will be registered with the correspondent service flows, descriptors and network configuration, and long as the ones that have not been provisioned will be added to the network with no service flows or network configuration, so they will be seen in the "*User Stats*" section but the will not be able to transmit/receive data with the BS.
Max. Init-Rng invited opportunities	The total amount of slots that the BS will assign to perform *Initial Ranging*.
Max. negative RSSI error	When a user tries to enter the network, the BS makes power corrections to take the user into a working RSSI range. This parameter sets the minimum value of this range.
Max. positive RSSI	Analogue to the previous parameter, it sets the maximum RSSI value

error	into the working range.
Max time error	In relation with the previous two parameters, this field sets the maximum number of Physical Slots that will be let until the user is inside the allowed RSSI range.
Max Initial-Ranging corrections	It sets the maximum number of power and synchronism corrections that will be made with every user in the *Initial Ranging* phase.
Min. SS apply corrections time	It is related with the SSs and their adjustment speed. When the BS sends a correction to a SS, it will let the user a minimum time until it considers that the SS has been able to apply the correction. This parameter fixes this wait time.
T9	Registration Timeout: Time allowed between the BS sending a RNG-RSP (success) to an SS, and receiving a SBC-REQ from that same SS.
T13	Maximum time allowed for an SS to send a TFTP message to the BS.
T17 Auth	Maximum time allowed for a SS to complete "*CPE Register, Authorization and Key Exchange*" in its network entrance procedure.
T17 Auth Disabled	CPE register timeout when RSA Authentication is not enabled.
RSA Authentication required	When this field is activated, the "*SS Authorization and Key Exchange*" will be performed (go to Figure 4), using **X.509 digital certificates**, which is a public-key certificate that binds the SS's identifying information to its RSA public key in a verifiable manner. The X.509 certificate is digitally signed by the SS's manufacturer, and that signature can be verified by a BS that knows the manufacturer's public key. The manufacturer's public key is placed in an X.509 certification authority (CA) certificate, which in turn is signed by a higher-level CA.

Table 11 - Network Entry Parameters

- **NETWORK MAINTENANCE PARAMETERS**

The network maintenance parameters are listed and explained below in Table 12, with some configuration recommendations.

Parameter	Description
Max. UL opportunities not used	When a BS gives *Time Slots* to a SS, these opportunities should be used or not. If the SS does not respond and does not use a certain amount of opportunities, the BS will drop it from the network. This parameter sets this number of maximum opportunities.
Max. Rng failed corrections	It has the same meaning that the analogue parameter for Network Entrance; this one applies to a user that is already inside the network. It sets the maximum number of power and synchronism corrections that will be made with every user in the *Ranging* phase.
Max. negative/positive RSSI error (dropping)	These parameters specify the maximum difference from the ideal Rx RSSI level at the BS. If a SS has RSSI with a range that exceeds these parameters, the BS will try to correct using ranging procedures and if the number of retries defined in "*Max. Rng failed corrections*" also expires the SS will be dropped with cause "*Periodic Ranging Failed*".
Max. negative RSSI error (not dropping)	If this range is exceeded, the user will not be dropped; the BS will try to adjust the RSSI levels.
Max. time error	It has the same meaning that the analogue parameter in the *Network Entrance*.

DSA/DSD/DSC Request retries	It defines the number of times that the BS will try to create a service if the user does not respond. If this number of retries is exceeded, the user will remain in the network but no service flows will be provisioned.
RSSI maintenance interval	It defines the periodic time where the BS will send power corrections to a user that is on a non-dropping RSSI error value.
UL report request interval	It defines the time between every UL-stats request.
T27 – Idle/Active	Minimum time between UL grants when Idle/Active: this parameter applies to the minimum time between unicast grants to SSs when BS believes SS uplink transmission quality is "*good enough*".
T7	Maximum DSA/DSC/DSD Response timeout: it sets the timeout between every DSA/DSD/DSC request retry.
T10	Maximum wait for transaction end time: once a response is received, the BS waits a guard time. This parameter sets the value of this time.
AK Lifetime	When a SS sends an "*Auth Request*" message, the "*Auth Reply*" message contains several parameters like the AK (*Authorization Key*) and the key's lifetime. This AK shall remain active until it expires according to its predefined AK Lifetime. This parameter allows the operator to set the time this key is valid.
TEK Lifetime	This parameter is used for setting the lifetime of the new Traffic Encryption Key at the target BS.
Rx CINR – Modulation Table Adjustment	This parameter allows the adjustment of the internal "*CINR-Modulation*" tables. Positive values (>0) will artificially increase the measured CINR, thus allowing higher modulations. Negative values (<0) will artificially decrease the measured CINR, forcing to lower modulations.

Table 12 - Network Maintenance Parameters

3.10. BW & Scheduler Setup

Any equipment capable to guarantee and implement QoS mechanisms must perform at least these differentiated functions: *Admission Control*, *Service Classification*, *Traffic Shaping & Polling* and *Scheduling*. This final phase is performed by the MAC *Scheduler*, which is responsible of transmitting the data packets in base of every packet's priority. It will be responsible of filling in the *Time Slots* in the WiMAX frame with the data from all the SSs, fulfilling the requests of the provisioned flows. Thus, the *Scheduler* is an essential component in any QoS granting architecture, as it performs the resource allocation for all the active users.

This section allows configuring some parameters around the MAC *Scheduler* and the frame distribution, as it is explained below. A snapshot of this menu can be viewed in Figure 30.

Figure 30 - "*BW & Scheduler Setup*" menu

► SCHEDULER BW EQUALIZER

The BS *Scheduler* can be equalized in this block, allowing the operator to configure it in *Equal Rate*, *Equal Symbol* or any other combination, using a defined weight scheme per modulation, independently in the UL and in the DL. Note that this equalization **will only affect the Best Effort traffic**. Thus, the QoS mechanisms will not be affected by this functionality.

The mode of the *BS Scheduler* can be set by the operator in the "*Mode*" labelled box located the top, where the three options may be chosen: *Equal Rate*, *Equal Symbols* and *User Defined*. By selecting one of the first two options, the system will configure the weights automatically as explained below, whereas the last option gives the operator total control in the assignment.

The default configuration follows the Equal Rate idea: every modulation is given the same weight (i.e., 1) so the BS will try to offer the same binary rate to every active

user. This means that if one user with poor link conditions is forced to use BPSK1/2, the BS will have to give him much more symbols than to a 64QAM3/4 operating user (approximately nine BPSK1/2 symbols for every 64QAM3/4 symbol). This guarantees that users are treated equally regardless their link conditions. The disadvantage of this method is that the overall throughput provided by the BS gets reduced for those users with poor modulations that use many symbols at slow binary rates.

The Equal Symbols mode gives different weights to the different modulations, so the overall system throughput could be enhanced giving more symbols to the users with the highest modulations. Referring to the example mentioned earlier with a BPSK1/2 user and a 64QAM3/4 user, if the weight given to the 64QAM3/4 modulation was "9" instead of "1", the Equalizer would operate in Equal Symbols mode. The BS will try to offer the same time slots to both users, so if the symbols used by both users are the same, the higher modulation one will achieve a much higher binary rate than the BPSK1/2 one.

Finally, by selecting the User Defined mode, the operator may decide the weight that will be assigned to every modulation. In conclusion, this block gives the operator completely control in the MAC Equalizer.

FRAME DIVISION

As explained before, *IEEE 802.16-2009* is designed to function in a framed format. The *frame* concept can be defined generally as a structured data sequence of fixed duration. The operation mode will be different in TDD and FDD systems; in the case of TDD, the uplink and downlink transmissions share the same frequency but are separated in time. Thus, the WiMAX frame will be divided into one *Downlink subframe* and one *Uplink subframe*, as shown in Figure 31 and in Figure 32.

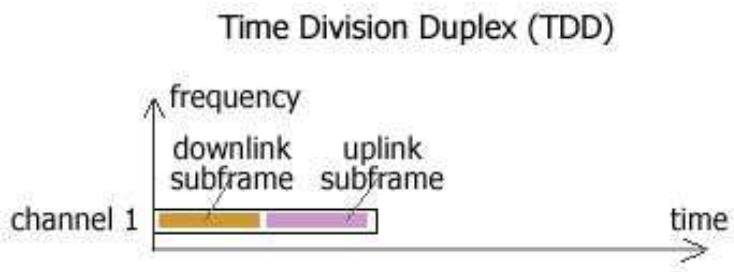


Figure 31 - TDD frame format

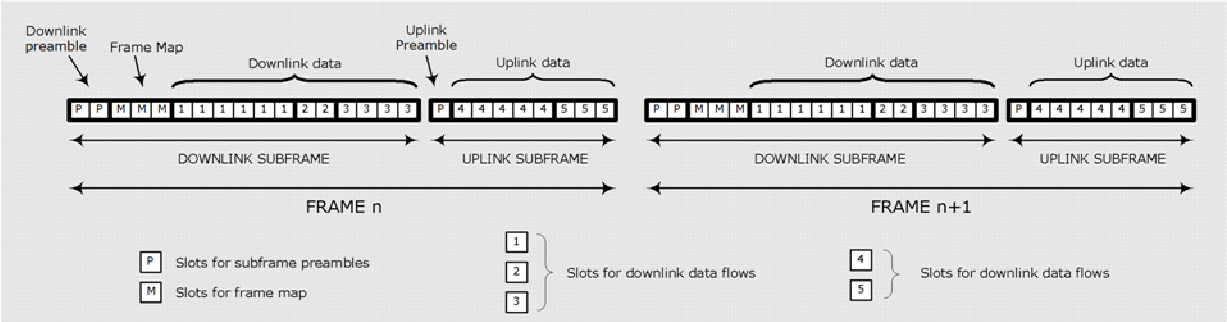


Figure 32 - *IEEE 802.16-2009* simplified frame scheme

TDD framing is adaptive in that the link capacity allocated to the downlink versus the uplink may vary. **AST** (*Allocation Start Time*) is the parameter that allows specifying the percentage of frame that is allocated to DL (so it also controls the UL time). Many Point-to-Point scenarios require symmetric capacity between UL and DL, what means that both subframes should have the same length. However, AST gives the chance to personalize the distribution of UL/DL for non-symmetric applications such as video broadcasting.

The BS lets to customize the frame distribution with the following parameters:

- **Frame Division**: as it has been explained before, the duration of DL and UL subframes may vary depending on the operator's needs. This parameter defines the percentage of the WiMAX frame that will be assigned to the DL subframe- As this percentage is referred to all the frame, including overheads and control information at the beginning and at the end of the frame, the *Frame Division* value will be limited automatically by the web interface if the allowed limits are exceeded. The limitation will vary with the current *Frame Duration* in "*Radio Parameters*" section.
- **DynAST**: in this mode, the BS automatically and dynamically divides the frame relying on the UL and DL traffic needs. This allows an efficient usage of the total available over-the-air throughput when the needs are variable between UL and DL. When this option is enabled, two new fields will be activated: *Min frame Div* and *Max frame Div*, trimming the dynamic range of the frame division.
- **Minimum Frame Division**: this parameter is associated to the DynAST functionality. It sets the minimum selectable *Frame Division*.
- **Maximum Frame Division**: this parameter is associated to the DynAST functionality. It sets the maximum selectable *Frame Division*.
- **Next Frame**: this parameter indicates the BS how to schedule UL data slots, both in the current frame or in the next frame. If "*Next Frame*" is selected, the slots allocated by the BS in the current frame will be transmitted by the CPEs in the next frame. If "*Next Frame*" is not selected, the CPEs will transmit allocated slots in the current frame. "*Next Frame*" selection allows some CPEs to perform better in the UL but it is not needed in most of the cases, so it can be left disabled.
- **DL->UL Extra gap**: this parameter selects the number of extra symbols to include as a separation between downlink and uplink subframes. Generally it is recommended to leave it as default (0 symbols).
- **UL->DL Extra gap**: number of extra symbols to include as a separation between uplink and downlink subframes. Generally it is recommended to leave it as default (0 symbols).

► SCHEDULER CONFIGURATION

- **Max. Contention RNG**: maximum number of broadcast contention ranging opportunities the BS will schedule in the UL per frame. These opportunities are scheduled using the symbols not needed for data traffic. The remaining symbols after de ContRNG are used for broadcast contention BW request opportunities.
- **Min. Contention Bandwidth**: this parameter refers the minimum number of broadcast contention band width request opportunities to be scheduled in the UL each "Contention BW Period" frames.
- **Contention Bandwidth Period**: it indicates the number of frames the BS waits to schedule at least "Min Contention BW" UL broadcast BW request

opportunities. Setting this parameter to "1" forces the BS means to schedule at least "*Min ContBW*" every frame.

- **Minimum Poll Rate**: this parameter adjusts the minimum number of connected CPEs/SSs that the BS will poll each frame. Higher values increase the frame overhead, but also reduce the overall latency.
- **DL Preambles**: by selecting this mode the BS inserts a preamble for each burst in the downlink subframe. These preambles may help in the DL reception in some radio conditions.
- **UL Gaps**: if this mode is enabled, the BS allocates one extra free symbol between UL bursts.

AGGREGATED BW

The throughput towards the wireless link can be adjusted using service flows with QoS specifications. However, if the cabled link (i.e. the backbone) cannot provide as much throughput as the WiMAX link, those QoS mechanisms should not be ensured end-to-end. To avoid this, the BS also allows the operator to limit the total aggregated traffic in the DL and in the UL directions. This is a very powerful tool when the deployment scenario has a limited backhaul BW. The selectable fields are the following:

- **Maximum Sector BW**: specifies the maximum allowed aggregated throughput, expressed in Kbit/s. "0" value sets this field to "*No Limit*" state (default configuration).
- **Maximum UL BW**: specifies the maximum allowed throughput in the *Downlink*, expressed in Kbit/s. "0" value sets this field to "No Limit" state (default configuration).
- **Maximum DL BW**: specifies the maximum allowed throughput in the *Uplink*, expressed in Kbit/s. "0" value sets this field to "No Limit" state (default configuration).

SCHEDULER STATS

- **Scheduler Stats Weight**: scheduler statistics are averaged by low-pass filtering as they are collected. This parameter allows this filtering to be adjusted. Averaged values are calculated by weighting the previous sample with this parameter and adding the current sample with the complimentary weight.

3.11. User Stats

There is a set of statistical parameters that can be studied in order to analyze the link state of every SS in the system. It shows the link statistics of users connected to de cell. The "*User Stats*" section is split in two tabs, where either a "*Basic View"* or a "*Detailed View"* can be found in order to get quick and basic information about the link state and also monitoring in more detail all the parameters. This is shown in and. This section is very useful to determine the optimal values for the radio parameters of the "*Radio Setup*" menu.

3.11.1. "*Basic View*" tab

This tab is represented in Figure 33. In this tab, the link state indicators are shown in a table, while each row represents a unique CPE. The screen will only show those users that are currently in the system or that are trying to connect or disconnect to the BS, so users that are not authorized to enter the network will not appear as Active. The *Web* browser's screen will be automatically refreshed to get updated values for every indicator.

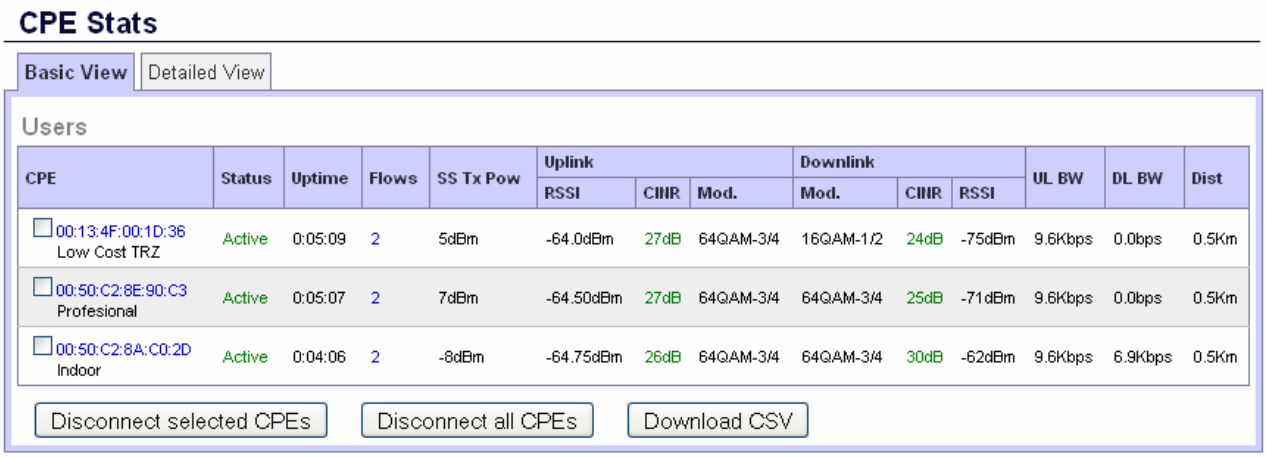


Figure 33 - "*User Stats*", Basic View tag

The most indicative link-state parameters are the following three: **RSSI**, **CINR** and **Modulation**, both for UL and DL. When referring to the UL, they indicate how the BS is receiving every SS, and when referring to the DL, they indicate how a SS is receiving the BS. The BS is capable to read these parameters from every SS and to show them in this section. These parameters are going to be explained more in detail in the following:

- "***Disconnect*" checkbox**: this checkbox next to a SS allows selecting one or many CPEs to force a manual disconnection from the BS. Remember that when a CPE is forced to disconnect from the BS, it will try to reconnect immediately. To definitely disconnect from the BS, it should not be provisioned in the "*Local AA*" Database.
- **CPE**: it indicates the MAC address of the associated SS as long as the SS alias (if specified). It includes a link to the "*Data Services*" submenu.
- **Status**: it indicates the status of that user (*Active*, *Connecting*, *Registering*…).
- **Uptime**: it indicates the time that has passed since the last time the CPE was connected to the BS.

- **Flows**: it indicates the number of service flows that have been correctly provisioned for that user. It includes a link to the "*Data Services*" submenu.
- **SS Tx Power**: it is the transmission power of the equipment, expressed in dB. Recall that this parameter is fixed automatically by the BS by using TCP (*Transmit Control Protocol*). When connecting to several SSs, the ones that indicate higher values of "*SS Tx Power*" are the ones that need more transmission power to reach a certain level of UL RSSI. This may happen because they are situated farther or because their antennas are pointed worse, for example.
- **UL/DL RSSI**: the RSSI (*Received Signal Strength Indication*) is a measurement of the power received by the radio-communications equipment. When referring to the UL RSSI, this parameter will represent the power received by the BS from this SS. On the other hand, the DL RSSI will represent the received power level by this SS from the BS. It is measured in dBm: $P(dBm) = 10log(P(mW))$.
- **UL/DL CINR**: the CINR (*Carrier to Interference plus Noise Ratio*) is a measurement of signal effectiveness, expressed in dB units. The carrier is the desired signal, and the interference may either be noise or co-channel interference or both. In order for the signal receiver to be able to decode the signal, the signal must fall into an acceptable CINR range. A better CINR will allow using a higher modulation and in conclusion to get a higher throughput, so the operator should try to maximize this parameter in both UL and DL.
- **UL/DL Modulation**: this value indicates the modulation type that is being used both in UL and DL. Recall that this modulation will be selected by the BS at each moment depending on the link budget and the current CINR values. The BS will select the modulation that offers the higher throughput for the current CINR.
- **UL/DL BW**: this value indicates the throughput that the user is currently using, in UL and DL, measured in bps/Kbps/Mbps.
- **Distance**: it is the estimated distance from the BS to that user, expressed in kilometres. The distance is calculated by the BS using the delay time of the transmitted messages, and will have an overall error margin of 500 meters, approximately.
- **"*Disconnect selected CPEs*" button**: when clicking this button, all the SSs whose "*Disc.*" checkbox is activated will be forced to disconnect from the BS.
- **"*Disconnect all CPEs*" button**: when clicking this button, all the SSs will be forced to disconnect from the BS.
- **"*Download CSV*" button**: when clicking this button, a text file in CSV format (*Comma-Separated Values*, a simple text file for a database table) will be downloaded, containing the link-state parameters that are shown in the screen.

NOTE

¿How are these parameters measured?

All the "measurable" parameters (RSSI, CINR…) are expressed as an average of various instantaneous values using an IRR low-pass filter. To explain how they are calculated, it is important to remember the framed structure of WiMAX.

Looking to the time axis, the BS structures the communication using frames, so over the air there will be consecutive frames like this:

[F1, F2, F3, …, F_{n-1}, F_n,…]

Every frame contains PDUs (*Protocol Data Unit*) belonging to the different users connected to the BS, and every PDU gives information about the instantaneous

values for these parameters (RSSI, CINR …). For parameters referring to the *Downlink* (information in the user's side), the information comes itself in the PDU datagram, and for the parameters referring to the *Uplink* (information in the BS's side), the BS will measure the signal entering the N-connector and will calculate the obtained value for each PDU.

These average values are calculated every frame, and the calculation procedure depends on the firmware version of the Base Station, as it will be explained below:

→ **3.2 or previous releases:** the calculated average value for one parameter regarding one user will only consider the information contained in the first PDU of this user in the current frame, applying a low-pass filtering using the value that has been calculated in the previous frame. For example, the calculation of the average CINR in the "**n**" frame will be:

$$CINR_{AVRG(n)} = 0.7*CINR_{1^{st}\_PDU\,(n)} + 0.3*CINR_{AVRG(n-1)}$$

→ **3.3 or later releases:** the calculation method is slightly more accurate after the 3.3 releases. Instead of considering only the first PDU for a given user in the "**n**" frame, it will be considered the main average between all the PDUs of this user in "**n**" current frame. For example, the calculation of the average CINR in the "**n**" frame will be:

$$CINR_{AVRG(n)} = 0.7*CINR_{AVRG\_PDUs\_FRAME(n)} + 0.3*CINR_{AVRG(n-1)}$$

3.11.2. "*Detailed View*" tab

This tab shows a wide amount of more detailed statistics related to the link status, in order to give more detailed idea. As shown in Figure 34, five information blocks are displayed in this screen.

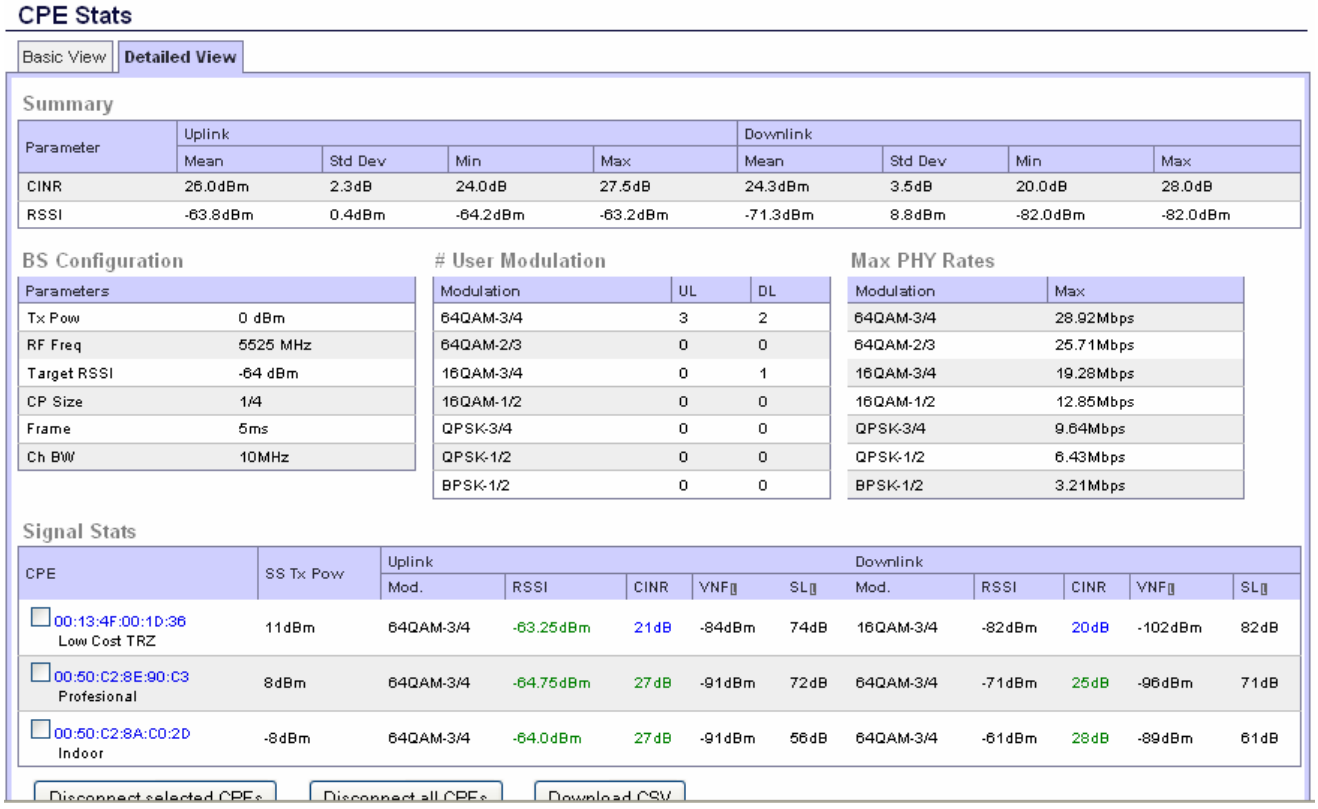


Figure 34 - "*User Stats*", Detailed View tag

- **SUMMARY**: this block offers statistical information about the CINR and the RSSI measured for all the active users, both in the UL and DL. The table includes the "***Mean Value***", ***"Standard Deviation***", "***Minimum Value***" and "***Maximum Value***" for CINR and RSSI.
- **BS CONFIGURATION**: this informative block indicates the current radio configuration of the BS, the one which has been set in the "*Radio Parameters*" section: *Transmission Power*, *Frequency*, *Target RSSI*, *Frame duration*…
- **USER MODULATION**: this table summarizes the number of active users that are working on each modulation, both in the UL and in the DL.
- **MAXIMUM PHYSICAL RATES**: this table informs about the maximum theoretical throughput at the Physical Layer for each modulation. The achievable bitrates for each modulation will be different depending on the current radio configuration in the BS: *Channel Bandwidth*, *Frame Duration*, *Cyclic Prefix*…
- **SIGNAL STATS**: besides the link-state parameters already shown in the "*Basic View tag*" (modulation, RSSI, CINR, etc.), this block contains new indicators for UL and DL: The **Virtual Noise Floor** (VNF) and the **System Losses** (SL):
    - **VNF**: it gives an overview of the unwanted signal level such as noise and interference at the receiver (in the Uplink section, the receiver will be the BS and in the Downlink section, the receiver will be the CPE). It is calculated by subtracting the CINR measure to the received signal level.
    - **SL**: it shows the signal losses from transmitter to receiver radio connectors, so it is useful for measuring the total propagation losses including the antenna gain.

3.11.3. *Data Services* submenu

This submenu will be shown when clicking into the *SS* or *Flows* fields of the "*Basic View*" tag. There, the provisioned service flows will be listed and describes, as long as specific information about the current SS. The screen is shown in Figure 35, and it is presented in two blocks: *CPE Summary* and *Flow Management*.

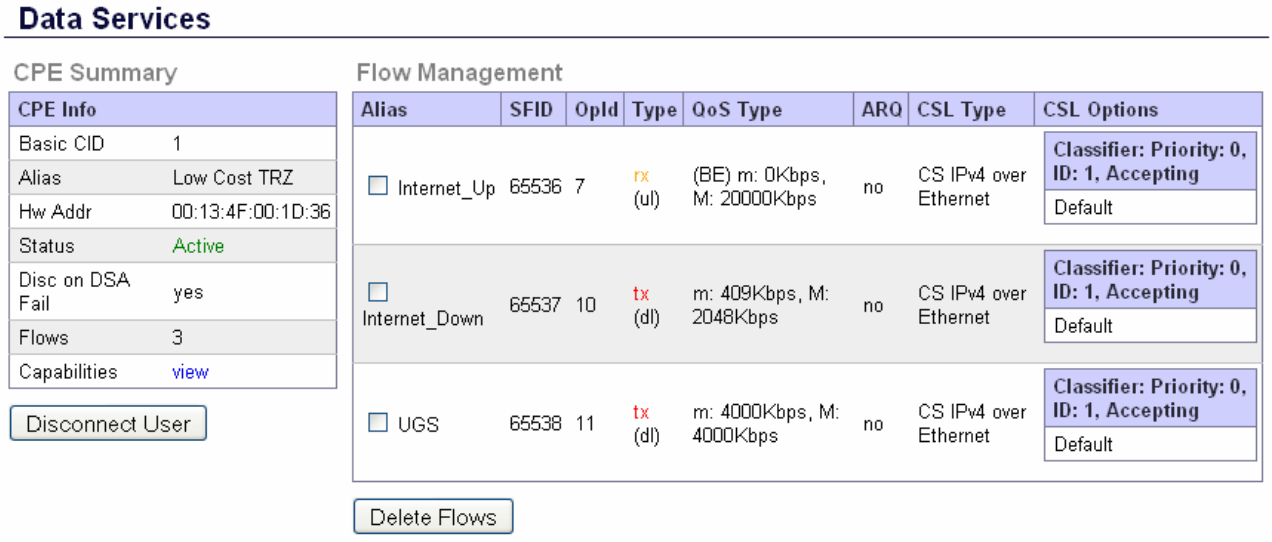


Figure 35 - "*Data Services*" submenu

► **CPE SUMMARY**

It shows general information about the SS, such as:

- **Basic CID**: every user will be assigned a CID identifier by the BS.
- **Alias**: the user alias specified in the provisioning database (if any).
- **HW address**: it indicates the MAC address of the associated SS.
- **Status**: it indicates the status of that user (*Active*, *Connecting*, *Registering*…).
- **Disc on DSA Fail**: it shows the status of this option; if it is not active, after a certain number of DSA retries is exceeded without getting any response from the CPE, the CPE will remain active but some of the provisioned flows will not be added. On the other side, if the "*Disc on DSA Fail*" field is active, the CPE will be dropped from the BS instead of being added without service flows.
- **Flows**: the total amount of provisioned flows.
- **Capabilities**: It includes a link to the "*Data Services*" submenu, which will be explained in 3.11.4.
- **"*Disconnect User*" button**: it forces to disconnect the current user.

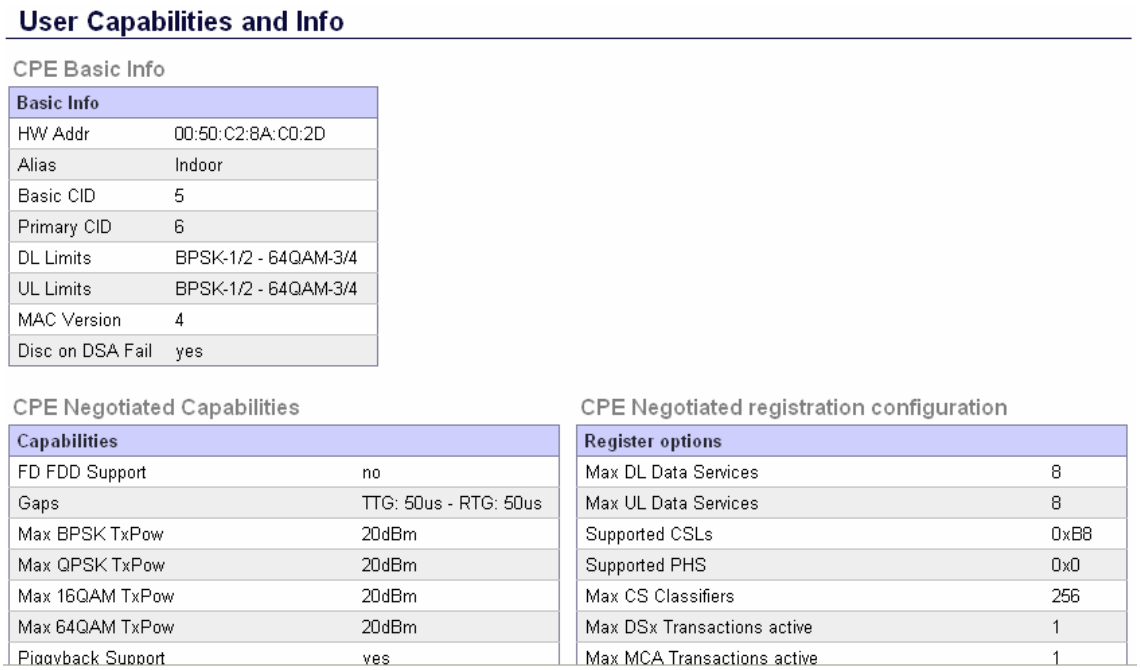
► **FLOW MANAGEMENT**

Represented as a table where every row will refer to a service flow, it shows general information about the provisioned flows. In the following these parameters are going to be explained more in detail:

- **"*Delete*" checkbox**: it is situated next to a service flow and allows selecting one or many flows so they could be deleted with the "*Delete flows*" button.
- **Alias**: the service flow alias specified in the *Flow Descriptor* (if existing).
- **SFID**: it indicates the *Service Flow Identifier* number. This identifier will be assigned by the BS randomly to every flow when is created.
- **Operator ID**: it shows the *Operator Identifier* of the service. As opposed to the SFID, which is different every time the flow is created, the *Operator Identifier* has a fixed value as defined in the provisioning database of the BS.
- **Type**: it indicates the type of the flow (TX or RX).
- **QoS Type**: it shows some QoS properties of the flow, such as minimum/maximum bitrates as long as the type of QoS (BE, RTPS; UGS…).
- **ARQ enabled**: it indicates if the flow supports ARQ.
- **CSL Type**: it indicates the current CSL type.
- **CSL Options**: it shows information related to the flow priority and the specified classifiers, if any.
- **"*Delete flows*" button**: it forces to delete the selected flows.

3.11.4. *User Capabilities and Info* submenu

This submenu will be shown when clicking into the *Capabilities* field in the "*Data Services*" submenu. It shows different information about the CPE and the negotiated capabilities with the BS, and a snapshot can be viewed in Figure 36.



User Capabilities and Info

CPE Basic Info

Basic Info	
HW Addr	00:50:C2:8A:C0:2D
Alias	Indoor
Basic CID	5
Primary CID	6
DL Limits	BPSK-1/2 - 64QAM-3/4
UL Limits	BPSK-1/2 - 64QAM-3/4
MAC Version	4
Disc on DSA Fail	yes

CPE Negotiated Capabilities

Capabilities	
FD FDD Support	no
Gaps	TTG: 50us - RTG: 50us
Max BPSK TxPow	20dBm
Max QPSK TxPow	20dBm
Max 16QAM TxPow	20dBm
Max 64QAM TxPow	20dBm
Piggyback Support	yes

CPE Negotiated registration configuration

Register options	
Max DL Data Services	8
Max UL Data Services	8
Supported CSLs	0xB8
Supported PHS	0x0
Max CS Classifiers	256
Max DSx Transactions active	1
Max MCA Transactions active	1

Figure 36 - "*User Capabilities and Info*" submenu

As explained before, during the network entrance procedure and immediately after completion of ranging, the SS informs the BS of its basic capabilities. Depending on the SS model and vendor, some capabilities may be supported and other not. In this submenu these capabilities can be analyzed in detail.

3.12. BW Stats

This section shows information about the real-time traffic statistics: Bytes/sec per flow, total Packets/s, aggregated traffic, frame utilization, etc... The screen is automatically refreshed and a sample screenshot is shown in Figure 37. This is a very interesting section because it offers useful traffic statistics and allows controlling that the traffic is being transported using the correct service flows.

The screen is divided in four tabs in which basic and detailed information about the cell stats and service stats can be found. These subsections will be explained below.

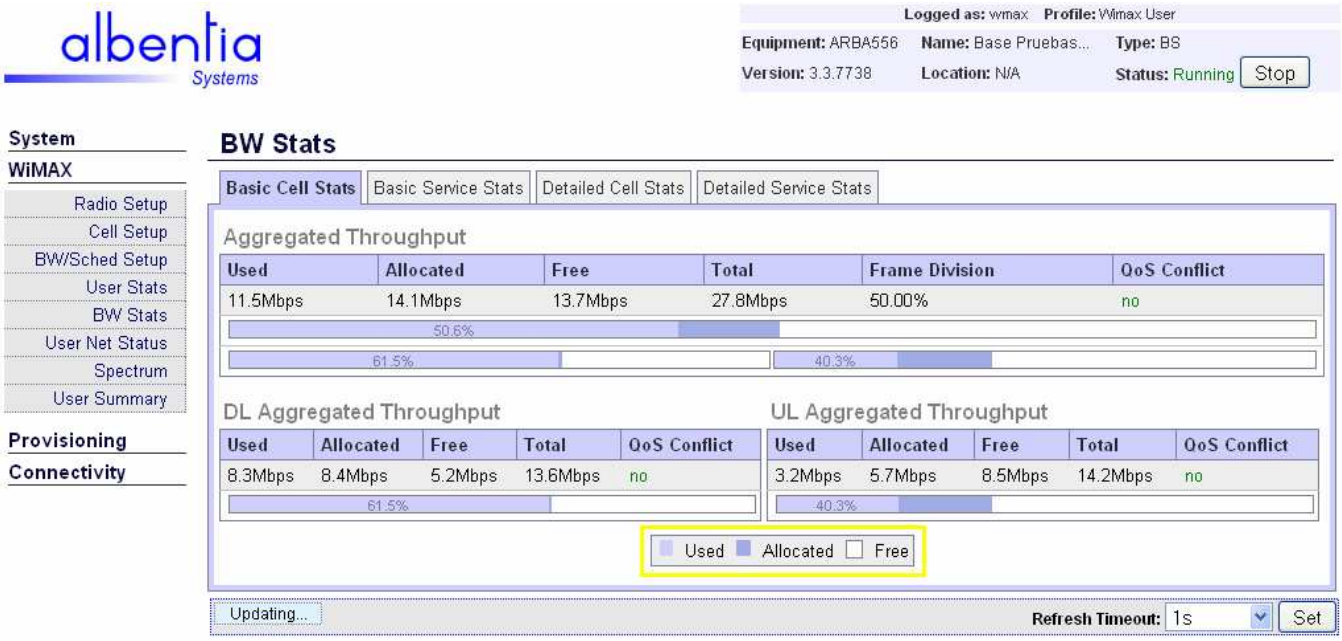


Figure 37 - "*BW Stats*" menu, Basic Cell Stats tag

3.12.1. "*Basic Cell Stats*" tab

As shown in Figure 38, this tab gives information about the overall throughput in the cell, representing the current usage of the frame. The upper block tells about the Aggregated Throughput, and the two blocks in the bottom show information about the Downlink and the Uplink, respectively. These parameters are shown:

- **Used**: throughput that is being currently used in Mbps. It will not be higher than the allocated throughput
- **Allocated**: throughput of the reserved symbols by the BS. This value will vary depending on to the current status of the cell (current modulations), the traffic demands of all CPEs, and the provisioned QoS mechanisms for the data flows.
- **Free**: it indicates the current free throughput in the frame, taking into account the not-used symbols.
- **Total**: it is the potential maximum throughput that can be obtained both in the Uplink and in the Downlink with the current modulation schemes of the active users. When the frame is empty, the total throughput will be approximately the same than the free throughput.
- **Frame Division**: the percentage of duration of DL and UL subframes as configured by the operator in the "*Bandwidth and Scheduler*" section.

- **QoS Conflict**: it shows if the BS is having any problem on provisioning the configured services (for example when the BS has not enough free symbols in the frame to meet the established QoS requirements.

Besides the numeric information, the results are also shown graphically using bars and different colours, so the operator can easily visualize what is going on in the cell.

3.12.2. "*Basic Service Stats*" tab

This screen shows basic information about all the active Service Flows. In the "*Tx (DL) Data Service Stats*" and "*Rx (UL) Data Service Stats*" blocks, all the active downlink and Uplink service flows, respectively, are shown. This information is represented in a table where each row refers to a unidirectional single flow, so it is possible to know all the information about how the traffic is being currently served in the cell. This is useful for the operator to check how much throughput is used by every CPE, as long as to check if the classifiers are correctly created and working. The parameters that can be found are:

- **User**: the MAC address of the associated CPE, the alias (if any) and the BS's network interface that this flow is using.
- **Service**: it shows information about that single flow service for its identification, such as *Service Identifiers* (CID, SFID and Operator ID) and *Service Provisioned QoS* (Type, Minimum rate and Maximum rate).
- **CS Queued**: number of packets being queued by the BS in the Convergence Sublayer when transmitting.
- **Dropping**: it indicates if packets are being dropped in the BS when transmitting. The BS will start dropping packets when the queue of that flow is full.
- **Tx Rate**: the throughput used by that service flow, measured in bps/kbps/Mbps.
- **Usage**: percentage of the service flow that is being used according to the provisioned maximum bit rate for that flow.

Two more blocks in the left of the screen give further information: in *Summary* an extract of the basic statistics can be found: total amount of service flows, throughput in Mbps and packets, both for DL and UL. *Ethernet Stats* sums up the current traffic at the Ethernet interface of the Base Station (the received traffic via WiMAX is transmitted via Ethernet and vice versa).

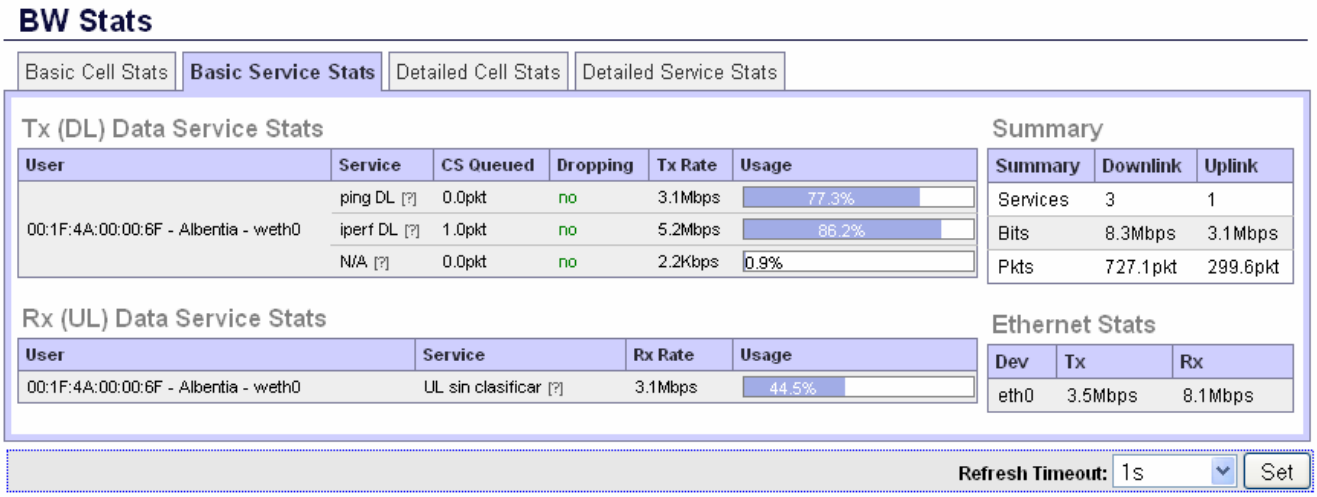


Figure 38 - "*BW Stats*" menu, Basic Service Stats tag

3.12.3. "*Detailed Cell Stats*" tab

As shown in Figure 39, this tab gives a very complete description of the allocated throughput scheduled by the BS in the cell. It is structured in four blocks where several statistics can be found. This information can also be downloaded in text format by pressing the "Download CSV" button.

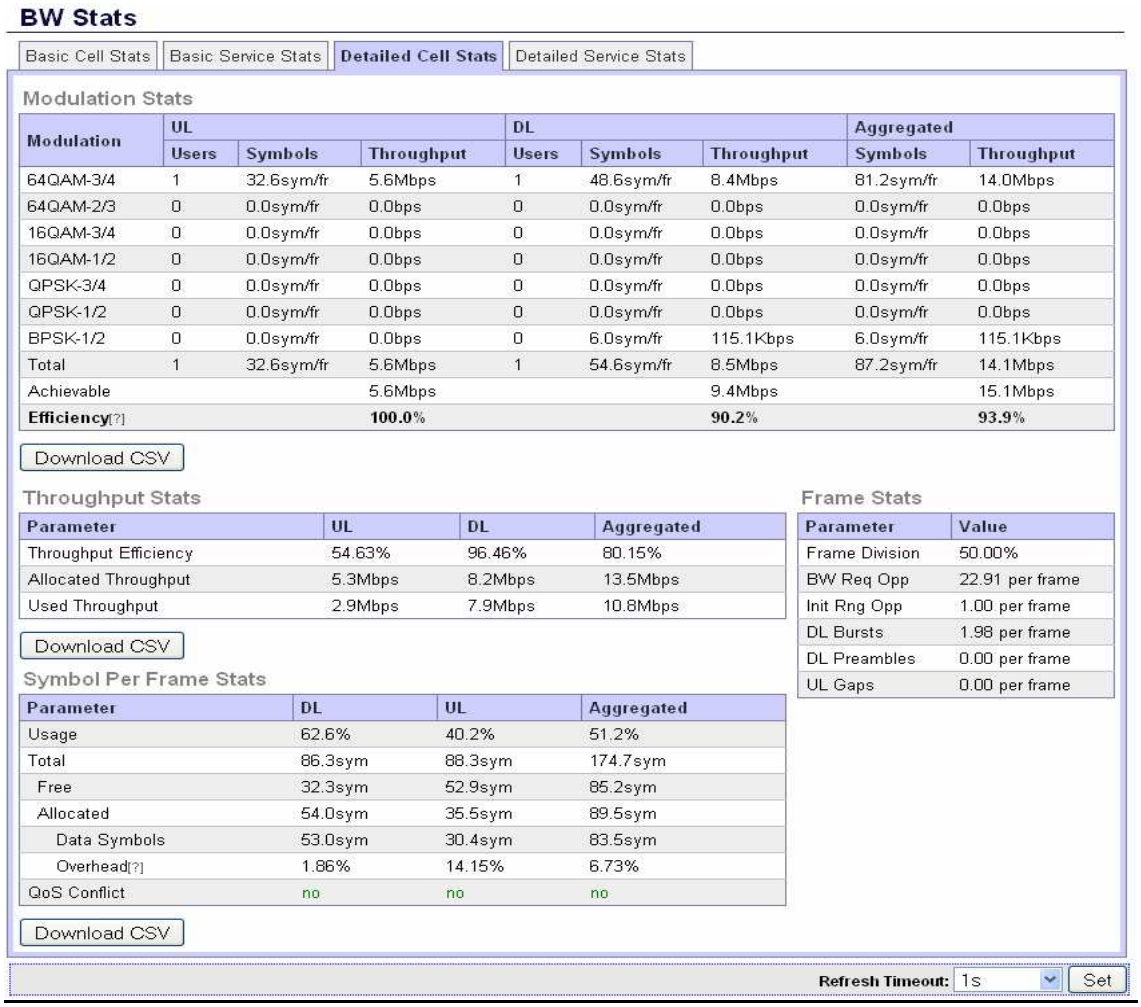


Figure 39 - "*BW Stats*" menu, Detailed Cell Stats tag

- **Modulation Stats**: this table describes the allocated throughput in the cell regarding the modulations currently used. For UL and DL, it informs about the number of users working in each modulation, the symbols per frame used by each modulation, and the currently allocated throughput. It shows also the aggregated (UL and DL) rates and the total traffic allocated when considering all the modulations, as well as the achievable throughput (in the case all symbols were scheduled using the best modulation in terms of bytes per symbol). Finally the *Modulation Efficiency* is also calculated, which gives an overview of the modulation efficiency of the cell taking into account the allocated throughput versus the achievable throughput.

NOTE

Despite no users are connected to the Base Station, a little and permanent BPSK1/2 traffic may be found in the Downlink when the MAC is started. This traffic corresponds to broadcast messages sent by the BS to inform about the frame configuration (DL-MAP, UL-MAP, DCD, UCD, and FCH, among others). The standard sets that these broadcast messages must be transmitted in the worst possible modulation.

- **Throughput Stats**: this table summarizes for the UL and DL the allocated throughput, the used throughput and the efficiency, as well as the aggregated statistics.
- **Frame Stats**: this block gives an overview of the status of the frame. It shows information like the Frame Division, the BW Request and Initial Ranging opportunities, the DL Burst and Preambles and the UL Gaps.
- **Symbol per Frame Stats**: in this table some parameters regarding the symbols per frame for DL, UL and Aggregated are showed: percentage of usage, free, allocated and total amount of symbols, and QoS conflict. Allocated symbols are split between Data Symbols and Overhead (percentage of symbols filled with frame signalling information versus symbols filled with data).

3.12.4. "*Detailed Service Stats*" tab

This screen gives detailed information and statistics about the service flows. It follows the same structure that the basic view but some more parameters can be found. In "*Tx (DL) Data Service Stats*", "*Rx (UL) Data Service Stats*" and "*Secondary Management Channel Stats*", all the active Tx, Rx and SMC service flows are shown, where some new statistics appear.

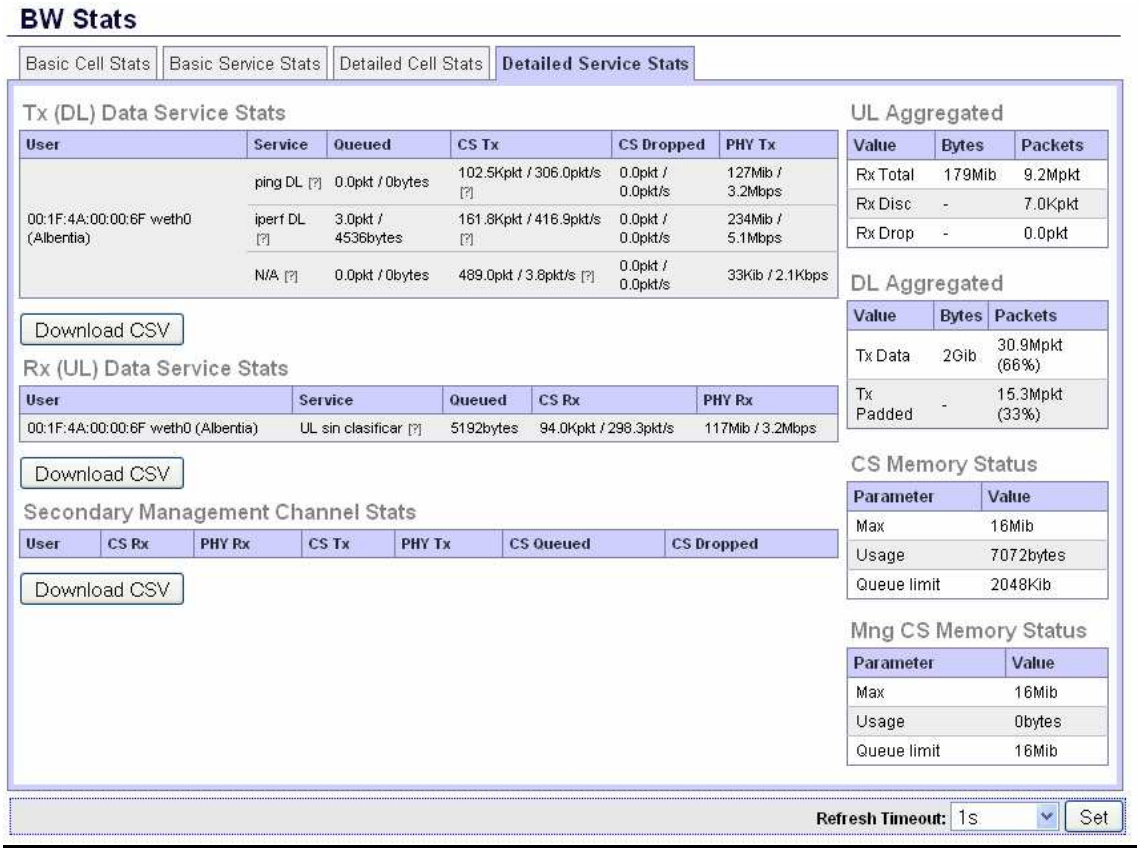


Figure 40 - "*BW Stats*" menu, Detailed Service Stats tag

- **Queued**: it indicates the status of the transmission queues in the convergence sublayer, expressed in packets and bytes.
- **CS Tx**: it indicates the overall and current traffic at the convergence sublayer, expressed in packets (overall) and packets/second (current). It informs also about the maximum length of the queue, the length of the queued data, the maximum memory of the queue and the memory used.
- **CS Dropped**: it indicates the overall and current dropped traffic in the convergence sublayer, expressed in packets (overall) and packets/second (current).
- **PHY Tx/Received**: it indicates the overall and current traffic at the Physical Layer, expressed in megabits (overall) and megabits/second (current).

In the right side of the screen, additional information related to the service flows can be found. In "*UL Aggregated*" current statistics can be found in bytes and packets, such as the total amount of received packets or the discarded and dropped packets. In "*DL Aggregated*" the transmitted data and transmitted padded in bytes and packets are displayed. Finally "*CS Memory Status*" and "*Mng CS Memory Status*" blocks show information about the WiMAX Convergence Sublayer and the Management Convergence Sublayer, respectively, with the following information: *Maximum Available Memory*, *Currently Used Memory* and *Memory Queue Limit*.

3.13. User Net Status

This menu displays the current network configuration of all the virtual wireless interfaces (*wethx*) that are currently active in the BS. The information will be displayed in up to four different tables, one for each network operation mode: **Routed**, **Bridged, Bridged VLAN** and **Local Network**. In addition, a summary is shown in the right side of the screen. A sample screenshot is shown in Figure 41.

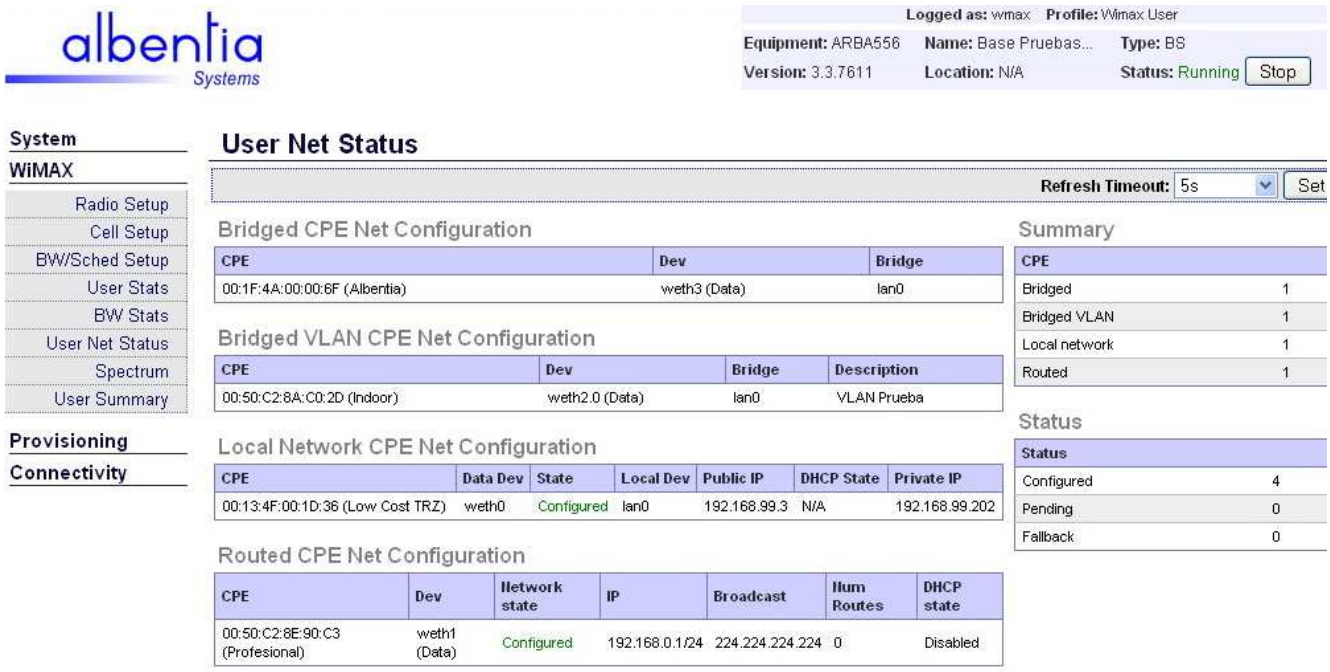


Figure 41 - "*User Net Status*" menu

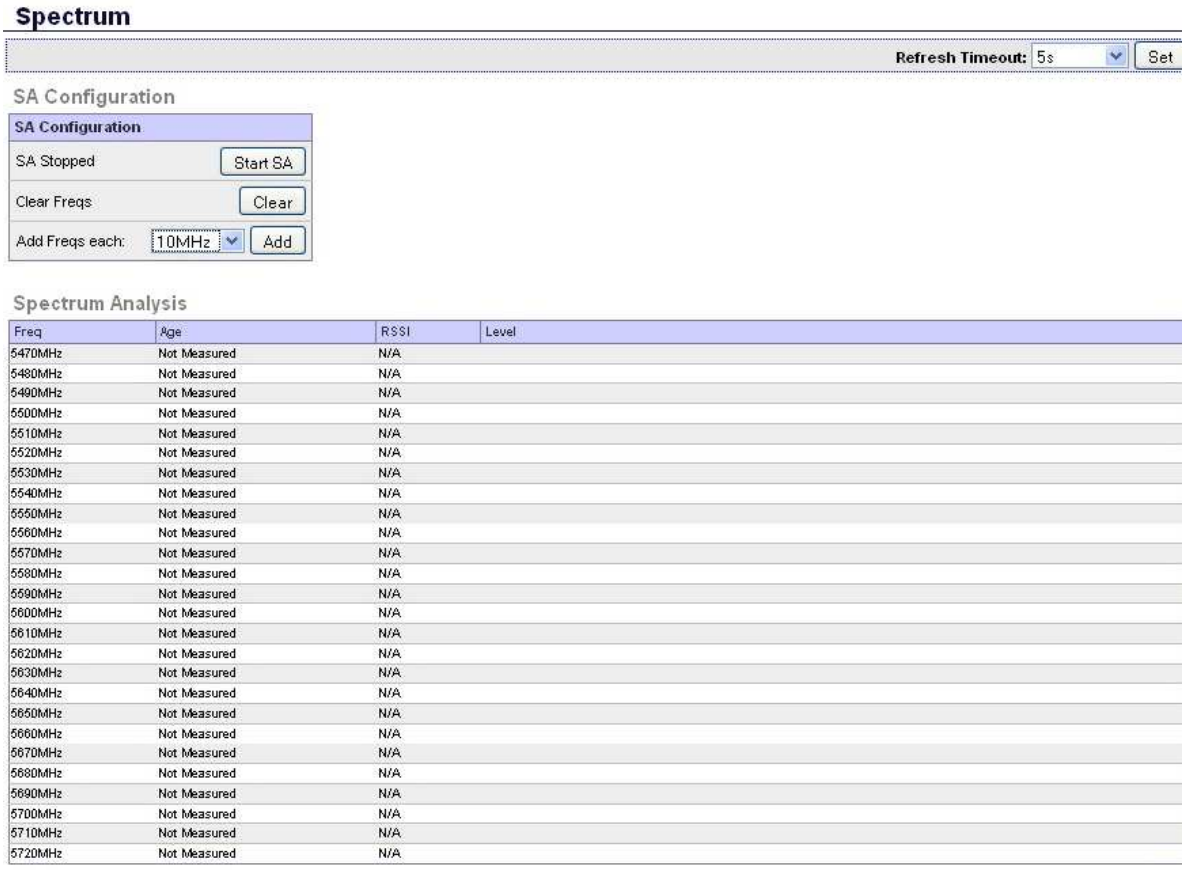
NOTE

When DHCP is being used, useful information may be found in the "DHCP State" column. If the state is "*Bound*", a [+] tooltip will appear, showing these parameters: "*DHCP Server IP address*", "*Total Lease Time*" and "*Remaining Lease Time*".

3.14. Spectrum

This section includes a very useful feature for field operation: the **Spectrum Analyzer**. This tool scans the radio spectrum all along the frequency band (ETSII or FCC, depending on the unit) and measures the RSSI levels of the incoming signals. It is very useful for detecting other equipment working in the same frequency band. The recommended procedure is to run always the Spectrum Analyzer before choosing the working frequency of the ARBA135, as it gives a good idea about how the spectrum is being used in that location, showing the signal-free channels.

Figure 42 - "*Spectrum*" section



Freq	Age	RSSI	Level
5470MHz	Not Measured	N/A	
5480MHz	Not Measured	N/A	
5490MHz	Not Measured	N/A	
5500MHz	Not Measured	N/A	
5510MHz	Not Measured	N/A	
5520MHz	Not Measured	N/A	
5530MHz	Not Measured	N/A	
5540MHz	Not Measured	N/A	
5550MHz	Not Measured	N/A	
5560MHz	Not Measured	N/A	
5570MHz	Not Measured	N/A	
5580MHz	Not Measured	N/A	
5590MHz	Not Measured	N/A	
5600MHz	Not Measured	N/A	
5610MHz	Not Measured	N/A	
5620MHz	Not Measured	N/A	
5630MHz	Not Measured	N/A	
5640MHz	Not Measured	N/A	
5650MHz	Not Measured	N/A	
5660MHz	Not Measured	N/A	
5670MHz	Not Measured	N/A	
5680MHz	Not Measured	N/A	
5690MHz	Not Measured	N/A	
5700MHz	Not Measured	N/A	
5710MHz	Not Measured	N/A	
5720MHz	Not Measured	N/A	

Figure 43 - Spectrum analyzer (before measuring)

First step is to select the measurement steps for the Analyzer: **1MHz**, **2.5MHz**, **5MHz**, and **10MHz**. A smaller channelization involves a more complete and accurate radio analysis, but it will take more to finish (it must perform more measurements). On the other hand, the 10MHz step gives a less precise idea of the medium but is the fastest available analysis. Note that it takes about 2.5 seconds to measure a channel, so it must be taken into account when selecting the channelization step. Once the user selects the step and after pressing the "*Add*" button al the channels will appear in the screen automatically, as shown in Figure 43. For selecting a different channel step, just click in the "*Clear Freqs*" button to delete the current analysis, and select the new step as explained before.

The "*Spectrum Analysis*" table includes one row for each frequency to be measured, and shows the measurement Age (seconds since it was performed), the RSSI (in dBm), and a "*Level bar*" which is a graphical representation of the measured RSSI for each frequency.

Once the frequencies have been added, the analysis will start after pressing the "*Start SA*" button. An animated icon will display the word "***Scanning***", and the obtained values will start filling in the table. Note that after finishing the scan of the last added frequency, the analyzer will keep on scanning starting again from the first frequency. It must be stopped manually by the user, pressing the "*Stop SA*" button. A complete analysis sample with a 10 MHz step is shown in Figure 44.

Spectrum Analysis

Freq	Age	RSSI	Level
5470MHz	101.9s	-100dBm	
5480MHz	99.3s	-99dBm	
5490MHz	96.7s	-98dBm	
5500MHz	94.0s	-97dBm	
5510MHz	91.4s	-97dBm	
5520MHz	88.8s	-98dBm	
5530MHz	86.2s	-98dBm	
5540MHz	83.6s	-98dBm	
5550MHz	81.0s	-98dBm	
5560MHz	78.4s	-98dBm	
5570MHz	75.8s	-98dBm	
5580MHz	73.2s	-97dBm	
5590MHz	70.6s	-93dBm	
5600MHz	68.0s	-81dBm	
5610MHz	65.3s	-83dBm	
5620MHz	62.7s	-95dBm	
5630MHz	60.1s	-95dBm	
5640MHz	57.5s	-95dBm	
5650MHz	54.9s	-90dBm	
5660MHz	52.3s	-75dBm	
5670MHz	49.7s	-82dBm	
5680MHz	47.1s	-97dBm	
5690MHz	44.5s	-98dBm	
5700MHz	41.9s	-97dBm	
5710MHz	39.3s	-98dBm	
5720MHz	36.6s	-97dBm	

Figure 44 - Spectrum analyzer, after measuring

⚠ ATTENTION!

While the Spectrum Analyzer is working, the BS must stop the WiMAX transmissions, so all active users in the cell will be dropped until the Analyzer is stopped. Once the SA is stopped by the user, the WiMAX MAC will remain stopped too, so it is necessary to restart it manually (for example using the "*Start*" button in the System Connection Area, in the top-right side of the web.

NOTE

Remember that once the Analyzer starts measuring, it will not stop until the "*Stop SA*" button is pressed. When the access to the web interface is being performed via a WiMAX link, using this tool may leave the unit unreachable, because when it scans the WiMAX MAC is stopped and the SA must be stopped manually.

NOTE

The measurements provided by the Spectrum Analyzer will remain in memory as long as the unit is powered on. If the unit is rebooted, the data will be lost and a new Analysis may be required.

3.15. User Summary

This section allows to obtain the overall status of a single CPE connected to the cell, displaying a lot of related information: radio levels, currently served traffic, service flow information… It is intended to be a very useful section for CPE installers, as long as they can have all the related information of a CPE that they are installing. The first screen of this section is shown in Figure 45.

Figure 45 - "User Summary" menu

First step is to select the CPE that is going to be looked up. It is possible to select one from the "*Active users*" list, or to fill in the MAC address manually in the "*Search User*" field. Obviously if there is no CPE connected in the cell, it will not be possible to select anything. When pressing the "*View*" button, all the information related to that CPE will appear, divided in two tabs: **Summary** and **Detail**.

3.15.1. "*Summary*" tab

This tab is shown in Figure 46 and displays two main information groups:

- **Radio Levels**: it shows basic current radio information, both in the Uplink and in the Downlink: *RSSI*, *CINR*, *Modulation* and *Transmission Power*.
- **Traffic Summary**: it shows aggregated throughput information, both in the Uplink and in the Downlink: *overall and instantaneous bit rate*.

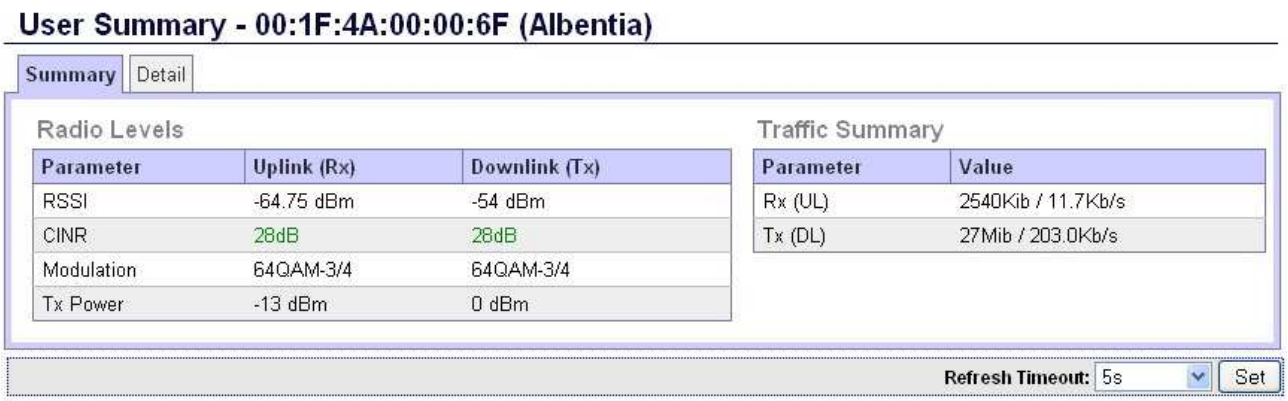


Figure 46 - User Summary: Summary tab

3.15.2. "*Detail*" tab

This tab is shown in Figure 47 and displays many information groups:

- **UL/DL Services**: it shows information related to the active service flows, such as their alias, QoS, classifiers, ARQ,… as long as their throughput information
- **Network information**: basic networking information such as the network mode (Bridging, Routing…), DHCP state, active Net Hooks…
- **Radio Levels**: current radio information, both in the Uplink and in the Downlink: *RSSI*, *CINR*, *Modulation*, *Transmission Power* and *Approximate Distance*.
- **Status & Information**: CPE uptime, Authentication enabled, Secondary management Connection enabled.
- **"*Disconnect CPE*" button**: this button disconnects this CPE from the cell.
- **UL/DL RSSI and CINR graphics**: these graphics show different measures of CINR and RSSI, so it is possible to watch the maximum achievable values while performing the CPE alignment. Each graphic is prepared to show up to 14 measured values, and the Measure Age will depend on the refresh time of this tab (selectable by the "*Refresh Timeout bar*").

All the groups may be minimized or maximized using the **[-]** an **[+]** icons displayed before the group title.

Figure 47 - User Summary - Detail tab

3.16. Provisioning System: Local AA

3.16.1. Theory of Operation

WiMAX (*802.16*) systems, in opposite to other wireless systems, must be provisioned. This means that *users* and their associated *services* must be previously defined according to this provisioning system, so that when a new user tries to get into the network, the BS decides whether to allow the new user (SS) into the cell or not. The BS must also know which data services the new SS is permitted to have.

The mechanisms that control, over the air, the user entry and the allocation of new data services are fully described in the *802.16-2009/05* standards. As it was stated before, these mechanisms only have control over the "air interface" operations of the system, and therefore do not describe how the Bs manages to get the provisioning data (it is specific of each implementation). Figure 48 shows a basic user network entry and data services allocation.

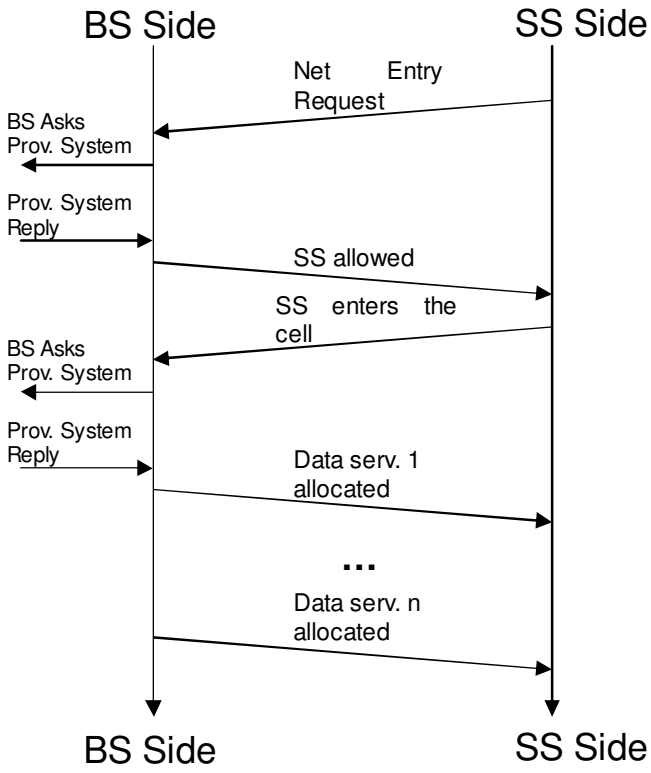


Figure 48 - Initial negotiation between BS and SS

As shown in Figure 48, BS and SS exchange messages to allow the SS to enter the network and, afterwards, to allocate data services. These procedures are covered by the previously mentioned standards, and are implemented by both BS and SS equipment.

In Figure 48 is also shown that the BS needs a system to provide the SS network entry information and service flows. This is the provisioning system. ARBA135 BS family is shipped with an internal local provisioning system. This system architecture is depicted in Figure 49.

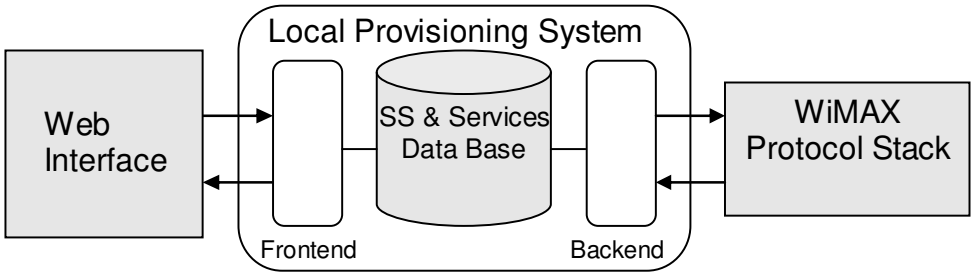


Figure 49 - System architecture scheme

Using this local provisioning system, the BS equipment holds a data base in which all the allowed users and their data services are stored. When a new user has to be provisioned in the cell, the operator accesses the provisioning system using the BS's web interface. In order to open the local provisioning web interface, log into the BS web and then click on the "*Local AA (Authentication and Authorization)*" button on the left menu. Figure 50 shows the local provisioning main page.

Figure 50 - "*Local AA*" menu

This interface allows the operator to provision users or to delete existing ones, and to manage data services of provisioned users. This system also informs the operator about which provisioned users are currently active in the cell. In addition, the system provides the ability to provision groups of users, sharing the same configuration amongst them. A group of users is defined by a base MAC address and a mask,

proving that if a user MAC address *bitwise AND-ed* with the mask is equal to the base address, the user belongs to that group.

⚠ ATENTION!

This web page is the frontend to the provisioning system. This implies that if a user that is active is de-provisioned, the user will not be disconnected; only removed from the database. If the user is dropped using the tools available in the system, for example in the "*User Stats*" menu, then it will not be able to get into the cell again as it has been de-provisioned.

This also applies to service provisioning. When a user that is already active in the cell is provisioned with a new service, or a current service is changed, the changes will take effect the next time the user connects to the BS

NOTE

The title of the "*Provisioned Users*", "*Provisioned Groups*", "AA Local Database" and "*AA Database Backup*" blocks is preceded by a - or + symbol which may be used to contract or expand the contained elements.

3.16.2. User and Group Provisioning

As explained before, the local provisioning system allows the operator to add, remove, and modify users or groups of users in the BS database. Only allowed or provisioned users in the local database may connect to the cell. A user can be directly provisioned as a standalone user or can be included into a user group.

The web tool to manage user database is accessed via the "*Local AA*" menu. The main view shows the current status of the database and a summary of the users that are connected, connecting or disconnecting. In Figure 50 the provisioning database has defined 5 different users with the different alias "*Albentia*", "*Low Cost CPE", etc.* and a group with the alias "*EVERYBODY*".

As shown in Figure 50, the Local AA menu presents different blocks in which the following information can be found:

- **PROVISIONED USERS**

  - **SS Address**: it indicates the MAC address of the associated CPE. It includes a link to the "*SS/User Description*" submenu.
  - **Alias**: is shows (if specified) a user-friendly text string that the operator may provide when allocating new users. This alias is used in many dialogues in the web and management system to make it easy to manage.
  - **Status**: it indicates the current status of that user (*Active/ Disconnected*).
  - **Access**: this tool allows the operator setting the access of a user by pressing the *"Set"* button. Sometimes the operator may want to temporarily forbid entering the WiMAX cell to a provisioned user or group, without deleting it from the database. There are 3 possibilities for the access: "*Allow*" means that the user is allowed to enter the cell; by selecting "*Reject*", the user or group will not be allowed to enter the cell and the BS will drop it, and "*Deny*" refers that the user is not allowed, but if the device is rebooted, it will switched to allowed

automatically. Clicking "*Allow*" again, the access to the WiMAX cell will be restored, and the BS will not drop it any more

- **Actions**: is contains two buttons, "*Copy*" is used for creating a copy of the user, so that it is not necessary to specified every parameters of the new user in case they are the same. Provisioned items may be easily removed from the local database; the "*Delete*" button removes the user or group for the database.

► PROVISIONED GROUPS

This menu allows also provisioning a group of users identified by a *Group address* and a *Mask,* (in the example, **00:00:00:00:00:00** and **00:00:00:00:00:00,** which means that every user belongs to this group). If there were another group identified, for instance, by a base address **00:50:C2:BE:90:00** and mask **FF:FF:FF:FF:FF:00**, it would mean that every user with a MAC address between 00:50:C2:BE:90:00 and 00:50:C2:BE:90:FF belongs to this group so it will be provisioned with the provisioning conditions specified in the group. The following points will go over it in more detail. (The *Alias*, *Access* and *Actions* parameters are the same that the explained for single users).

NOTE

When denying or rejecting a CPE, it will be automatically dropped by the BS, but in case of Groups of users, it is necessary to disconnect the group to apply the changes.

NOTE

In the case that a user MAC address is provisioned as a single user and also belongs to a provisioning group, the former specification has a higher priority.

► AA LOCAL DATABASE

The local database's implementation is an XML file in this version of the system:

- To download the image of the current database press "*Download Current*" button and the web browser will download the XML file, named ***_config_AA.xml***. This file can be easily viewed or edited using a plain-text editor such as *WordPad* or *vim.*
- The "*Browse*" and "*Upload New File*" buttons allows uploading the database back to a working BS, from a previous backup or copied from another BS. This is an easy method to clone provisioning between different BS.
- The current local provisioning database may also be removed by pressing "*Clear Current*".

► AA DATABASE BACKUP

To the current state of the Local Provisioning System is always saved in an **XML** file, as explained before. When the "*Local AA*" section changes, the BS modifies automatically this file. Thus, this XML is modified with every modification in the provisioning system.

Due to this, there is another possibility to save the current state of the AA: making a System Backup. When performing this action (pressing the "*Backup Now*" button), the current state of the system will be saved in a **.BKP** text file. If an involuntary change is applied to the provisioning system, the XML file will change too, but not the Backup file. This means that it is possible to have a Backup copy of a previous state of the system. In addition, the last backup can also be downloaded to the computer by pressing "*Download Backup*", and uploaded back again like explained in the "Local AA Database" section.

NOTE

To upload a Backup XML file to the unit using the "Upload New File", remember to change the extension from .BKP to .XML.

Adding new user

To add a new user to the local data base, just click the "*Add SS*" button in the provisioning main view. The dialog in Figure 51 will be shown.

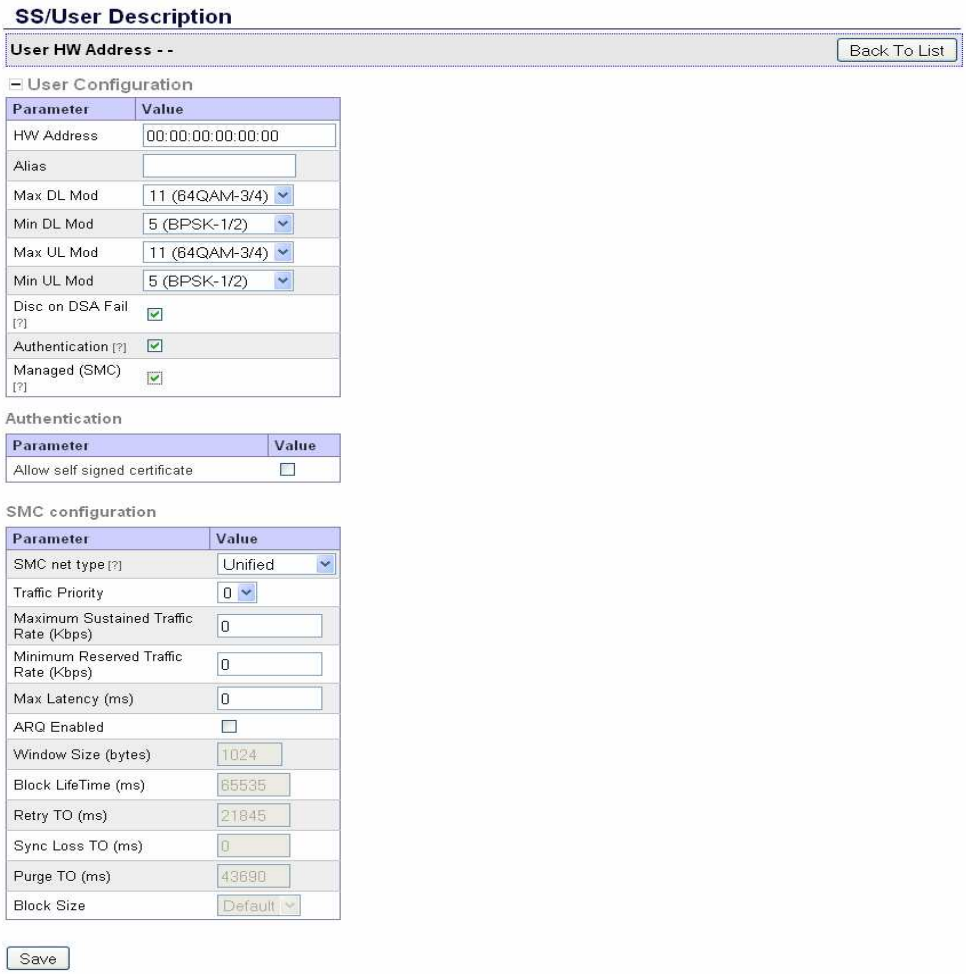


Figure 51 - Adding new user

This dialog allows the operator to add a new user to the database. The parameters are structured in the following blocks:

► **USER CONFIGURATION**

- **HW Address (mandatory):** it refers to the MAC address of the new SS. This is the unique required field in this dialog.
- **User alias (optional):** it indicates a user defined text string that is used as an alias to the HW address. This is an optional field.
- **Max/Min DL Modulation (optional):** when these limits are set to other than the default values, the user is bound to use those modulations as most/least robust ones in the downlink direction of the link. These are optional fields.
- **Max/Min UL Modulation (optional):** when these limits are set to other than the default ones, the user is bound to use those modulations as most/least robust ones in the uplink direction of the link. These are optional fields.
- **Disc on DSA Fail (recommended):** when this field is activated, if the maximum number of opportunities to create a service flow (DSA retries) is exceeded, the SS will be dropped from the BS instead of being added without service flows. After being dropped the SS will try to start again the registering process.
- **Authentication:** RSA authentication will be performed if supported by the remote equipment. There are advanced options when selected explained below.
- **Managed (SMC):** Secondary Management Channel will be negotiated if supported by the remote equipment. The configuration parameters are described below.

► **AUTHENTICATION**

- **Allow self signed certificate:** if enable, the CPE does not need to be certified by the chain of truth of the Base Station. (This option is by default disabled for more security).

► **SMC CONFIGURATION**

- **SMC net type:** there are two possible modes:
  - Unified: both data and management traffic share the same wethX virtual interface, but use different services. Traffic addressed to the user HW address will use an additional secondary management service different from the provisioned data flows.
  - Out of band: an independent methX interface is created for management traffic. Traffic addressed to the user HW address will use the secondary management connection and device, whereas any other traffic will use the data services.
- **Traffic priority:** it indicates de priority of the management traffic, from 0 to 7.
- **Max/Min Sustained Traffic Rate:** allows setting the maximum and minimum management traffic rate in kbps.
- **ARQ Enabled:** this checkbox allows enabling the ARQ. If active, some parameters regarding the ARQ can be set. They are explained bellow in section 3.16.3.

Once all the data is filled, clicking the "*Save*" button the new user will be added to the database.

Adding a new group of users

When referring to a group, the only difference is that it is necessary to provide SS base and mask MAC addresses instead of a unique SS MAC address.

To add a new group of users to the local data base, click in the "*Add Group*" button in the provisioning main view. The dialog in Figure 52 will be shown.

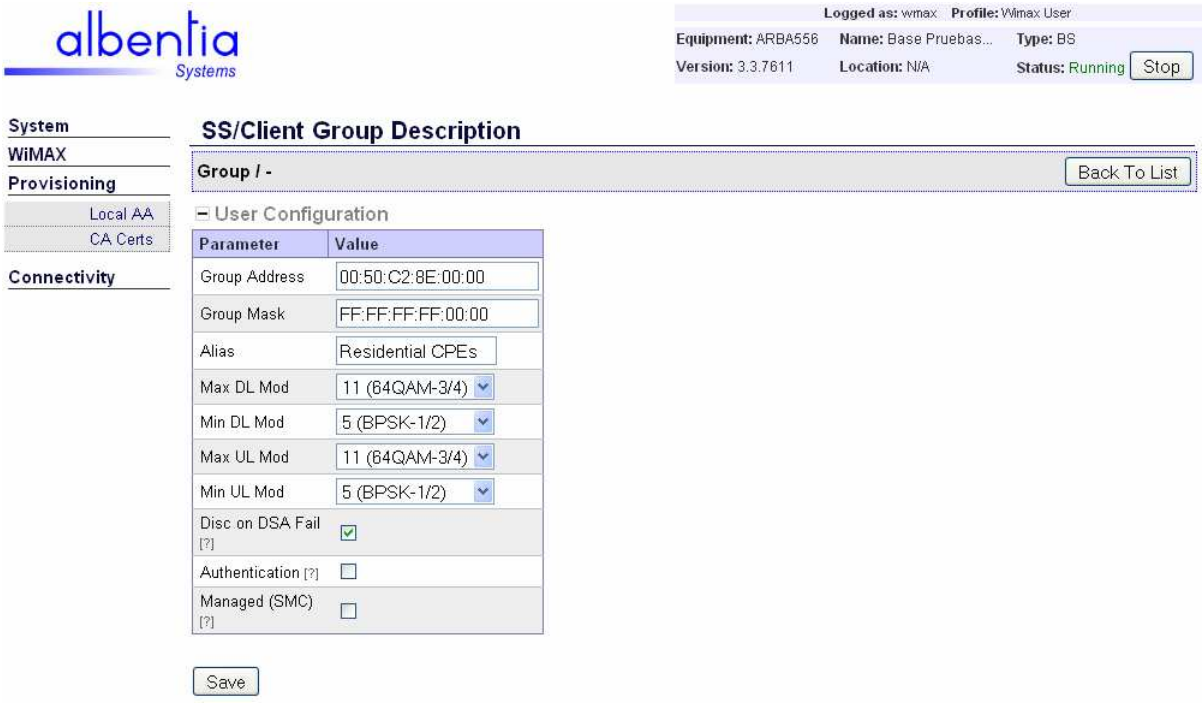


Figure 52 - Adding new group

NOTE

In the "*Cell Setup*" section, the "*Check Hardware Address*" field allows to enable/disable this authentication control in the Initial Ranging. When this field is disabled, all SSs in the operation range of the BS will be accepted and will enter the cell, but no user flows will be provisioned, so communication with SSs will not be possible.

There is another possibility to allow every SS entering the cell, assigning service flows to them. This can be performed using the "Add EVERYBODY" button which creates a new group with the less restrictive MAC Address condition:

-Group Address: 00:00:00:00:00:00

- Group Mask: 00:00:00:00:00:00

With this configuration, all SS in the operation range of the BS will be accepted and connected to the cell. In addition, if service flows are provisioned to this group, all SS will be provisioned with those user flows.

Copying an existing user / group

When two or more users or groups are going to be provisioned in the same way, the provisioning system provides a tool to make copies of a previously provisioned user or group.

In the "*Local_AA*" section, every row representing a user or group includes a button labelled "*Copy*". When clicked, the dialog in Figure 53 will be shown.

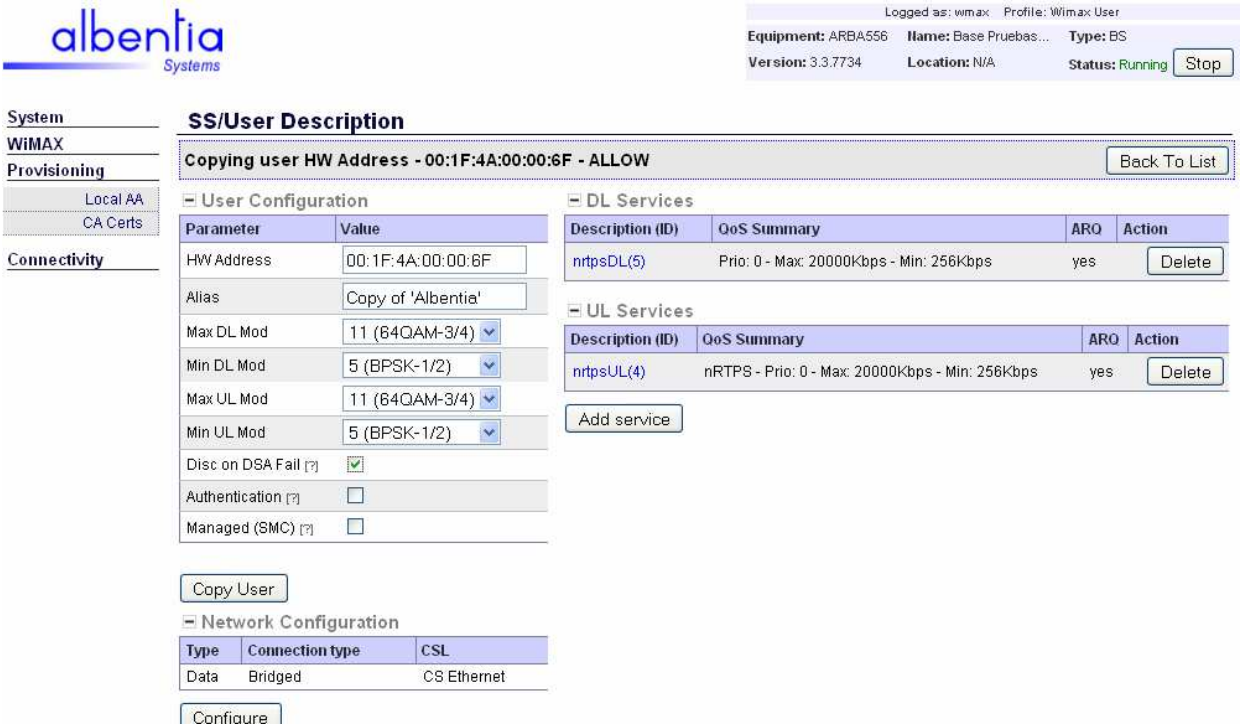


Figure 53 - Copying an existing user

This dialogue allows the operator to set the new HW address and to change any other parameter. Once the "*Copy*" button is clicked the new user is added to the database. Note that de service flows and network configuration are also copied.

This process can be performed similarly for groups of users; where at least the base and mask MAC addresses should be modified.

NOTE

If the user/group has been provisioned with data services or if it has defined a specific network configuration, these parameters will also be copied to the new user/group.

Modifying an existing user / group

Provisioned items may also be modified. In the main provisioning dialog, the different users and groups are listed as rows of the provisioning table. Every "*SS MAC Address*" field links to the "*Edit Dialog*" dialogue, as shown in Figure 54.

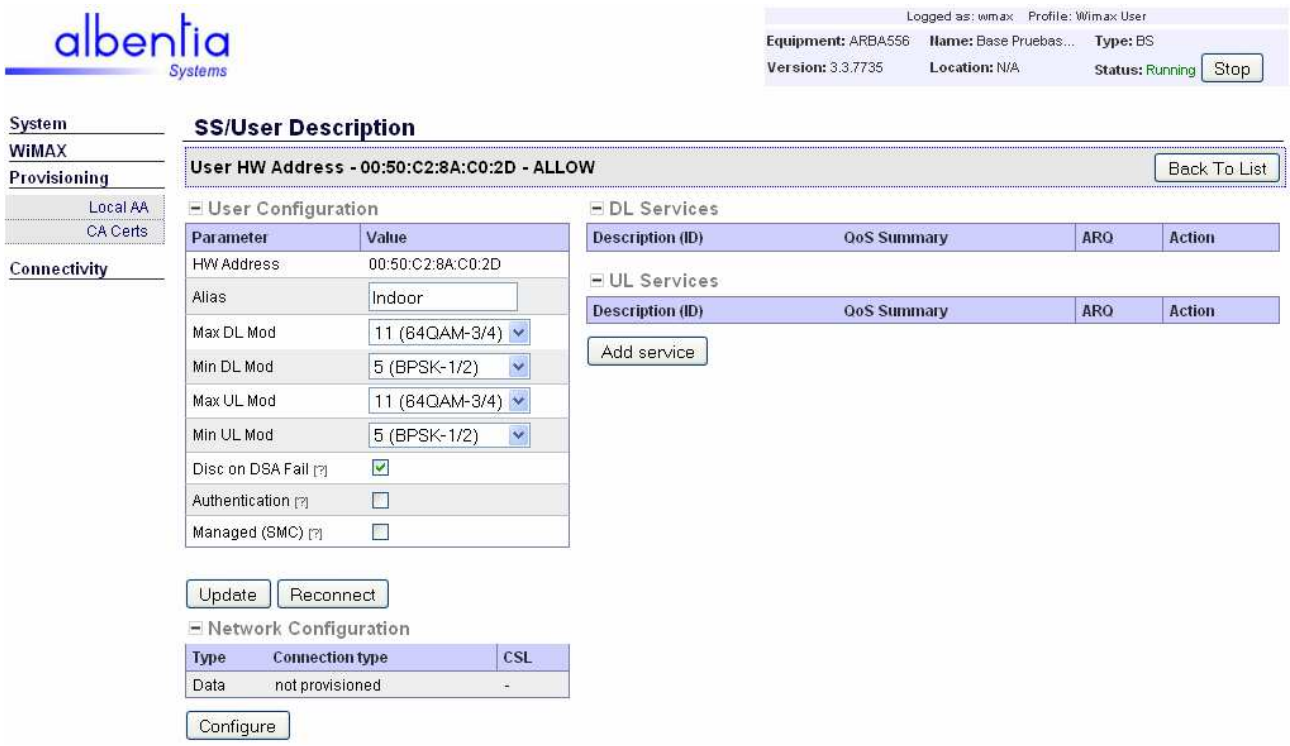


Figure 54 - User modification screenshot

If any of the parameters of the user or group needs to be changed, modify the correspondent field and then click the "*Update*" button. This dialog also allows adding new provisioned flows, as it will be explained in the following points.

⚠ ATENTION!

Remember that any change made to an active user is only stored in the database and not applied to the active users. If the user is active, the "*Reconnect*" button is shown. Clicking this button forces the active SS to drop from the cell and to reconnect. In this new reconnection all the modified parameters will be taken into account by the system

3.16.3. Data Service provisioning

Once the users have been defined and provisioned, the next step should be to create the appropriate *Service Flows* for each user. These flows are also provisioned in the BS, using the "*Local AA*" section. When a provisioned SS enters the cell, the BS queries the local provisioning system about services provisioned for it. If the local database has service descriptors for the user, those will be allocated using WiMAX mechanisms on the air.

The local provisioning system and its front-end allow the operator to add, remove and modify services for a provisioned user or group. To get to the main provisioning dialog, proceed as it follows:

1. Get into the provisioning main dialog by browsing BS web and then click on the "*Local AA*" button on the main menu.
2. Select the user or group that needs to be provisioned with services and click on the link included in the MAC Address.

The *Service Provisioning* dialog, unique for each user or group, is shown in Figure 54. Information referring to the flows will be displayed in the "*Provisioned Flows*" table. A quick description of the existing flows will be displayed as a row inside this table.

Important notes about data services

There are some important points about services that must be noted:

- **Services are unidirectional:** As the *IEEE802.16-2009/5* states, data flows are unidirectional. That means that a service flow can only transport data either in the downlink or in the uplink, but not both at the same time.
- **Direction of a service:** In the provisioning system, the service direction is noted as Tx or Rx. This means Tx or Rx as seen from the BS. Thus a Tx provisioned service will transport data in the downlink, and an Rx provisioned service will transport data in the uplink. For any bidirectional communication, two service flows are needed.
- **QoS of a service:** QoS is independent by service. Each service has its own QoS parameters, so the UL and DL service flows of a communication do not have to be necessarily provisioned in the same way.

NOTE

In this document and in the ARBA135 interface, the terms "*Data service*", "*Data Flow*", "*Service Flow*" and "*Flow*" are used as synonyms.

Adding a new service

To add new services get into the "*Service Provisioning*" main dialog and click in the link inside the MAC address of the current SS. Then press the "*Add provisioned flow*" button link to show the "*Flow Description"* dialog, as shown in Figure 55.

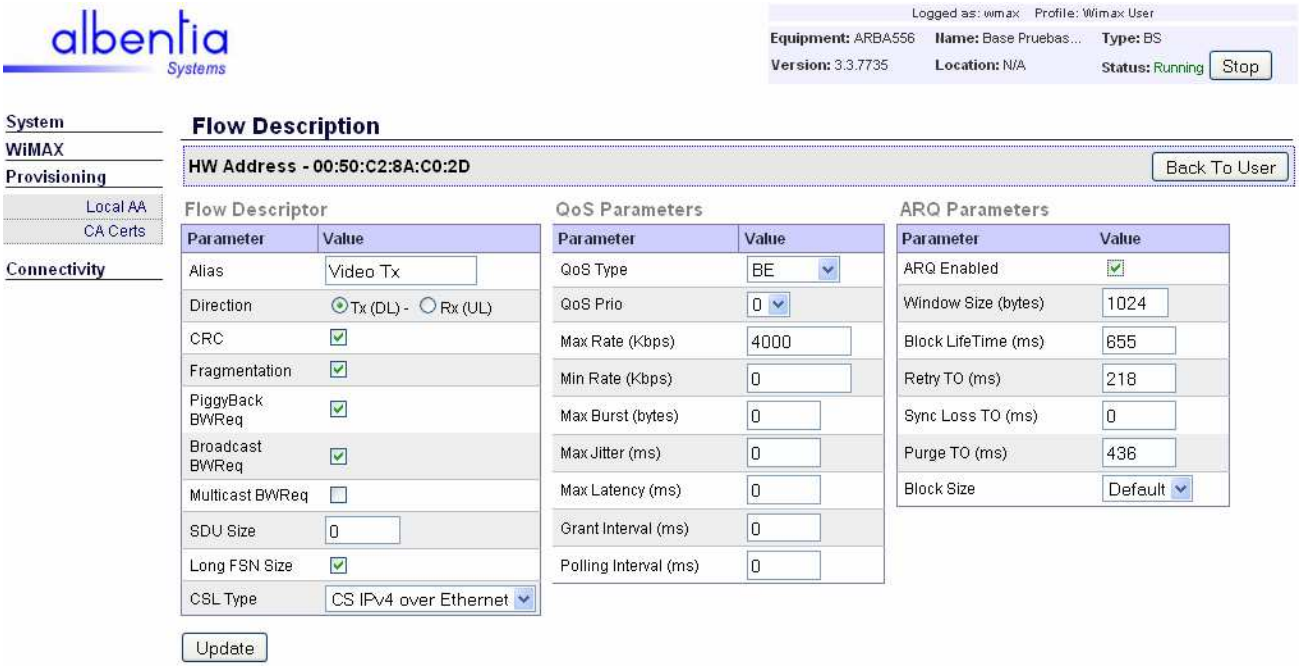


Figure 55 - "*Flow Description*" menu

This dialogue allows the operator to change the QoS parameters such as the guaranteed traffic rates or the peak traffic rates of the new provisioned service flow. Once all the parameters have been correctly set, the "*Update*" button will add the new service to the local database.

This section is divided into 4 main blocks: *"Flow Descriptor*", "*QoS Parameters*", "*ARQ Parameters*" and "*CS Descriptor*". They will be explained in the following.

- **FLOW DESCRIPTOR**

  - **Alias**: it gives an alias to the current flow (optional).
  - **Direction**: selectable between TX and RX, it indicates the direction of the flow (mandatory).
  - **CRC (*Cyclic Redundancy Check*)**: MAC PDUs may include an optional CRC fragment at the end. This checkbox activates/deactivates this feature.
  - **Fragmentation**: fragmentation is the process by which a MAC SDU is divided into one or more MAC PDUs. This process can be necessary in order to accomplish QoS requirements of a connection's service flow. The authority to fragment traffic on a connection is defined when the connection is created by the MAC SAP. Fragmentation may be initiated by a BS for downlink connections and by an SS for uplink connections. This checkbox activates/deactivates this feature. For non-ARQ connections, fragments are transmitted once and in sequence. The sequence number assigned to each fragment allows the receiver to recreate the original payload and to detect the loss of any intermediate packets. For ARQ-enabled connections, fragments are formed for each transmission by concatenating sets of ARQ blocks with adjacent sequence numbers.
  - **Piggyback Bandwidth Request**: Requests refer to the mechanism that SSs use to indicate to the BS that they need uplink bandwidth allocation. A Request may come as a stand-alone bandwidth request header or it may come as a *Piggyback* Request. Certain services need to request bandwidth before transmitting data. There are two mechanisms to request bandwidth: either an absolute request (standalone) or a *Piggyback* request. The capability of *Piggyback* Request is optional. This checkbox activates/deactivates this feature.
  - **Broadcast Bandwidth Request**: this field allows the use of the broadcast channel to send BW requests for the current flow.
  - **Multicast Bandwidth Request**: when users are divided into groups, this field will activate multicast bandwidth requests, which will be only available for users belonging to that group. This procedure allows segmenting the bandwidth opportunities.
  - **SDU size**: the value of this parameter specifies the length of the SDU for a fixed-length SDU service flow. This parameter is used only if packing is enabled and the service flow is indicated as carrying fixed-length SDUs. The default value is 49 bytes.
  - **Long FSN size**: FSN (*Fragment Sequence Number*) refers to the sequence number of the current SDU fragment. This field is increased by one with each fragment, including unfragmented SDUs. The standard defines that this size could be 3-bits or 11-bits. This checkbox activates/deactivates the 11-bits size.
  - **CSL Type (Convergence Sublayer)**: as the standard states, each allocated service must have an instance of a convergence sublayer (CSL).

This is related to the type of traffic that a service can handle. All the available CSL types are those that can transport packetized traffic and are included into a higher level CS called "*Packet CS*". The main difference between selecting one CSL or another is the variety of available classifiers (for example, the "CS ETHERNET" CSL type will only be able to make filtering up to OSI-model's Layer-2). Once the flow has been created, this option is the only one that may not be modified.

► **QoS PARAMETERS**

- **QoS Scheduling Type**: The value of this parameter specifies the scheduling service that shall be enabled for the associated service flow. Scheduling services represent the data handling mechanisms supported by the MAC scheduler for data transport on a connection. Each connection is associated with a single data service, and each data service is associated with a set of QoS parameters that quantify aspects of its behaviour. Five services are supported: *Unsolicited Grant Service* (**UGS**), *Extended Real-time Polling Service* (**ErtPS**), *Real-time Polling Service* (**rtPS**), *Non-real-time Polling Service* (**nrtPS**), and *Best Effort* (**BE**). The following paragraphs provide a brief description of each of the supported scheduling services.
  - BE: this service is designed to support data streams for which no minimum service level is required and therefore may be handled on a space-available basis. Best effort delivery describes a network service in which the flow does not provide any guarantees that data is delivered.
  - nrtPS: is designed to support delay-tolerant data streams (non real time) consisting of variable-sized data packets for which a minimum data rate is required, such as high bandwidth FTP. The nrtPS offers unicast polls on a regular basis, which assures that the service flow receives request opportunities even during network congestion.
  - rtPS: it is designed to support real-time data streams consisting of variable-sized data packets that are issued at periodic intervals, such as *Moving Pictures Experts Group* (MPEG) video. The service offers real-time, periodic, unicast request opportunities, which meet the flow's real-time needs and allow the SS to specify the size of the desired grant. This service requires more request overhead than UGS, but supports variable grant sizes for optimum data transport efficiency.
  - ertPS: it is a scheduling mechanism that builds on the efficiency of both UGS and rtPS. The ertPS is designed for real-time traffic with variable data rate (such as VOIP service with silence suppression) over the WiMAX network.
  - UGS**:** it is designed to support real-time data streams consisting of fixed-size data packets issued at periodic intervals, such as T1/E1 or VoIP without silence suppression. The service offers fixed-size grants on a real-time periodic basis, which eliminate the overhead and latency of SS requests and assure that grants are available to meet the flow's real-time needs.
- **QoS Priority**: this parameter, also known as "*Traffic Priority*" in the standard, specifies the priority assigned to a service flow. Given two service flows with identical QoS parameters, the higher priority service flow should be given lower delay and higher buffering preference. For otherwise non-identical service flows, the priority parameter should not take precedence over any conflicting service flow QoS parameter. Selectable from 0 to 7, higher numbers indicate higher priority.

- **Maximum Rate**: this parameter, related with the "*Maximum Sustained Traffic Rate*" parameter in the standard, defines the peak information rate of the service. The rate is expressed in *kilobits per second* and pertains to the SDUs at the input to the system. Explicitly, this parameter does not include MAC overhead such as MAC headers or CRCs. This parameter does not limit the instantaneous rate of the service since this is governed by the physical attributes of the ingress port. This field specifies only a bound, not a guarantee that the rate is available.
- **Minimum Rate**: this parameter, related with the "*Minimum Reserved Traffic Rate*" parameter in the standard, specifies the minimum rate reserved for this service flow. The rate is expressed in *kilobits per second* and specifies the minimum amount of data to be transported on behalf of the service flow when averaged over time. The specified rate shall only be maintained when sufficient data is available for scheduling. When insufficient data exists, the requirement imposed by this parameter shall be satisfied by assuring that the available data is transmitted as soon as possible. The BS shall be able to satisfy bandwidth requests for a service flow up to its *Minimum Rate*. If less bandwidth than its *Minimum Rate* is requested for a service flow, the BS may reallocate the excess reserved bandwidth for other purposes. The aggregate *Minimum Rate* of all service flows can exceed the amount of available bandwidth. If this parameter is omitted, then it defaults to a value of 0 bits per second (no bandwidth is reserved for the flow).
- **Maximum Burst**: this parameter, also known as "*Maximum Traffic Burst*" in the standard, defines the maximum burst size that shall be accommodated for the service, expressed in *bytes*. Since the physical speed of ingress/egress ports, the air interface, and the backhaul will, in general, be greater than the maximum sustained 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 Jitter**: this parameter, also known as "*Tolerated Jitter*" in the standard, defines the maximum delay variation for the connection. It is expressed in *milliseconds*.
- **Maximum Latency**: this parameter, also known as "*Maximum Latency*" in the standard, specifies the maximum latency between the reception of a packet by the BS or SS on its network interface and the forwarding of the packet to its RF Interface. If defined, this parameter represents a service commitment (or admission criteria) at the BS or SS and shall be guaranteed by the BS or SS. A BS or SS does not have to meet this service commitment for service flows that exceed their minimum reserved rate. It is expressed in *milliseconds*.
- **Grant Interval**: the BS will give a SS the bandwidth requested ate lest every "*Grant Interval*" time.
- **Polling Interval**: it sets the maximum interval the BS will wait before making a Poling request, asking that user for bandwidth requests.

► ARQ PARAMETERS

ARQ (*Automatic Repeat Request*) is a communication protocol in which the receiving device detects errors and requests retransmissions. When the receiver detects an error in a packet, it automatically requests the transmitter to resend the packet. This process is repeated until the packet is error free or the error continues

beyond a predetermined number of transmissions. ARQ may be used in WiMAX communications to guarantee data integrity.

The ARQ mechanism is a part of the MAC, which is optional for implementation. When implemented, ARQ may be enabled on a per-connection basis. The per-connection ARQ shall be specified and negotiated during connection creation. Similar to other properties of the MAC protocol, the scope of a specific instance of ARQ is limited to one unidirectional connection.

A distinct unit of data is carried on an ARQ-enabled connection. Such a unit is assigned a sequence number, and is managed as a distinct entity by the ARQ state machines. Block size and other related parameters will be negotiated during connection establishment.

This section allows enabling the ARQ mechanism for the current flow as long as to modify some related parameters. However, *Albentia Systems* recommends using the default parameters, which will be automatically calculated to be the more efficient ones for the current flow. The parameters are explained in the following points:

- **"*ARQ Enabled*" checkbox**: it indicates whether or not ARQ use is requested for the current service flow.
- **Window Size**: it is the maximum number of unacknowledged ARQ blocks at any given time. (An ARQ block is unacknowledged if it has been transmitted but no acknowledgment has been received).
- **Block Life Time**: it is the maximum time interval an ARQ block shall be managed by the transmitter ARQ state machine, once initial transmission of the block has occurred. If transmission (or subsequent retransmission) of the block is not acknowledged by the receiver before the time limit is reached, the block is discarded.
- **Retry Timeout**: it is the minimum time interval a transmitter shall wait before retransmission of an unacknowledged block for retransmission. The interval begins when the ARQ block was last transmitted.
- **Sync Loss Timeout**: it is the maximum time interval ARQ_TX_WINDOW_START or ARQ_RX_WINDOW_START parameters shall be allowed to remain at the same value before declaring a loss of synchronization of the sender and receiver state machines when data transfer is known to be active. The ARQ receiver and transmitter state machines manage independent timers. Each has its own criteria for determining when data transfer is "active".
- **Purge Timeout**: it indicates the time interval the receiver shall wait after successful reception of a block that does not result in advancement of ARQ_RX_WINDOW_START value, before advancing to a new ARQ_RX_WINDOW_START.
- **Block Size**: it indicates the length used for partitioning an SDU into a sequence of ARQ blocks prior to transmission.

NOTE

When using service flows with ARQ, it is necessary that both BS and SS support the implementation of this mechanism.

NOTE

ARQ is referred to unidirectional flows, what means that it may be applied only in one direction (Uplink or Downlink).

► CS DESCRIPTOR

Once the flow has been created, in the "*Flow Description*" dialog this new section will appear in the down side of the screen (squared in yellow in Figure 56). From this section, the flow classifiers can be added and modified. This operation will be next explained in more detail.

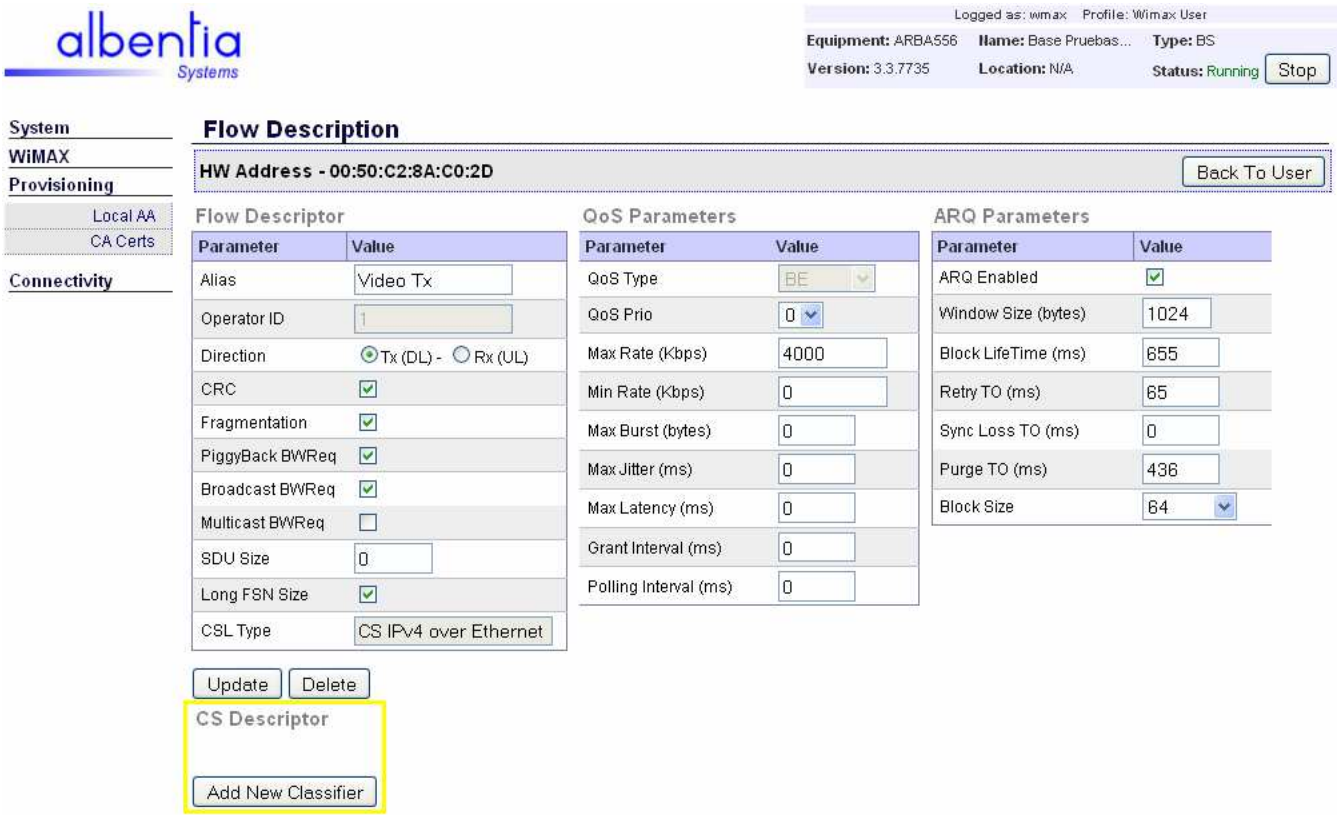


Figure 56 - "*CS Descriptor*" section

▪ Data filtering with flows: Classifiers

The *WiMAX* systems allow the data to be filtered by certain criteria and mapped to specific flows, so that QoS might be different depending on the traffic types. This is done by the *Classifiers* mechanism, which will be associated to the convergence sublayers of the flow.

Once a new service has been provisioned, classifiers can be added to the service so that only the desired traffic is transported through it. To do this, get into the "*CS Description*" section and click into the "*Add New Classifier*" button. In Figure 57 and Figure 58 different "*Classifier Description*" dialogues can be observed.

NOTE

The available *Classifiers* will be different depending on the selected Convergence Sublayer, so only some matching criteria can be selected according to the selected CSL type. For example, a "CS IPv4overEthernet" CSL type will offer much more possibilities than a "CS Ethernet" CSL Type.

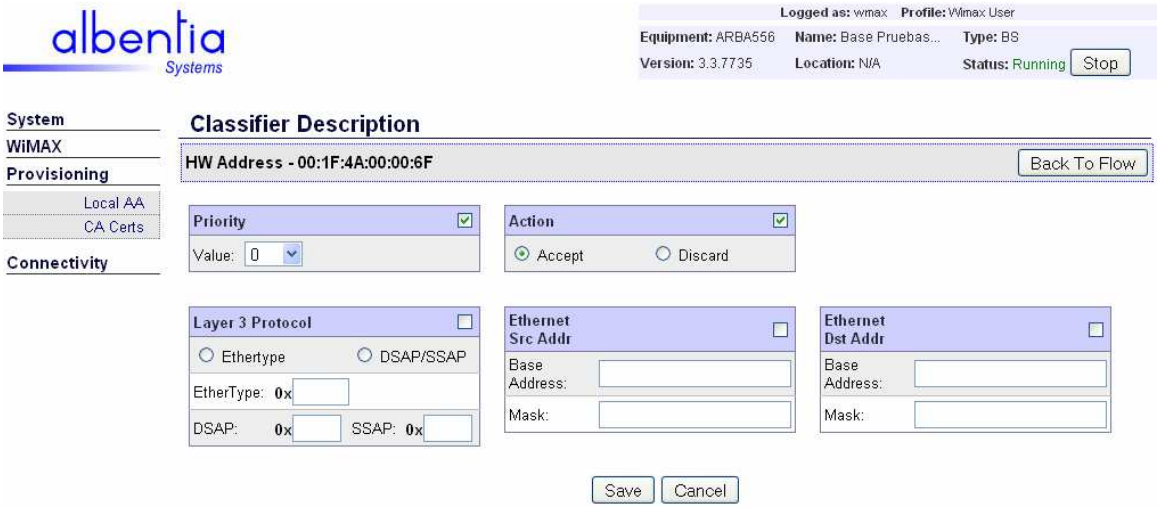


Figure 57 - Classifier Description over a "*CS Ethernet*" CSL type

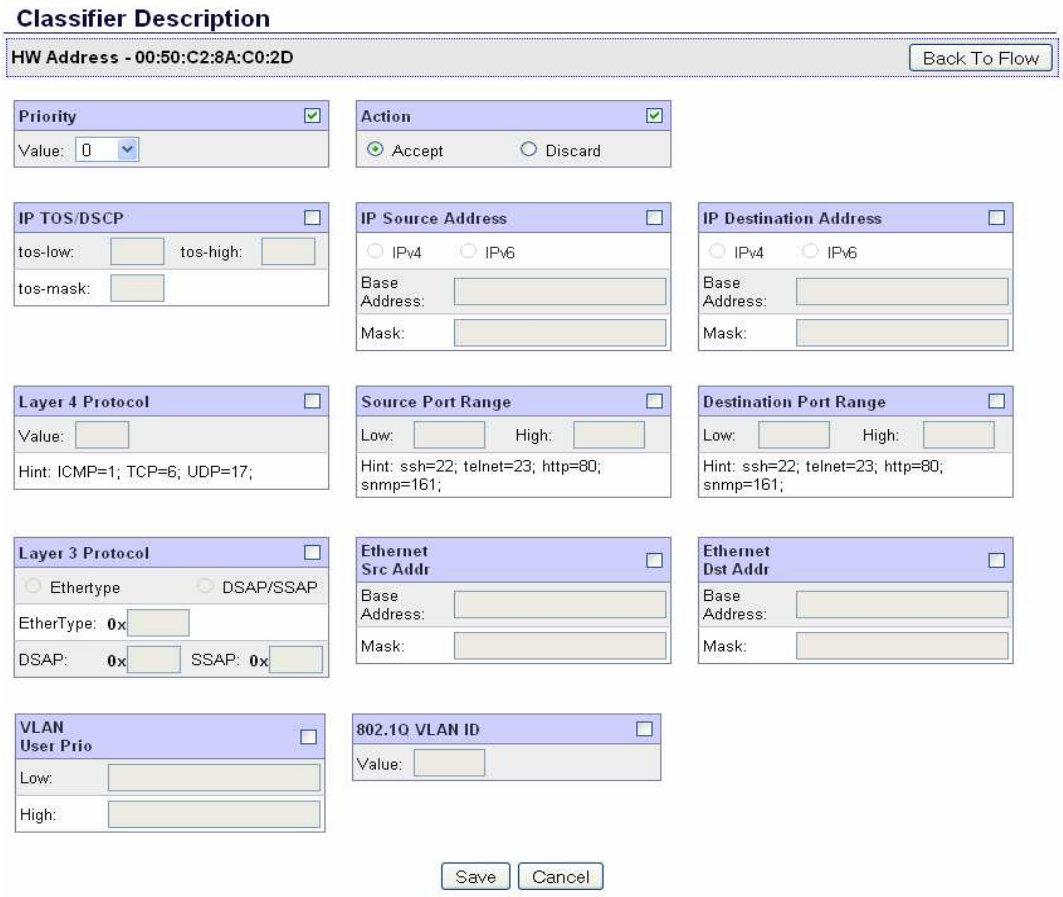


Figure 58 - Classifier Description over a "*CS IPv4overVLAN*" type

The classification rules are various: "*Destination/Source IP address*", "*Destination/Source MAC Address*", "*Destination/Source Port range*", "*TOS field*", "*VLAN User priority*"… giving the operator a great filtering flexibility. They are all described in Table 13.

Classifier	Description	CSL type
IP TOS/DSCP	*The IPv4 frame header includes an 8-bit "Type of Service" field that specifies the parameters for the requested service to perform Layer-3 QoS. The bits are structured as follows: Bits 7-5:* ***Precedence****, Bit 4: Delay, Bit 3: Throughput, Bit 2: Reliability, Bits 1-0: not-used.* *Later the TOS was redefined to the DSCP value (Differentiated Services Code Point, as in RFC2474 and RFC2475). Routers that support DiffServ use this DSCP value to select per-hop behaviour and provide the appropriate Layer-3 QoS service to traffic. The bits are structured as follows: Bits 7-2****: DiffServ Codepoint*** *(DC), Bits: 1-0: ECN (Explicit Congestion Notification).* *DC field in DSCP is backwards compatible with TOS precedence field. When converting between TOS precedence and DSCP, match the three most significant bits. For instance: TOS Precedence 5 (101) maps to DSCP DC 101 000.* This classifier filters by the 8-bit "*Type*" field on the Layer-3 protocol frame header, both for TOS and DSCP. **Selection**: a filtering range can be selected defining the lower and the higher margins (TOS-Low and TOS-High), expressed in decimal notation. A TOS *Mask* should be defined, also in decimal notation, to select the bits that are going to be filtered. TOS Low/High values and TOS Mask will be combined with an AND logical operation, resulting the TOS final filtering value, whereas: $TOS_{MIN} \leq TOS_{pckt} \& TOS_{MASK} \leq TOS_{MAX}$ **Note**: *operator should understand properly the TOS/DSCP fields and its bit distribution in order to use this classifier properly.*	**IPv4** **IPv4overVLAN**
IP Source Address	It filters by the "*Source address*" field on the Layer-3 protocol frame header. **Selection**: The filtering IP address range will be defined with a *Base Address* and a *Mask Address,* performing a logical AND operation, whereas: $\mathbf{Filter\_IP = IP_{BASE\_ADDRESS} \& IP_{MASK}}$ For example when filtering by a unique IP address, the mask should be 255.255.255.255. In addition, the address format should be specified (IPv4 or IPv6).	**IPv4** **IPv4overVLAN**
IP Destination Address	It filters by the "*Destination address*" field on the Layer-3 protocol frame header. **Selection**: similar as explained before in the "*IP Source Address*" classifier.	**IPv4** **IPv4overVLAN**
Layer-4 Protocol	It filters by the type of transport protocol that is being used,	**IPv4**

	as specified in the 8-bit "*Protocol*" field on the Layer-3 frame header. The IANA (*Internet Assigned Numbers Authority*) is a regulatory entity that has defined the Internet Protocol Numbers. Thus, every Layer-4 protocol is defined with a numerical value: ICMP = 1, IGMP = 2, TCP = 6, UDP=17… **Selection**: the protocol number should be specified, expressed in decimal notation.	**IPv4overVLAN**
Source Port Range	It filters by the "*Source Port*" field as specified in the Layer-4 protocol frame header. **Selection**: a filtering range can be selected defining the lower and the higher margins in decimal notation. To filter a unique port, both low and high values should be the same.	**IPv4** **IPv4overVLAN**
Destination Port Range	It filters by the "*Destination Port*" field as specified in the Layer-4 protocol frame header. **Selection**: a filtering range can be selected defining the lower and the higher margins in decimal notation.	**IPv4** **IPv4overVLAN**
Layer 3 Protocol	It filters by the Layer-3 protocol specified in the Ethernet frame header. Filtering can me made using the *Ethertype* or the *DSAP/SSAP* fields: • "*Ethertype*" refers to the 2-byte "*Type*" field of the Ethernet frame header as defined by the Ethernet II framing networking standard. It is used to indicate which upper-layer protocol is encapsulated in the frame data. Each upper-layer protocol is identified by a 2-byte code (i.e.: IPv4 = 0x0800, ARP = 0x0806, 802.1q = 0x8100, IPv6 = 0x86DD…). • In the original IEEE 802.3 Ethernet standard, the frame header includes a part belonging to the IEEE 802.2 standard (LLC). Amongst them, there are the one-byte DSAP and SSAP fields. DSAP (*Destination Service Access Point*) indicates the service to which the LLC data unit is being sent, and SSAP (*Source Service Access Point*) indicates the service from which the LLC data unit is sent. **Selection**: first choose between "*Ethertype*" or "*DSAP/SSAP*" options, and then specify the adequate protocol number, expressed in hexadecimal notation.	**All**
Ethernet Source Address	It filters by the "*Source Address*" field in the Ethernet **IEEE 802.3** frame header. **Selection**: The filtering MAC address range will be defined with a *Base Address* and a *Mask Address,* performing an AND logical operation, whereas: **Filter_MAC = $MAC_{BASE\_ADDRESS}$ & MAC_{MASK}**	**All**
Ethernet Destination Address	It filters by the "*Destination address*" field in the Ethernet **IEEE 802.3** frame header. **Selection**: similar as explained before in the "*Ethernet Source Address*" classifier.	**All**
VLAN User Priority	*VLAN (Virtual Local Area Network) is a technique which allows the logical segmentation of different LANs into*	**VLAN** **IPv4overVLAN**

	multiple virtual LANs, or the creation of a unique logical LAN from physically segmented LANS. The protocol used in configuring VLANs is ***IEEE 802.1q****.* *Every packet belonging to a VLAN should be identified in some way (tagged). The* ***IEEE 802.1q*** *protocol specifies that when using VLANs, a tag should be added to the Ethernet frame header of every packet, including a three-bit "User Priority" field and a twelve-bit "VLAN Identifier-VID".* This classifier filters according to the three-bit "*User Priority*" field in the VLAN tag of every packet. **Selection**: a filtering range can be selected defining the lower and the higher margins, expressed in decimal notation.	
802.1q VLAN ID	This classifier filters according to the twelve-bit "*VLAN identifier*" field in the VLAN tag of every packet. **Selection**: the desired VLAN_ID value should be specified in decimal notation.	**VLAN, IPv4overVLAN**

Table 13 - Classifiers

There are two additional fields that are interesting and should be explained:

- **Priority**: when the BS is connected to a SS, all the different classifiers for the current network interface are stored in the CSL in some kind of list. When the BS wants to send a packet, it will sequentially check all the current classifiers in that list, and the data will be assigned to the first matching classifier's service flow. With the "*Priority*" parameter, it is possible to increase the priority of a classifier, so it gets higher in this classifiers' list. In conclusion, the BS will first check the filtering rules of the higher priority classifiers.
- **Action**: this field allows creating "*discarding flows*". The default value of this field will be "*Accept*", so the packets compliant with the filtering rules will be transmitted over the suitable service flow. On the other hand, selecting "Discard", all the packets compliant with the filtering rules will be discarded and dropped, so they will not be transmitted to the air.

There is also the possibility to select different filtering conditions following **AND** or **OR** rules. This can be explained with an example: if a unique classifier is created with both *"Destination IP Address*" and a "*TOS field*" rules, the BS will understand this as an *AND* condition: only the packets with that destination IP Address AND with the specified TOS values will be compliant with this classifier.

On the other hand, if two different classifiers are created, one with the "*Destination IP Address*" rule and another one with the "*TOS field*" rule, the BS will perform an OR condition: both the packets with that destination IP Address OR with the specified TOS values will be compliant with this classifier.

▪ Deleting an existing flow

Data flows may also be deleted or de-provisioned. To do this just get into the "*User Description*" dialog, choose the required flow and click "*Delete*" button.

3.16.4. Network provisioning

Network provisioning is a powerful functionality which allows to completely managing the networking configuration of all the active SSs. In other wireless systems (such as *Wi-Fi*), the Master node has a unique wireless interface to communicate with all the registered clients. Every networking configuration related to this interface, such as the operation mode or the IP routes, will be applied to all the managed hosts. This means that if the Master node's wireless interface is operating in bridging mode, all the clients should operate in bridging mode (as they will be connected to this shared-bridged-and-unique wireless interface).

In the ARBA Base Station, by contrast, there are **different and independent virtual wireless interfaces for each SS**. When a SS is registered in the cell, the BS will automatically create a virtual wireless interface (called *wethx*) to communicate with that user. This means that the BS has the possibility of configuring independently the networking mode of each SS. It would be possible to use the three different networking modes simultaneously (*Routing*, *Bridging* and *Local Network*) for different SSs connected simultaneously to the BS.

When a user has been provisioned with at least one service flow, the "*Network Configuration*" block will appear in the "*User/Group Description*" sub-menu. This block is highlighted in blue in Figure 59. When pressing the "*Configure*" button, the "*SS Network Configuration*" menu will be opened. As explained before, at network layer this equipment supports three main operation modes. These models will be briefly described below.

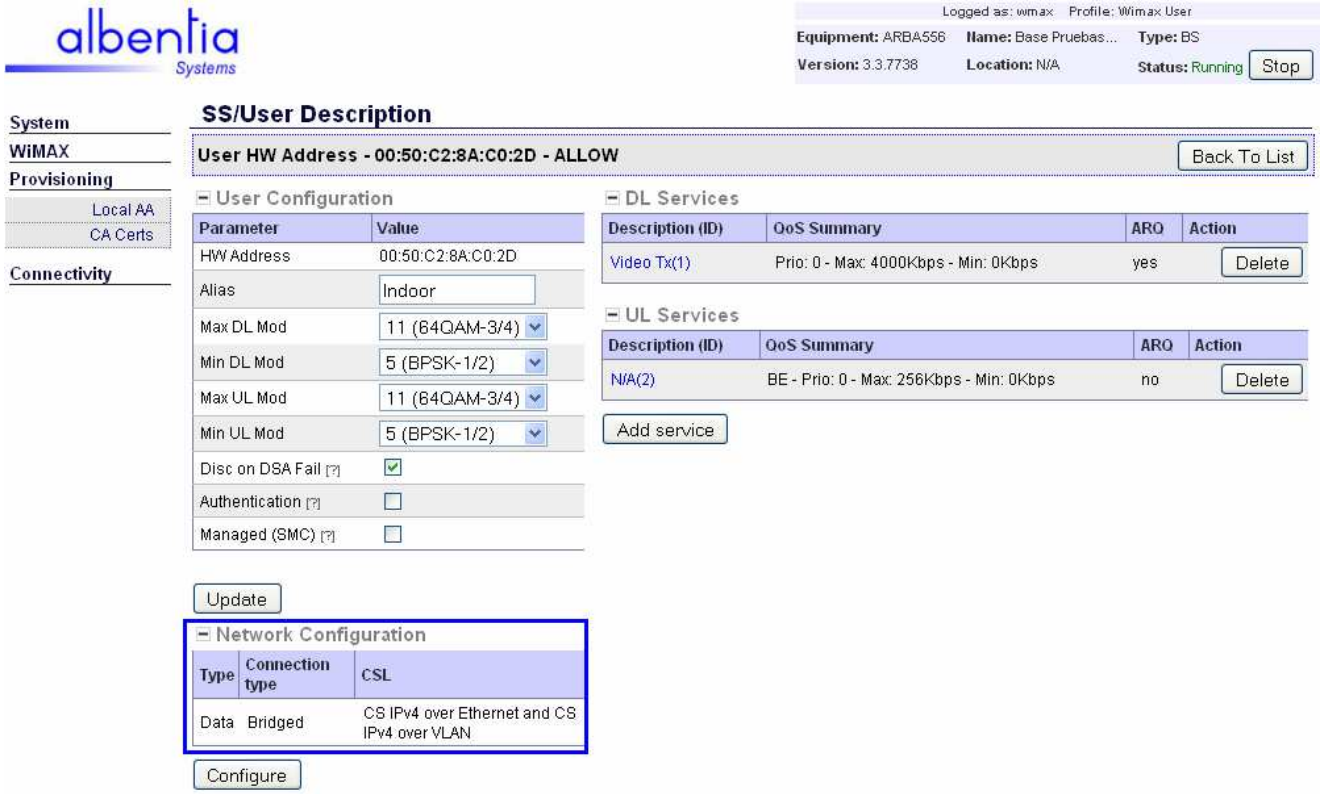


Figure 59 - "*Network Configuration*" provisioning block

- Bridging Mode

ARBA135 unit incorporates the possibility of performing transparent *Bridging* at Layer-2. In this mode, the *wethX* wireless interface is transparently bridged to the

defined logic bridge. All the traffic will flow at Layer-2 between all the interfaces belonging to that bridge. If a wired/VLAN interface is also added to that bridge, the user will have transparent access to the network.

It is a *Plug&Play* networking mode which does not need additional routing configuration, so it is probably the easiest networking mode available. The creation and configuration of a bridge in the BS is performed in the "*Bridging Setup*" section, as explained in paragraph 3.19. After creating a bridge, the operator may select in the network provisioning the adequate bridge to which the SS will be associated.

A schematic view of the *Bridging* architecture is shown in Figure 60, in order to illustrate a possible scenario that could use this mode. In this case, and being compliant with the *Bridging* concept, two networks with the same network mask will be connected by means of two *WiMAX* units. Both networks will work in the domain 192.168.2.0/24. The *Bridge*'s advantage is its simplicity an its *Plug-and-Play* feature, since once it is created and configured it will not be necessary to configure anything more, and the wireless link will be a transparent bridge which will communicate both sub-networks in a fully transparent way. It will not be necessary to add manually any route to the WiMAX units and neither to any other network equipment in the network, what makes this mode very interesting.

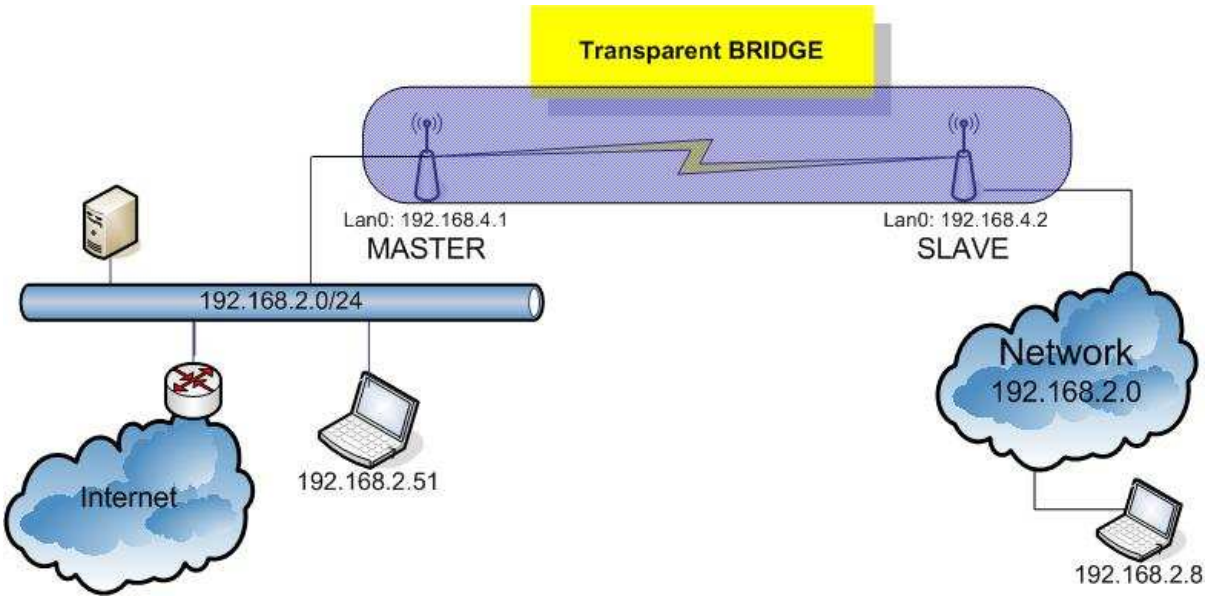


Figure 60 - Example of architecture with *Bridging* mode

This operation mode is selected in the "*CPE Network Configuration*" screen, selecting **Bridged** as the desired networking mode. If this mode is selected, the "*Bridge Mode Configuration*" block will be displayed, as shown in Figure 61. As explained before, Bridging mode is extremely easy to configure. The only thing the user should fix is the bridge to which the SS should connect. If there is only one unique bridge, the SS will be associated to it automatically. After configuring this, press the "*Update*" button and the changes will be automatically saved in the Local AA database.

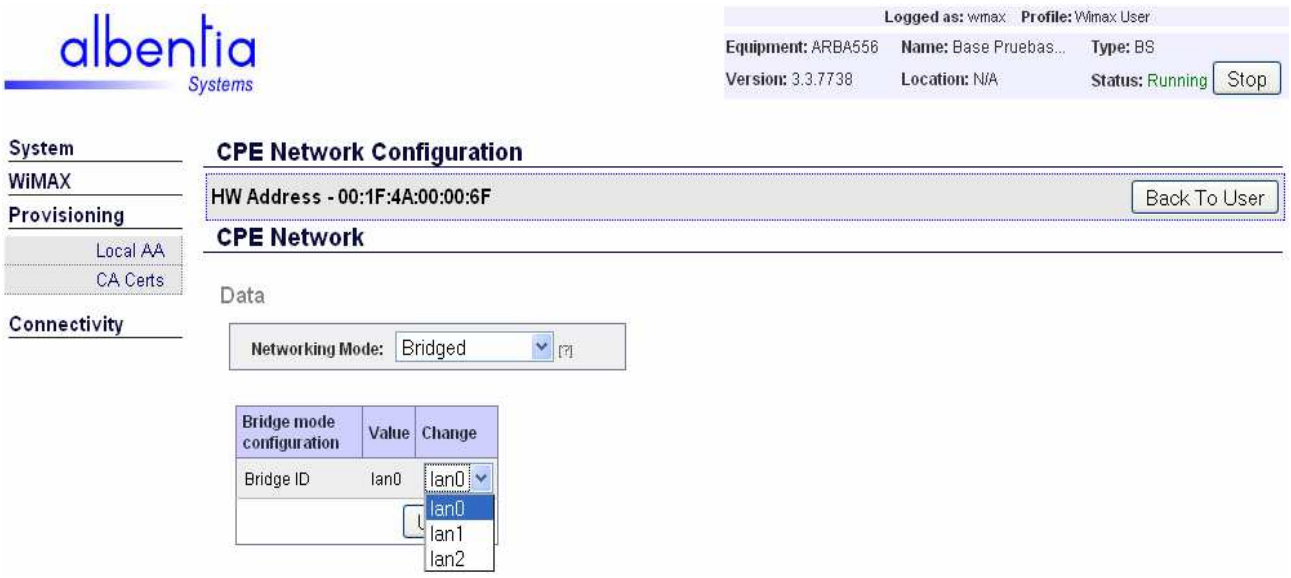


Figure 61 - CPE Network Configuration - Bridging mode

NOTE

The Bridging mode will be the Default provisioned networking mode, so if the network configuration of a SS is not manually configured, the BS will try to operate in Bridging mode with the first created bridge.

Bridged VLAN Mode

In "Bridged VLAN" mode the "*wethX*" interface is allowed to have up to four different VLAN devices, each one defined by a VLAN tag. Like Bridged mode, all the traffic of this VLAN device will flow at layer 2 between all the interfaces in the logic bridge defined and provisioned next to the VLAN tag (see Figure 62).

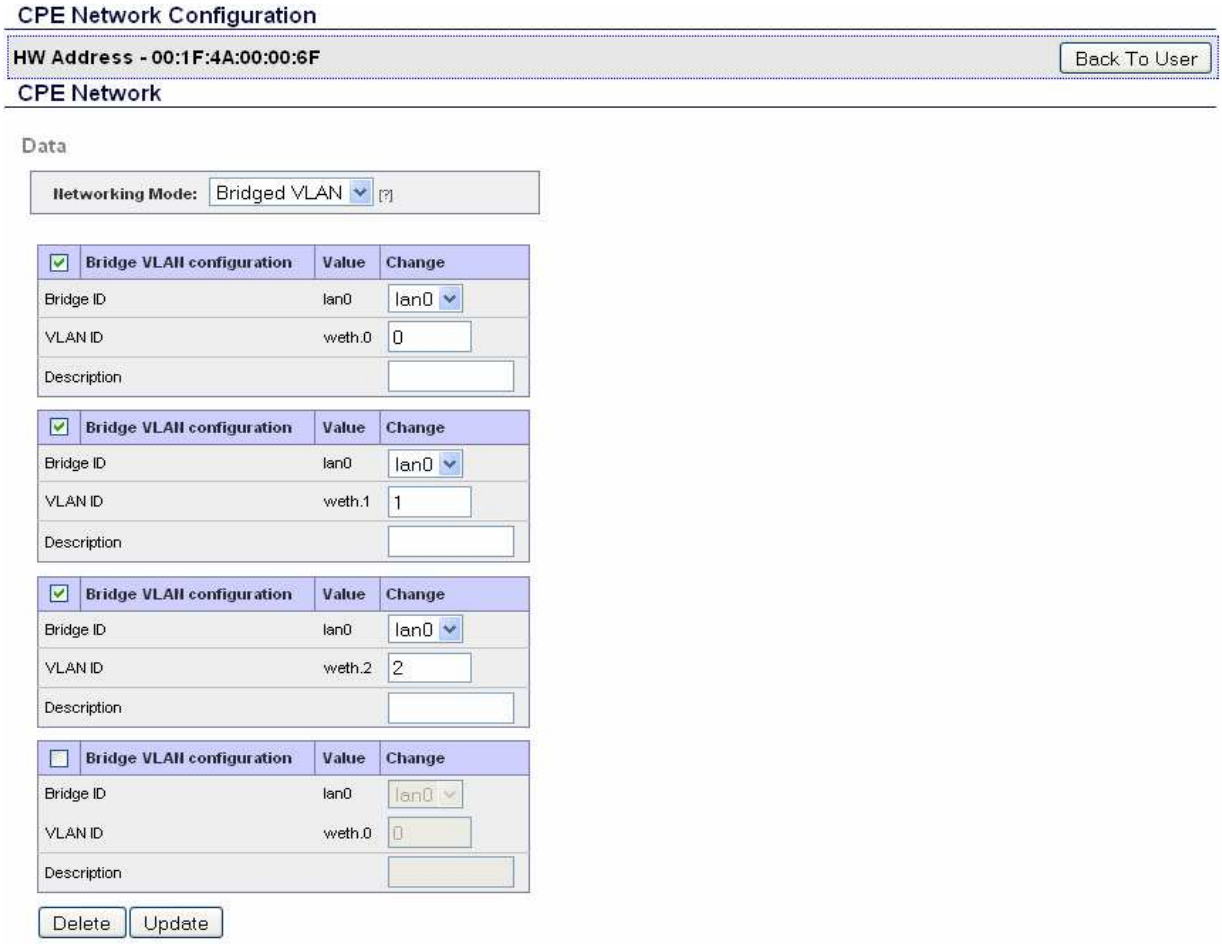


Figure 62 - CPE Network Configuration - Bridged VLAN

Routing Mode

The *Routing* mode is defined as the classic working mode where units have some routing tables defined, and they redirect packets through one interface or another following these previously established rules. These tables must be filled in by the network administrator, and it is very important to configure them correctly in order to make the system work properly.

In this networking mode, the *wethx* wireless interface associated to a certain user will be configured as a standard and static routed interface. An IP must be provided (or DHCP selected) to that interface and all the needed static routes may be added in the provisioning system.

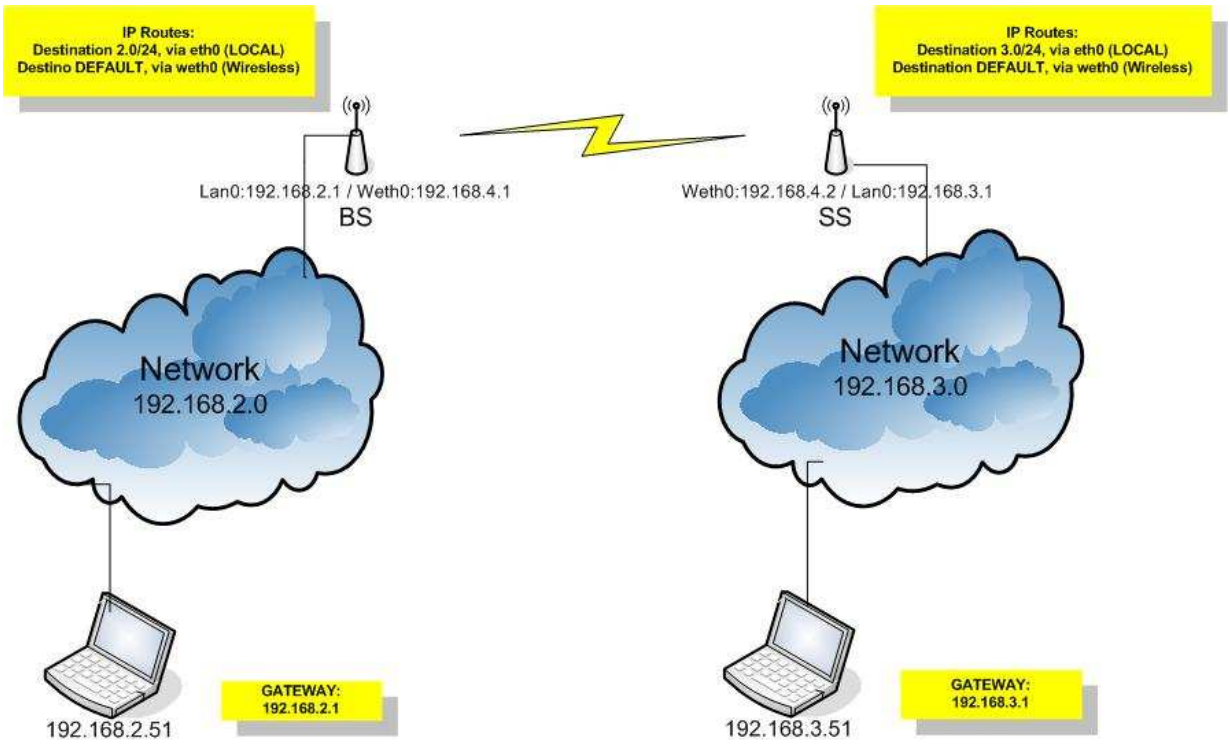


Figure 63 - Example of architecture with *Routing* mode

In order to show a possible scenario that uses this mode, a schematic is presented in Figure 63, where two differential sub-networks in different locations can be observed. A WiMAX link will be used to connect the network 192.168.2.0/24 with the network 192.168.3.0/24, using two units of *Albentia Systems*. The graph also shows an example of the routing tables that could be defined on each *WiMAX* unit in order to allow the communication between units from different networks in a natural way. Obviously, it will be also necessary to make a suitable configuration of the routing tables in each sub-network's equipment, in order to allow them to route traffic towards other network, because in this case its gateway would be the *WiMAX* unit that belongs to its own network.

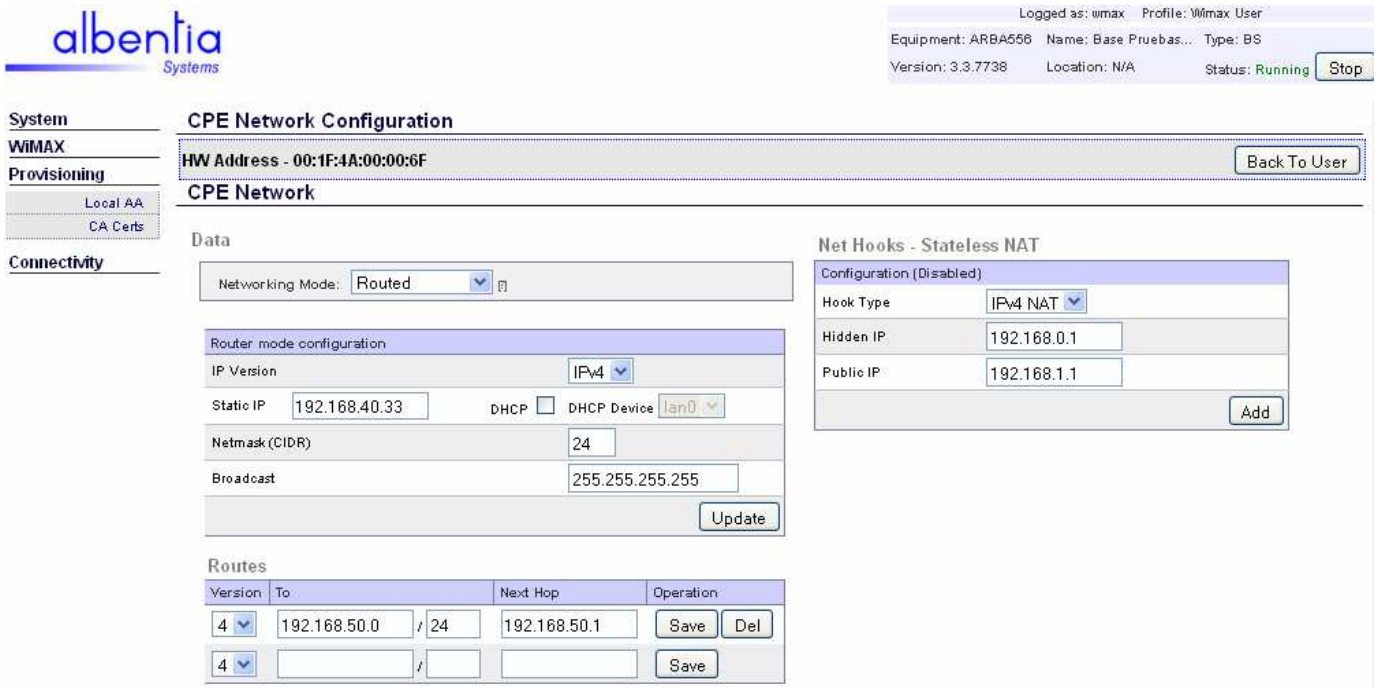


Figure 64 - CPE Network Configuration - Routing mode

This operation mode is selected in the "*CPE Network Configuration*" screen, selecting **Routed** as the desired Networking mode. If this mode is selected, the "*Router Mode Configuration*" block will be displayed, as shown in Figure 64. The fields that should be configured are described below:

- **IP version**: up to the 3.3 Firmware release, IP version 4 may only be selectable, although IPv6 will be available for future use in later releases.
- **Static IP:** it refers to the public IP that will be assigned to this *wethx* interface, when it is created. This IP address should be set either manually (static IP) or automatically, selecting the DHCP checkbox. In this case, a *Fallback* IP address should be specified, as long as the interface that will be used for the DHCP-requests.
- **Netmask**: this field must be filled with the net-mask of the current sub-network, using the CIDR notation (*Classless Inter-Domain Routing*).
- **Broadcast**: this field should be filled with the broadcast IP address. If no address is specified, the following default address will be selected: 255.255.255.255. When operating in DHCP mode, this field is not available.

After filling in this networking information and pressing the "*Update*" button, changes will be saved and the "*Routes*" block will appear below, where the IP routes may be configured manually. The Net-Hook is explained in the following.

Local Network Mode

In this mode the user is connected to a local network at the BS, and it will have data access via NAT to a data interface. This data interface should be selected and a data IP should be provided (or DHCP selected). In addition, this mode allows defining an additional management interface, thus providing a pair of interfaces to access the user: one for data and another one for management.

This operation mode is selected in the "*CPE Network Configuration*" screen, selecting **Local Network** as the desired Networking mode. If this mode is selected, the "*Local Network Mode Configuration*" block will be displayed, as shown in Figure 65.

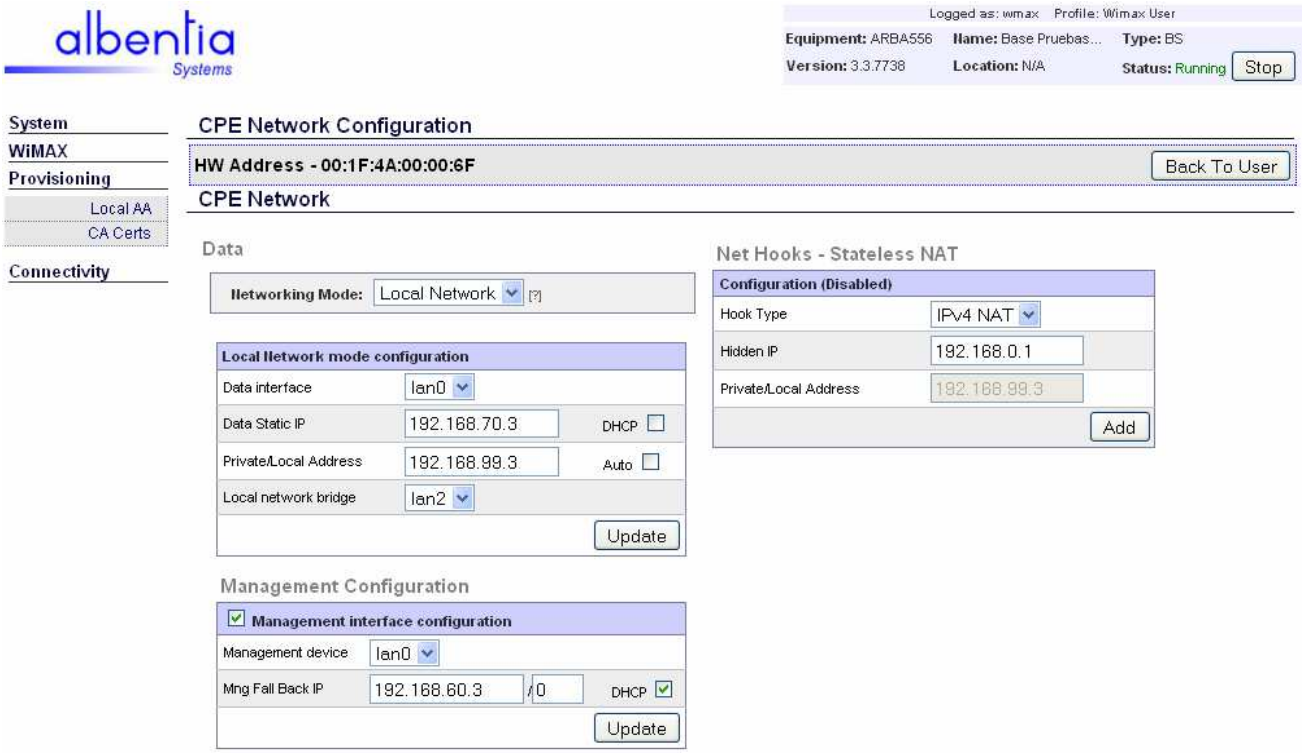


Figure 65 - CPE Network Configuration – Local Network mode

NOTE

The "*Management Configuration*" block will only appear once the Local Network mode is selected, after pressing the "*Update*" button.

This operation mode allows to give "*virtual*" IP addresses to SSs with even the same IP address (using the Net Hook functionality, which will be explained later) with the peculiarity that these "*virtual*" IP addresses do not have to belong to the BS's sub-network (what will be possible with the "Local Network Mode" configuration).

The fields that should be configured are explained below:

- **Data interface:** tit refers to the data interface. If DHCP is used, this device will be used for the DHCP requests.
- **Data Static IP**: it refers to the public IP address that will be assigned to this *wethx* interface, when it is created. This IP address should be set either manually (static IP) or automatically, selecting the DHCP checkbox. In this case, a *Fallback* IP address should be specified.
- **Private/Local Address**: in this field, the private "*virtual*" address that will be given to the SS can be set. There is also the possibility to fix it in automatic mode (selecting the "*Auto*" checkbox), and the BS will assign randomly and IP address inside the current subnet.
- **Local Network bridge**: this field allows to set the identifier of the bridge that will be used to perform the Local Network operation.

To understand better this concept, a sample scenario will be considered, with a BS in the 192.168.70.1 IP address and four SSs belonging to the 192.168.90.0/24 IP subnet, as shown in Figure 66.

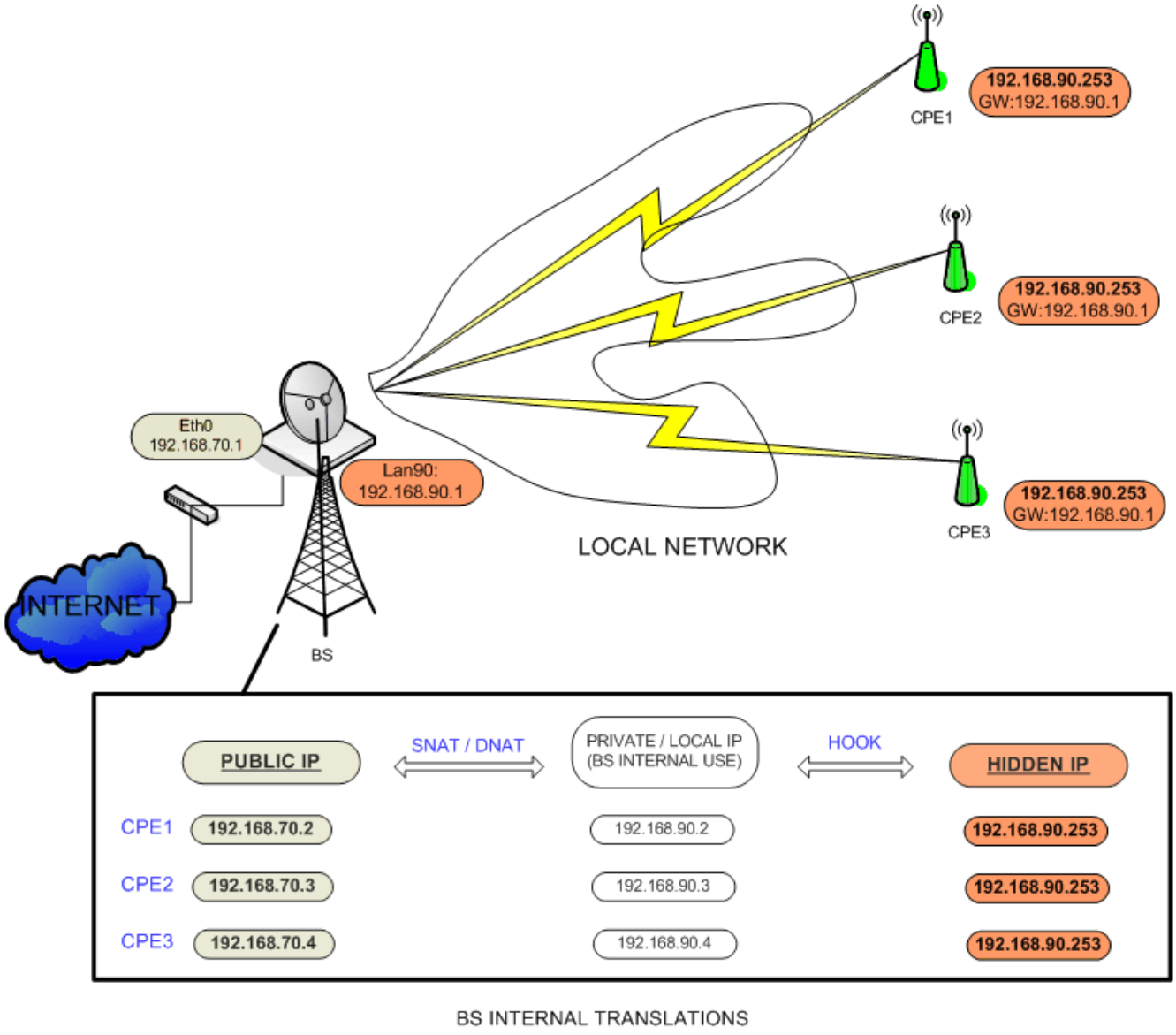


Figure 66 - Example of architecture with *Double NAT* mode

To use this functionality in this scenario, two conditions must be fulfilled:

a) SSs should have a "*real*" IP address which belongs to the desired operation sub-network (in this sample scenario, 192.168.90.0/24). Two different scenarios are supported: all SSs could have different "*real*" IP addresses, or they could have the same "*real*" IP address (i.e. the vendor default IP, which could be 192.168.**90.253**, for instance) using the "Net Hook" functionality, which will give every SS a different "*virtual*" IP address belonging to the original subnet (the Net-Hook is explained later). Once every SS has a different IP address belonging to the private subnet (192.168.90.0/24 in this sample) the BS will be able to translate this addresses into public IP addresses belonging to the public subnet (192.168.70.0/24 subnet in this

sample). The SSs will communicate with the BS or access the Internet using this public IP addresses.

b) SSs should have correctly configured its G*ateway*. In this sample scenario, their gateway would be the BS's IP in the 192.168.90.0/24 sub-network, which in the sample will be 192.168.**90.1**.

To be able to use the "Double-NAT" functionality, it will be necessary to create a specific bridge in the BS. This is performed easily in "*Bridging Setup*" menu. In the sample scenario the new bridge could be defined as "*lan90*", for example, and the given IP would be the gateway for the SSs in that sub-network: 192.168.90.1.

If the SSs already have different "*real*" IP addresses, the Net-Hook functionality will not be necessary, only the "*Local Network Mode*" fields should be filled in. In the current sample, where all SSs have the same "*real*" IP (192.168.**90.253**), the **Net-Hook** will perform the translation between "*real*" and "*virtual*" IP addresses. The fields should be filled on this way:

- **Data Static IP**: 192.168.70.X
- **Private/Local Address**: 192.168.90.X
- **Local Network Bridge**: 90

And referring to the Net-Hook:

- **Hook Type**: IPv4.
- **Hidden IP**: it indicates the "*real*" IP of that SS (i.e. 192.168.**90.253** in the current sample)
- **Private/Local Address**: it indicates the "virtual" private IP address of that SS (i.e. 192.168.**90.2**, 192.168.**90.3**, or 192.168.**90.4** in the sample). If the "*Local Mode Network*" configuration is being used, this field will be automatically filled in to keep the system coherence.

In conclusion: this section will configure the Double-NAT procedure which will allow translating IP addresses from one sub-net to another, and vice versa (in this sample, 192.168.70.0/24 and 192.168.90.0/24 subnets). For example, the SS that will be identified with the 192.168.**90.4** private IP address on the private sub-net will go to Internet using the 192.168.**70.4** as specified in the field "*Data Static IP*". Note that all these IP address translations will be performed in the BS. SSs will not be aware that the translation is being performed, as it is a transparent procedure.

► MANAGEMENT DOUBLE IP ADDRESS

Once the Local Network mode is activated and configured, a new block called "*Management Configuration*" will appear in the bottom of the screen, as shown in Figure 67. This section allows setting an additional IP address for the SSs which can be used for management operations. This IP address may be used as the source or destination address of IP datagrams, resulting that the configuration web interface of that SS could be accessible via this additional management IP address, for example.

The "*Management Configuration*" block allows setting this management additional IP address. For activating this functionality, just select the checkbox in the top of the table, and the IP address fields will now be selectable. The management IP address may be set either manually (static IP) or automatically, selecting the DHCP checkbox. In this case, a *Fallback* IP address should be specified, as long as the interface that will be used for the DHCP requests.

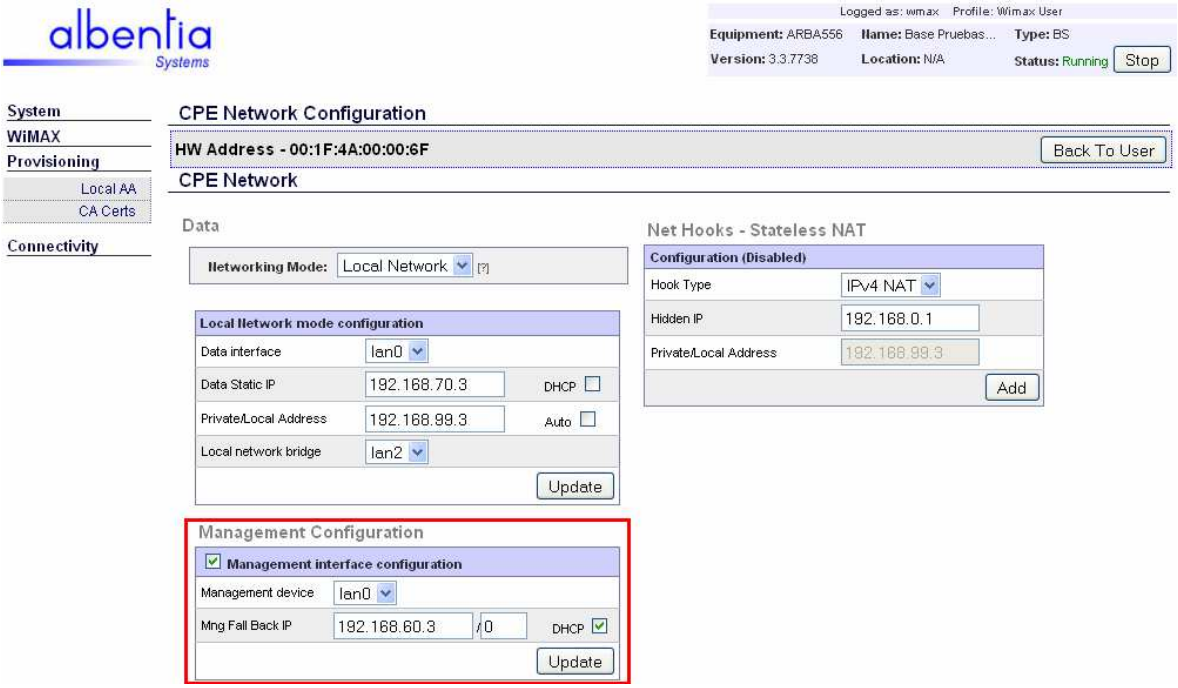


Figure 67 - Management additional IP address

- Net-Hook – Stateless NAT

The "*Net-Hook*" functionality can be configured for *Routing* or *Local Network* operating modes, and is used for giving a "*virtual*" IP address to a specific SS. Two important conditions must be filled:

1) The new Public IP address must belong to the same subnet of the real IP Address ("*Hidden IP*").

2) SSs should have correctly configured its G*ateway*.

The fields that should be filled are explained below:

- **Hook Type**: IPv4 or IPv6 (IPv6 is not available for 3.3 or earlier firmware versions).
- **Hidden IP**: it indicates the "*real*" IP of that SS.
- **Private/Local Address**: it indicates the "*virtual*" IP of that SS. If the "*Local Mode Network*" configuration is being used, this field will be automatically filled in to keep the system coherence.

⚠ ATTENTION!

Remember that the Net-Hook will only translate IP addresses belonging to the same subnetwork.

NOTE

Up to now, the "*Net Hook*" functionality is only supported for single users, although next firmware release will include it also for groups.

3.17. CA Certs

This screen allows configuring the authentication subsystem by means of *Certification Authority*" (CA) certificates. As explained in "*Cell Setup*" menu, when the "*Authorization required*" field is enabled in the BS, the "*SS Authorization and Key Exchange*" will be performed, using **X.509 digital certificates** (obviously, the CPE must support this option). This means that during the cell entry process, the CPE needs to be certified by the chain of truth of the Base Station. This is the first step for a SS to access the network: if authorization is required but not supported by the CPE, it will be directly disconnected; otherwise, the entry process will continue and the BS will decide whether allowing the SS into the cell or not, according to the provisioned users in the *local AA* Database (as explained in Section 3.16).

The X.509 digital certificate is a public-key certificate that binds the SS's identifying information to its RSA public key in a verifiable manner. It is digitally signed by the SS's manufacturer, and that signature can be verified by a BS that knows the manufacturer's public key. The manufacturer's public key is placed in an X.509 certification authority (CA) certificate, which in turn is signed by a higher-level CA.

This screen shows the currently CA certificates trusted in the BS. By default, three trusted certificates are loaded, as shown in Figure 68: *CPE Tranzeo CA*, Albentia *Systems Root CA* and *Albentia Systems Device CA*. Further information about the organizations can be found in the help of the screen. The operator can also load his own certificate by the "*Upload CA certificate*" tool where the authorized CPE's are specified, as a first control to the cell entry.

Figure 68 - "*CA Certificates*" menu

3.18. Network Setup

From this page all the characteristics of the network configuration of the system can be visualized. This section of the *Web* application allows visualizing and configuring all the network interfaces of the equipment, both physical and wireless, as well as the current configured IP routes or the gateway's IP address.

3.18.1. "*Interfaces*" tab

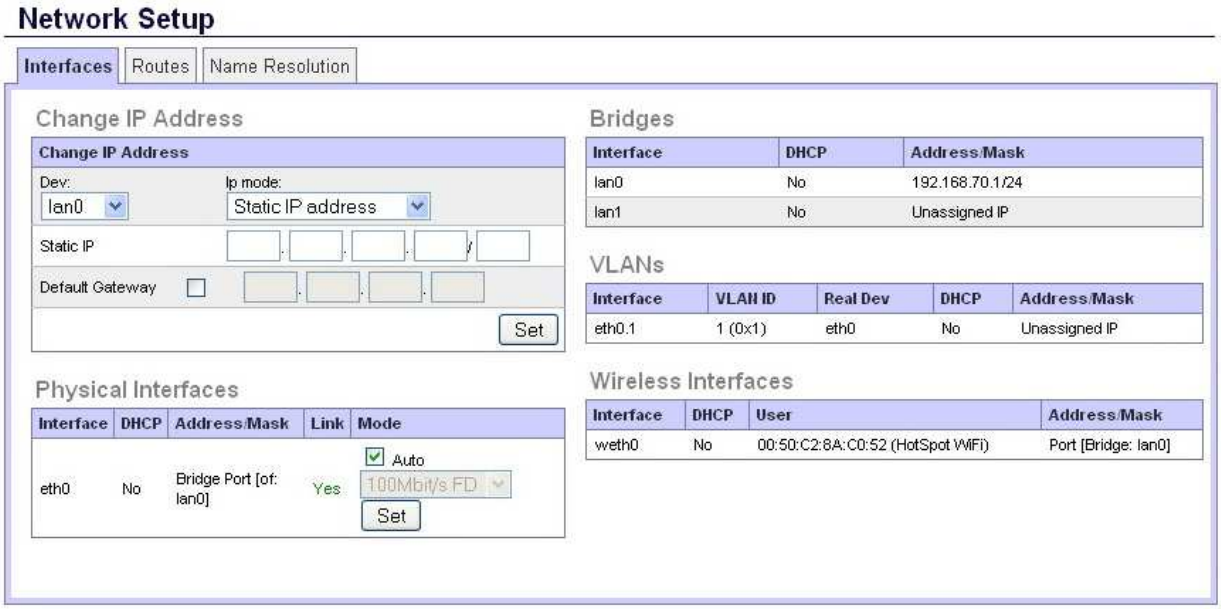


Figure 69 - Network Setup, Interfaces tab

This tab has an appearance as shown in Figure 69, and it contains different sections:

- **CHANGE IP ADDRESS**

In this block it is possible to change the IP addresses to all the current active wired interfaces (*ethx*, *lanx* and VLAN devices). There are two operation modes available:

a) **Static mode**: the IP address should be introduced manually by the user in the appropriate field (with a *0.0.0.0/X* notation), and the address of the default gateway may also be set.

b) **DHCP mode**: in this mode the unit will automatically ask for an IP address using the DHCP protocol. In this mode, the user may also define a *Fallback IP*, which will be assigned to that interface if the DHCP negotiation has not been successful.

The changes will take effect after pressing the "*Set*" button. The system will check that the address and the mask have valid values, and it will show a warning message before changing the IP.

- **PHYSICAL INTERFACES**

In this table it is possible to look up the available physical network interfaces, together with its IP address and other information. In the "*Mode*" field the operation mode of the Ethernet interface can be configured: the negotiation (auto-detecting or forced), the speed (10/100 Mbps), and the transmission mode (full/half duplex).

- **BRIDGES**

In this block the active *Bridges* (*lanx* interfaces) will be listed, if any, with some related information.

- **VLANs**

In this block the active VLANs will be listed, if any, with some related information.

- **WIRELESS INTERFACES**

This table shows a list with the active wireless network interfaces, in the same way as the *Physical Interfaces.* These interfaces will be automatically created and assigned to every user by the BS.

3.18.2. "*Routes*" tab

In this tab, the configured *unicast* routes will be listed. The user may add and delete routes easily. To add new one, just fill in the suitable fields (*destination*, *via*, *and interface*). In order to make the creation of routes easier, the system shows which interfaces are available. In addition, the "*Default*" checkbox allows defining the default Gateway, and the "*Local*" checkbox will route that traffic locally. This tab has an appearance as shown in Figure 70.

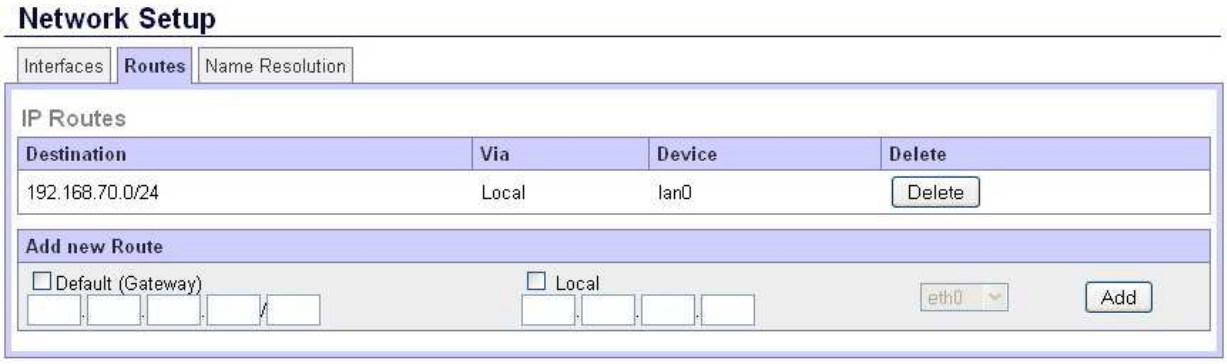


Figure 70 - Network Setup, Routes tab

3.18.3. "*Name Resolution*" tab

If the BS has access to the Internet, in this field the default DNS (*Domain Name System*) server can be defined. Just introduce the IP address of the server in the field and press the "*Set DNS*" button to activate this option. To de-activate, press the "*Reset DNS*" button. This tab has an appearance like the one shown in Figure 71.

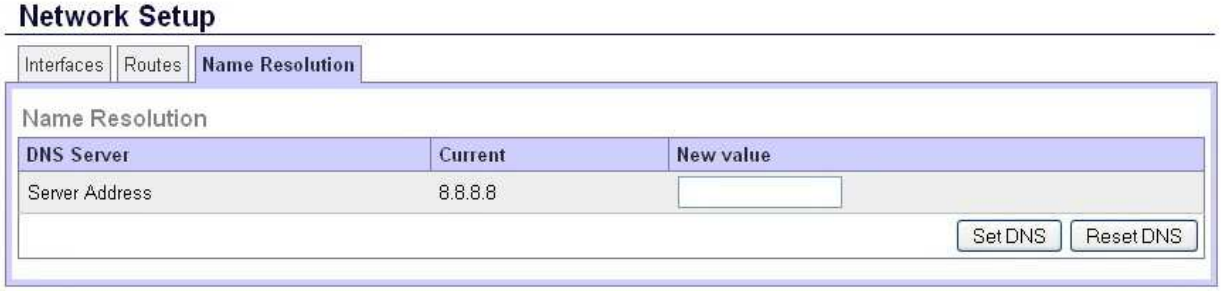


Figure 71 - Network Setup - Name Resolution tab

3.19. Bridging Setup

This section is useful when *Bridging* mode is going to be used. From this, different bridges may be created or deleted. The unit allows creating multiple bridges simultaneously, what means that a pair of units could interconnect different pairs of sub-networks sharing the same wireless channel, or that a BS with multiple users could put them into different groups using different Bridges, for instance. Figure 72 shows a sample screenshot were two bridges are defined:

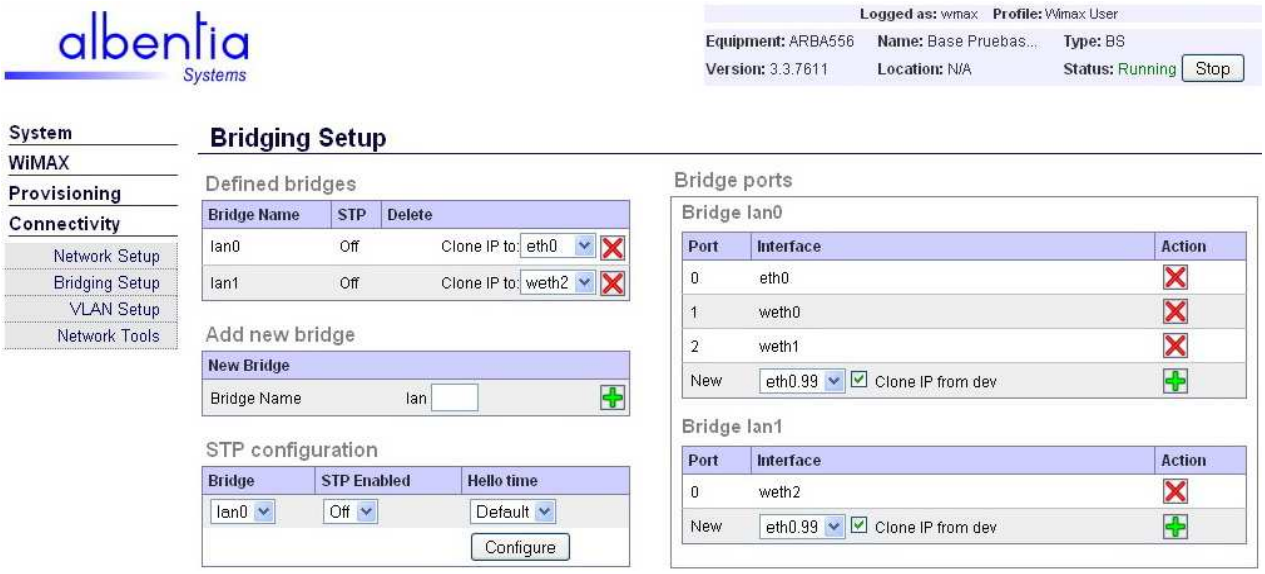


Figure 72 - "*Bridging Setup*" menu

- **Creating a Bridge:** it is a simple process: just go to the "*Add new bridge*" section, give an "*x*" number to the bridge and click in the "*Add Bridge*" icon. Once performed, a "***lanx***" named bridge will be automatically created and shown in the "*Defined bridges*" section. An IP address may be assigned to the new "*lanx*" interface just by going to "*Network Setup*" menu and assigning an IP to the "*lanx*" interface.
- **Adding interfaces to a Bridge**: it is possible to introduce the BS's wired interface ("*eth0*") in the bridge, just by going to the "*Bridging Setup*" menu, selecting the "*eth0*" interface and clicking in the "*Add port*" icon. If the "*Clone IP from device*" checkbox is selected, the current IP address of the "*eth0*" interface will be automatically copied to the "*lan0*" interface. Regarding the wireless interfaces, the BS will automatically create a "***wethx***" interface for every SS connected to the cell that has been configured in the "*Local_AA*" for belonging to a Bridge. The "*Bridge ports*" section also allows to delete manually an interface from a *Bridge*, clicking in the appropriate "*Delete*" icon.
- **Deleting a Bridge**: once a "*lanx*" has been created, it can be easily deleted in the "*Defined bridges*" section, just pressing the appropriate "*Delete*" icon. If the "*eth0*" is added to the bridge, deleting the bridge would also delete the IP of the unit, making it unreachable. To avoid this, it is possible to clone the IP of the bridge to the physical interface, keeping the IP address of the unit.

NOTE

Remember that after creating Bridges, every CPE should be associated to the correct bridge in the "*Network Provisioning*" section in the Local AA.

► SPANNING TREE PROTOCOL (STP)

STP is a Layer 2 protocol, typically based in the *IEEE 802.1D* standard, that runs on bridges and switches, and whose main purpose is to prevent loops when having redundant paths in the network. STP is a technology that allows bridges to communicate with each other to discover physical loops in the network. The protocol specifies an algorithm that bridges can use to create a loop-free logical topology. As the name suggests, STP creates a tree structure of loop-free leaves and branches that spans the entire Layer 2 network; it disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

STP operation is transparent to end-stations. Where two bridges are used to interconnect the same two computer network segments, Spanning Tree is a protocol that allows bridges to exchange information, so that only one of them will handle a given message that is being sent between two computers within the network.

Bridge Protocol Data Units (BPDUs) are used by bridges where STP is enabled, to exchange information regarding their status. The **Hello Time** is the time between each BPDU that is sent on a port. This time is equal to 2 seconds (sec) by default, but it may be tuned to be between 1 and 60 sec.

STP is an available functionality when using Bridging in ARBA135 units, so every Bridge is able to communicate with other Bridges/Switches in the network where STP is running. It is possible to activate STP (or not) for each existing Bridge using the "*STP Configuration*" section. The procedure is simple: select the Bridge name, select to enable or disable STP, and set the "*Hello Time*" parameter. Then just press the "*Configure*" button.

3.20. VLAN Setup

A Virtual Local Area Network (VLAN) is a local area network that groups together a set of hosts taking into account logic parameters like MAC address, port number, protocol, etc, regardless of their physical location. In this way it is possible to have multiple subnets on one VLAN or have one subnet spread across multiple VLANs. VLANs provide higher flexibility because network reconfiguration can be done through software instead of physically relocating devices. VLANs address issues such as scalability, security, and network management.

The ARBA135 is able to tag and un-tag packets as specified in the *IEEE 802.1Q* protocol, whose header contains a 4-byte tag header with the following elements: three-bit User Priority, one-bit CFI (Canonical Format Indicator) and twelve-bit VLAN identifier (VID). ARBA135 may be used to create and manage VLANs, operating either as a switching node or as a VLAN end-point. It supports up to 10 levels of Q-in-Q encapsulation, which allows adding an additional tag to a previously tagged packet. This mechanisms increases VLAN scalability, improves security via robust isolation of customer traffic, and ensures backward compatibility preserving existing customers VLAN structures.

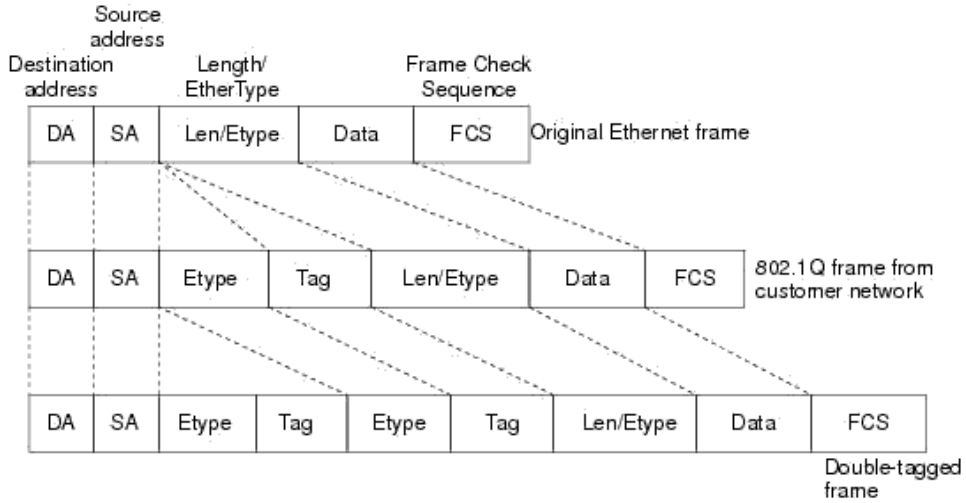


Figure 73 - IEEE 802.1Q tagged frame

VLANs may be defined in the "*VLAN Setup*" section, as shown in Figure 74. The screen is divided into two blocks: in the left side, the current VLANs are listed, and in the right side the new VLANs may be created. To perform this operation, the user should select the base interface, fill in the desired VLAN Identifier, and press the "*Add VLAN*" button. After this, a new row will appear in the "*Current VLANs*" block showing the related information. To assign an IP address to this new interface, go to the "*Change IP Address*" block inside the "*Network Setup*" menu. The new VLAN will be now a completely manageable interface, so it can be assigned an IP address, used to manage the SSs, etc…

As it has been explained before, thanks to the Q-in-Q encapsulation a new VLAN can be defined over an existing VLAN. To perform this, just select an existing VLAN as the "*Base device*" of the new VLAN.

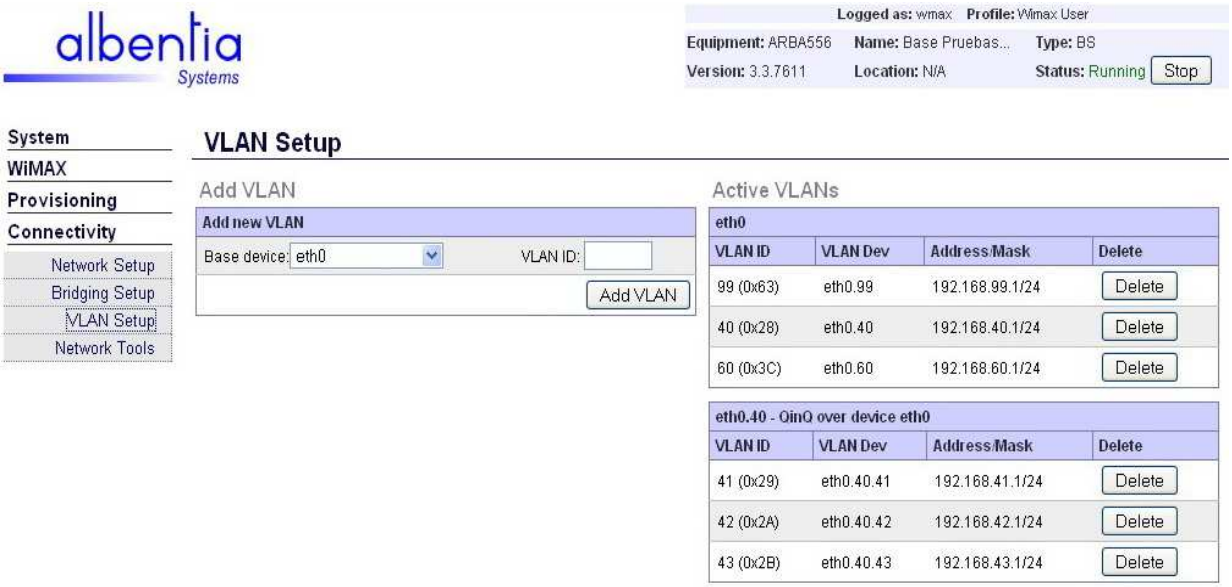


Figure 74 - "*VLAN Setup*" menu

3.21. Network Tools

Finally, the web interface includes some simple diagnostic tools to check network's connectivity, as shown in Figure 75 and as explained below:

- **Ping**: test whether a particular host is reachable across an IP network by sending ICMP "*echo request*" packets. The user must fill in the destination IP address ("*To(IP)*" field), and may also fill in the number of ping requests ("*Count*" field, default is 4), and the number of data bytes to be sent with every packet ("*Packet size*" field, default is 56 bytes which translates into 64 ICMP data bytes when combined with the 8 bytes if ICMP header). Once these fields have been filled in, after pressing the "*Ping*" button and the results will be displayed when the ping has finished.
- **Arping**: similar to ping, but it operates using ARP instead of ICMP. Thus, arping is only usable for hosts inside the current LAN. For using this command the user must fill in the destination IP address ("*To (IP)*" field) and the number of *arping* requests ("*Count*" field, default is 4). Then, select the interface from where the packets will be transmitted, and press the "*Arping*" button.
- **Traceroute**: this network tool is used to determine the route taken by packets across an IP network. For using this command the user must fill the destination IP address ("*To (IP)*" field) and then press the "*Traceroute*" button.

Once the required fields are filled in and the correspondent button is clicked, the results of the used command will be shown in the screen when finished.

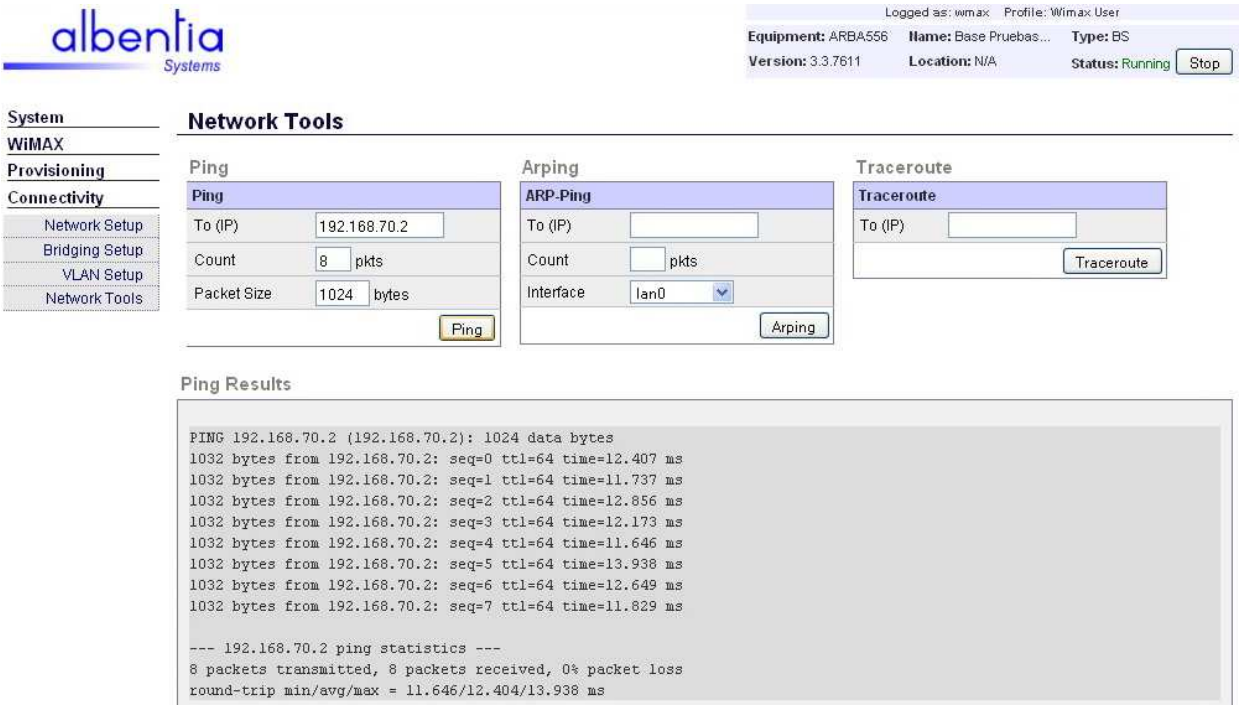


Figure 75 - "*Network Tools*" menu

4. COMMAND LINE INTERFACE (CLI)

All the operations that can be performed by the Web Interface are also available in the CLI interface. The CLI could be less intuitive and graphical, but it offers the same functionalities as when accessing via HTTPS, and it is an interesting alternative when an internet browser is not available, for example. It also may be interesting for interoperating with any other SW, or for building specific program scripts.

4.1. Accessing the CLI Interface

In order to use this interface, it is necessary to establish a SSH (*Secure Shell*) connection towards the IP address of the unit. The encryption used by SSH provides confidentiality and data integrity as it uses public-key cryptography to authenticate the remote computer. As the *Secure Socket Layer* (SSL) is the same as in HTTPS, the CLI interface will be as secure as the HTTPS Web Interface.

Once the SSH command is launched using for example

ssh BS_IP_Address

the screen will ask for login and password, which will be the same used for in the Web Interface. This procedure can be seen in Figure 76. The following figures have examples with ARBA556 but it's exactly the same in ARBA135. Once authentication has been correctly performed, the *prompt* (**[ARBA135]** in the case of a BS's CLI) will be shown, ready to process all the available commands.

Figure 76 - Accessing the CLI

As many things related to the system architecture and modes of operation have been explained before, the user is supposed to be familiar with all these aspects, so this interface will be described briefly.

NOTE

The CLI includes a complete help system that describes all the available commands in each section. This help system is easily accessed typing one of these commands: "*help*" or *"h"*.

4.2. Folder scheme

The CLI has a folder scheme similar to a reverse tree, as shown in Figure 77. The movement across the different folders is the typical in this kind of systems. Thus, to descend to a "*submenu_x*", it must be typed

cd submenu_x

and to return to the original folder, it must be typed

cd ..

There are five main menus/folders inside the application. The main menu is the **user menu**. From this menu it is possible to perform all the actions related to the users' global management as well as some administrative actions in the system. By typing "*help*", all the operations that can be performed inside this menu will be seen.

Besides this menu, there are four other specific menus in the equipment. Typing "*p*" or "*ls*" inside the **user menu**, these four folders will be listed, as shown in Figure 76. These menus are: **system menu**, **management menu**, **network menu** and **global menu**.

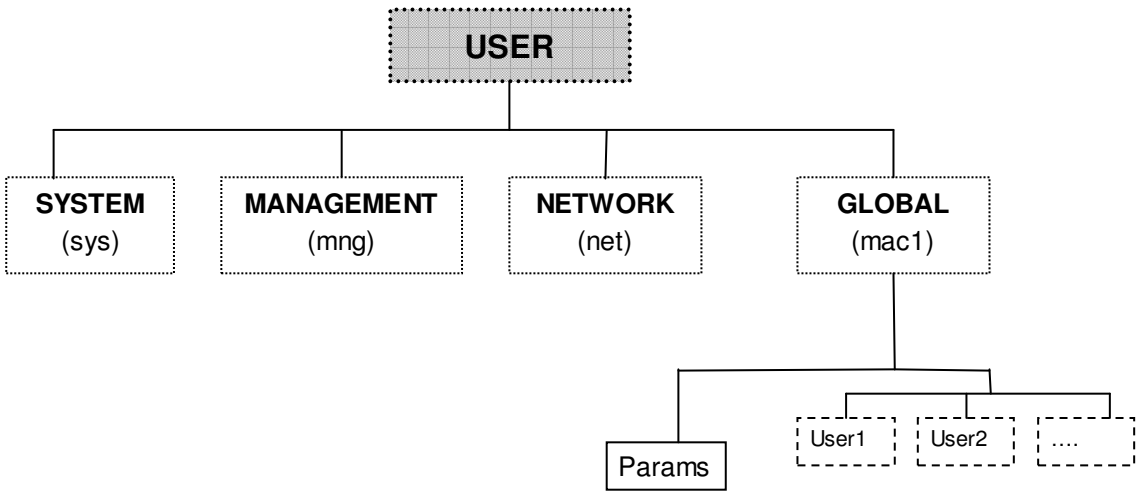


Figure 77 - CLI folder scheme

4.2.1. System menu

This menu provides information about the system and allows the user to manage the Configuration Files. The folder is reached from the "**User Menu**" typing:

```
[ARBA135]> cd sys
[ALB135/sys]>
```

From this folder, many operations can be performed: to save or load configuration files, show the SW version, execute a system reboot, set the system local time… By typing:

[ALB135/sys]>help

the "*SYS Menu help*" will be shown, describing all these options more in detail.

4.2.2. Management menu

This menu allows to configure all the aspects related to the Management of the unit. The folder is reached from the "**User Menu**" by typing:

[ARBA135]> cd mng
[ALB135/mng]>

From this folder, many operations can be performed: to enable or disable SNMP, activate the different XML-RPC modes, create specific management interfaces, change from a HTTPS server to a HTTP one,… By typing:

[ALB135/mng]>help

the "*MNG Menu help*" will be shown, describing all these options more in detail.

4.2.3. Network menu

This section allows the user to configure the management features of the unit. The folder is reached from the "**User Menu**" by typing:

[ARBA135]> cd net
[ALB135/network]>

From this folder, many operations can be performed: to set the IP routes, define a DNS server, operate with bridges, view the static multicast routes … By typing

[ALB135/network]>help

the "*NET Menu help*" will be shown, describing all these options more in detail.

In addition, the current network configuration will be displayed by typing the command "**p**". In the Figure 78 a sample screenshot is shown, where it can be observed that the BS is working in *bridging mode* and that it is connected to four different SS units. Their MAC address, their alias, and the current wireless interfaces are listed.

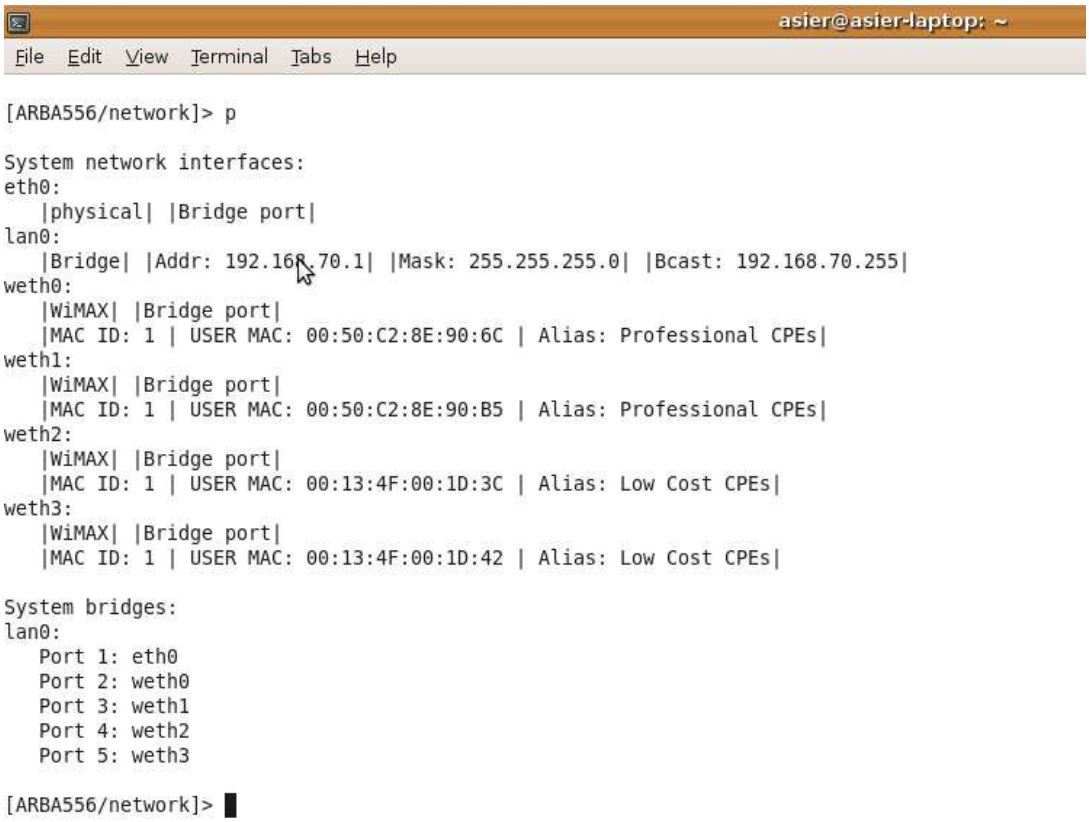


Figure 78 - "*Network*" CLI menu

4.2.4. Global menu

This menu is the more complete of the CLI. It allows to perform many different operations related to the physical and radio configuration of the unit as well as to the users and data services' management. The folder may be reached from the "**User Menu**" by typing:

[ARBA135]> cd mac
[ALB135/mac1[BS]]>

From this folder, many operations can be performed: to change the MAC status (stopped/started/paused), disconnect users, show information about the physical level, change radio parameters… By typing

[ALB135/mac1[BS]]>help

the "*MAC Menu help*" will be shown, describing all these options more in detail.

In addition, the current user configuration can be seen by typing the command "**p**". In the Figure 79 a sample screenshot is shown, where it can be observed that four different allowed users are active and connected to the BS.

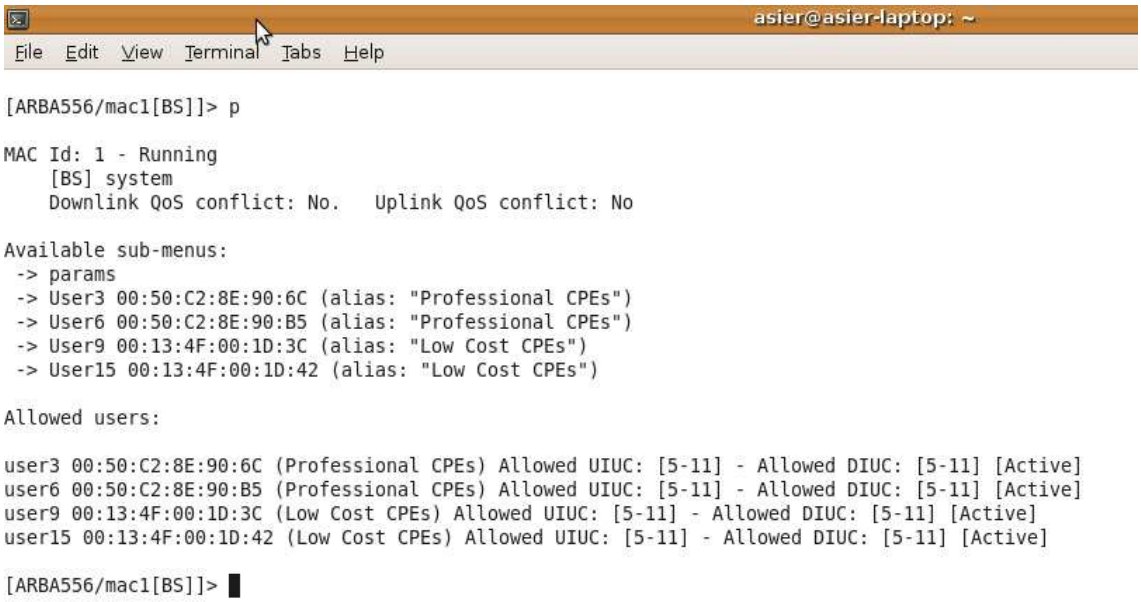


Figure 79 - "*Global*" CLI menu

This screenshot also shows that from the global menu different sub-menus may be accessed. First of all, there is the **parameters menu**, which allows modifying all the physical parameters: transmission power, maximum user distance, channel bandwidth… As it happens with all the folders, the "**help**" command will describe all these options more in detail, and the "**p**" command will display the physical configuration. In the Figure 80 a sample screenshot is shown with the current radio configuration.

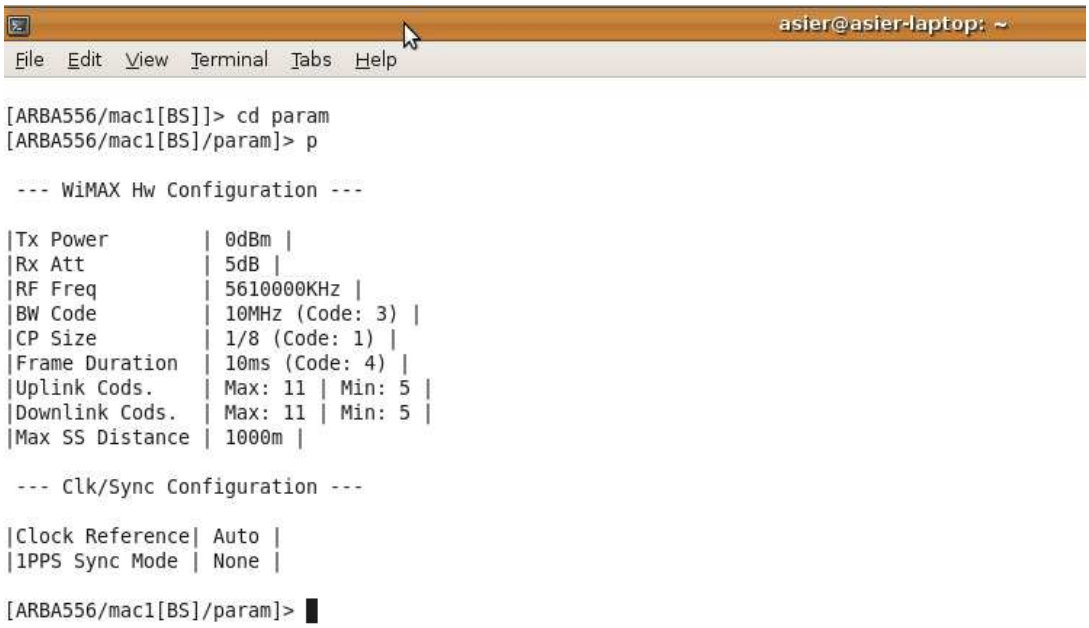


Figure 80 - "*Params*" CLI sub-menu

Besides, one **User_x sub-menu** will be created for every active user that is connected to the BS. In the sample shown in Figure 79, with four active users, four different sub-menus have been created: *user3*, *user6*, *user9* and *user15*, one for each SS. These numbers are randomly selected by the BS. From this user sub-menu, many operations referring to that user can be performed: to show link stats, create and delete

service flows,…As it happens with all the folders, the "**help**" command will describe all the available options more in detail, and the "**p**" command will display the flow configuration. In Figure 80 a sample screenshot is shown:

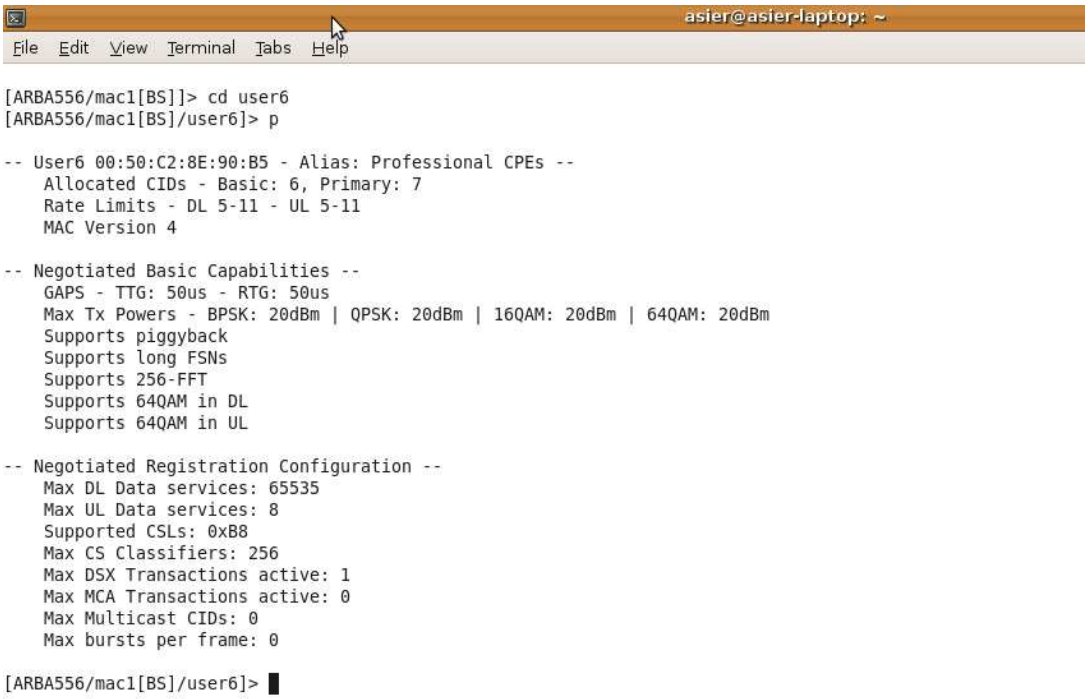


Figure 81 -"*User_x*" CLI sub-menu

5. SERIAL INTERFACE

ARBA135 unit includes a **RS-232** serial interface on its most recent enclosure. This interface may be used to access the unit when the Ethernet interface is not available (due to networking problems, for instance). It can also be used as an alternative when the IP address of the unit is forgotten.

When connecting the unit to a PC; the BS will act as the DCE (*Data Communication Equipment*) while the computer will act as the DTE (*Data Terminal Equipment*), so connection between them must be performed with a *straight through* serial cable instead of a *null modem* cable (used to connect two DTEs directly). In a *straight through* configuration, pin 1 is connected to pin 1, pin 2 to pin 2, etc. The BS has a DB9 female connector which only uses three pins: pin 2 (TX signal), pin 3 (RX signal) and pin 5 (GND). This signalling is defined from the DCE point of view.

The unit's signal functions follow the *EIA/TIA 574* norm for RS232 communication on DB9 that are described in detail in Table 14. The column marked *Direction* shows the signal direction with respect to the DTE.

Pin	Name	Direction	Notes / Description
1	*DCD*	*IN*	*Data Carrier Detect. Raised by DCE when modem synchronized.*
2	***RD***	*IN*	***Receive Data (also known as RxD or Rx). Arriving data from DCE.***
3	***TD***	*OUT*	***Transmit Data (also known as TxD, Tx). Sending data from DTE.***
4	*DTR*	*OUT*	*Data Terminal Ready. Raised by DTE when powered on. In auto-answer mode raised only when RI arrives from DCE.*
5	***SGND***	-	***Ground***
6	*DSR*	*IN*	*Data Set Ready. Raised by DCE to indicate ready.*
7	*RTS*	*OUT*	*Request To Send. Raised by DTE when it wishes to send. Expects CTS from DCE.*
8	*CTS*	*IN*	*Clear To Send. Raised by DCE in response to RTS from DTE.*
9	*RI*	*IN*	*Ring Indicator. Set when incoming ring detected - used for auto-answer application. DTE raised DTR to answer.*

Table 14 - DB9 (EIA/TIA 574) - View - looking into male connector

The *user* and *password* required by the serial connection are the same ones used at *Web* interface. Once logged, the user will access to the CLI interface. As explained before, CLI is an alternative to *Web* interface in order to configure the device. More information about CLI may be consulted in Point 4.

There are many applications to establish the connection between computer and BS using the serial port. Some of the most used are *Putty* in *Windows* and *Minicom* in *Linux*. The main steps to use both tools are described below, and serial connection parameters are reported in Table 15.

Speed (bauds)	Data bits	Parity	Flow Control
115200	8	*No*	*No*

Table 15 - Serial connection parameters

5.1. Connection with "*Putty*"

The main window of *putty* is showed in Figure 82. User should select "*Serial" as the Connection type* and the suitable *Speed*. Then, click in the "*Open*" button to start the serial communication.

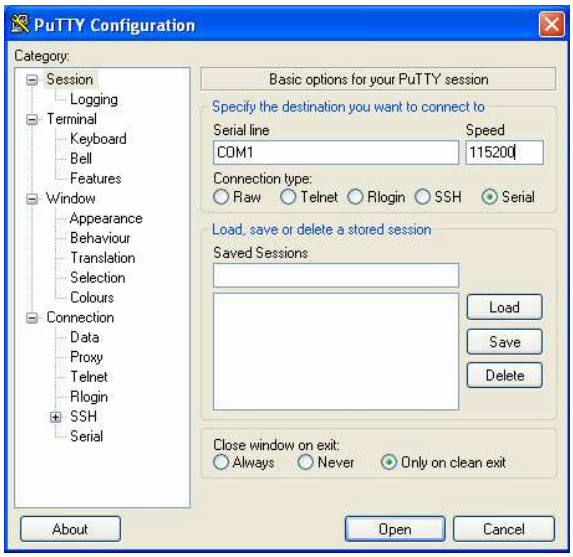


Figure 82 –Main window of *Putty*

A new window will appear with a CLI asking for a *user* and *password*. An example of this is shown in **Figure 83**.

Figure 83 – Login window with *putty*

5.2. Connection with "*minicom*"

Minicom is tool that allows establishing the connection with the BS using a Linux based system. However its configuration may require some more steps than in *putty* when used the first time. These steps are listed below:

1- Execute *minicom* command. This command will start the program.

2- To open the options menu press **CTRL+A**, and after releasing this keys press **Z**.
3- Select the configuration option by pressing the **O** key, which will open the menu shown in Figure 84 *a)*.
4- Inside the configuration menu, select the "*Serial port" configuration* option.
5- Set the parameters following Table 15, and insert ***/dev/ttyS0*** as *Serial Device*. The final configuration will look like the one shown in Figure 84 *b).*

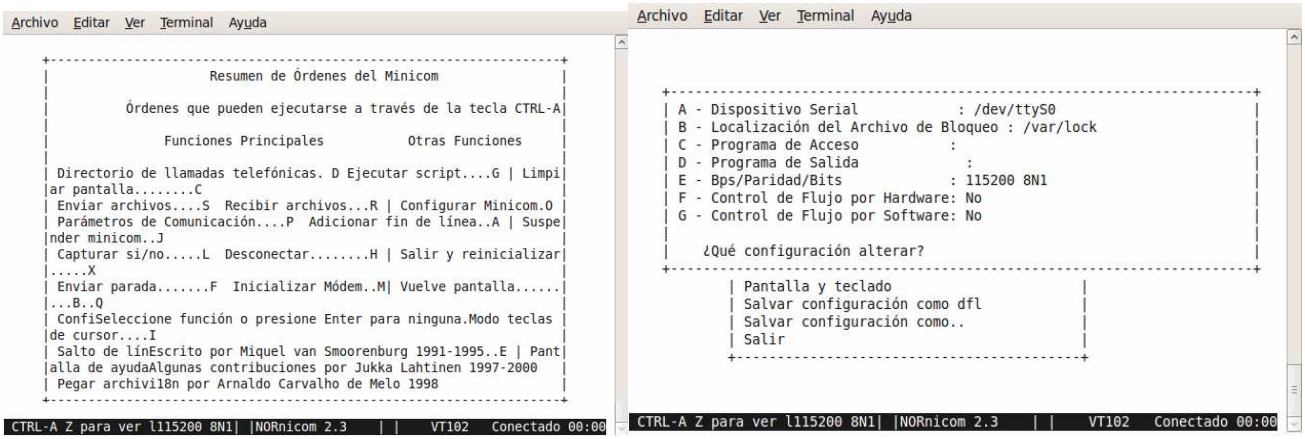


Figure 84 – a) Minicom options b) Minicom serial parameters

6- Save configuration as *dfl*.
7- Exit (***X*** option) and restart the program in order to load the new configuration. Now the program will connect with the BS through serial port and the starting window will look like the one shown in Figure 85.

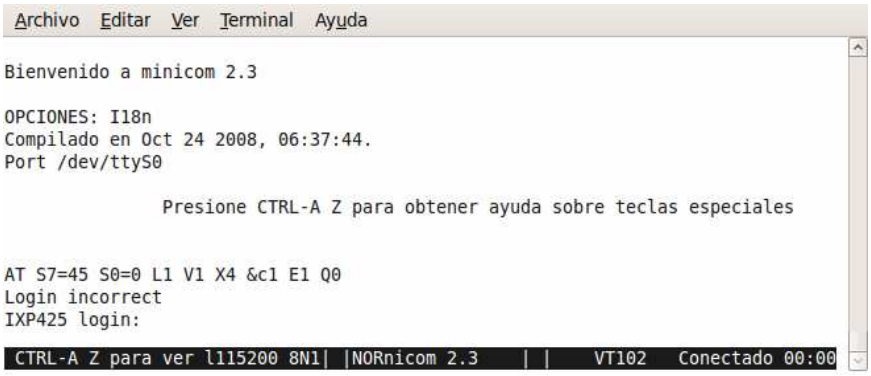


Figure 85 – Login window with *mincom*