



User Manual & Installation Guide for:
WiN7000 Compact Base Station (cBST)
Family

M/N:
Version: 4.4
Revision: 1.2
Date: April 2008

WiNetworks Win-MAX™ 802.16e

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESSED OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR WINETWORKS REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. WINETWORKS AND ITS SUPPLIERS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL WINETWORKS OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF WINETWORKS OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

COPYRIGHT ©2007 WINETWORKS. ALL RIGHTS RESERVED.

WINETWORKS AND WIN-MAX™ ARE REGISTERED TRADEMARKS OF WINETWORKS AND/OR ITS AFFILIATES IN THE U.S. AND CERTAIN OTHER COUNTRIES.

ALL OTHER TRADEMARKS MENTIONED IN THIS DOCUMENT OR WEB SITE ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS. THE USE OF THE WORD PARTNER DOES NOT IMPLY A PARTNERSHIP RELATIONSHIP BETWEEN WINETWORKS AND ANY OTHER COMPANY.

Table of Contents

Introduction.....	6
1.1 About this Manual.....	7
1.2 General Description.....	7
1.3 Package Components and Unpacking.....	9
1.4 Safety Information.....	10
Product Description.....	14
2.1 Introduction.....	15
2.2 IEEE 802.16e Mobile WiMAX Compliance	15
2.3 Block Diagram.....	15
2.4 Features.....	17
2.4.1 Mobile WiMAX Wave 2 MIMO Features.....	17
2.4.2 Security	18
2.4.3 Time Division Duplexing (TDD).....	21
2.4.4 Coding Rate.....	21
2.4.5 Modulation.....	21
2.4.6 Error Code Correction	21
2.4.7 Time Synchronization.....	22
2.5 Deployment Models.....	22
2.5.1 PMP Deployment	22
2.5.2 Non Line-of-Sight.....	22
2.5.3 Channelization.....	23
2.6 Service Flows.....	23
2.6.1 Service Flow Classification.....	23
2.6.2 Dynamic Service Addition.....	23
2.6.3 Default Service Flows	24
2.6.4 Scheduling.....	24
2.7 Physical Description.....	25
Mounting.....	27
3.1 General.....	28
3.2 Site Survey	29
3.3 Pole Mounting.....	30

3.4	Wall Mounting	30
3.5	Tower Mounting.....	30
	Installation Procedures	31
4.1	Safety Hazards	32
4.2	Installation Tools.....	32
4.3	Installing the WiN7000.....	32
	4.3.1 Pole Mount	34
	4.3.2 Wall Mount.....	37
	4.3.3 Tower Mount	38
	4.3.4 Cable Connections.....	39
	4.3.5 Power Cable	40
	4.3.6 Console Cable	40
	4.3.7 Antenna Cable	41
4.4	Power Connections.....	42
4.5	Multi-sector Base Station Daisy Chain.....	43
	Equipment Configuration and Monitoring	44
5.1	Configuring WiN7000	45
	5.1.1 Basic Configuration.....	45
	5.1.2 Monitoring.....	49
5.2	Configuring WiN7000 for MIMO.....	51
5.3	Configuring the ASN Gateway.....	52
5.4	Monitoring.....	53
	Management.....	54
6.1	General	55
6.2	SW Download/Upgrade	55
6.3	Web-Based Management.....	55
6.4	SNMP Management	56
	cBST WEB Manager.....	57
7.1	Overview.....	58
7.2	Audience	58
7.3	Using the Command Set.....	58
7.4	Commands by Functional Area.....	59
	7.4.1 Security	59

7.4.2	Logs	59
7.4.3	Misc	59
7.4.4	UnicastServiceFlow	60
7.4.5	SS.....	60
7.4.6	Statistics	60
7.4.7	MacFrame	61
7.4.8	FWD	61
7.4.9	Config.....	61
7.4.10	Private.....	61
7.4.11	Other.....	62
7.5	Command Reference	65
	Appendix A –Specifications	160
	List of Acronyms.....	161

1

Introduction

1.1 About this Manual

This manual describes the WiN7000 Outdoor Compact Base Station (cBST). It is designed for installers and operators.

WiN7013-2 and WiN7035-2 will be referred in this manual as WiN7000 from now on.

WiN7000 is a member of the Win-Max™ E family, a line of mobile WiMAX broadband wireless access systems based on the 802.16e mobile WiMAX standard. The Win-Max™ E family is described in the System Description manual of WiNetworks.

This manual assumes that users working knowledge of WiMAX technologies and procedures.

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

1.2 General Description

The Base Station unit provides the full base station functionality necessary for serving a single sector. The Base Station is powered by 48VDC.



The functions of the cBST includes:

- All outdoor, one-box Compact Base Station solution
- IEEE802.16e Wave2 Standard Compliance
- Backbone Ethernet connectivity via a 10/100 Base-T network interface
- Supports fixed and mobile CPEs

- Supports 5MHz,7MHz and 10MHz channel bandwidth
- Supports different RF options including 1.x, 3.x GHz bands
- MIMO (2x2) support
- Traffic classification and connection establishment initiation
- Policy-based data switching
- Quality of Service (QoS) management
- Alarms management
- An SNMP agent incorporated into the unit enables extensive In-Band (IB) management of the Base Station and all its registered CPEs
- R6 interface to ASN GW profile C

The WiNetworks WiN7000 is a member of the Win-MAX E family, a line of mobile WiMAX broadband wireless access systems based on the 802.16e mobile WiMAX standard. Win-MAX E systems are designed for robustness and simplicity, offering feature-rich services with low deployment and operation costs, for unmatched operator competitiveness and fast ROI.

The WiN7000 compact base station is an ideal, cost-effective solution for wireless access services designed for point-to-multipoint broadband wireless access applications in various conditions and locations.

The WiN7000 is a one-sector base station which supports up to 800 subscriber units. By adding switch routing units, the system can be extended to as many sectors as required and can support additional subscribers and bandwidths.

The WiN7000 provides all the functionality necessary to communicate with fixed and mobile subscriber units according to the service criteria and customer Service Level Agreements (SLA), and to connect to the backbone of the Service Provider, supporting the necessary end-to-end Quality of Service (QoS).

The system uses OFDMA radio technology, which is robust in adverse channel conditions and enables Non-Line-Of-Sight (NLOS) operation. This allows for improved coverage, while maintaining a high level of spectral efficiency. Modulation and coding are continuously adapted to prevailing link conditions, ensuring an optimal balance between robustness and efficiency. The use of STC/MRC and MIMO radio technologies optimizes link performance to ensure enhance bandwidth and service coverage.

WiNetworks WiN7000 is a full outdoor base station, especially designed for simple installation and mounting on various poles, street lamps or walls. The WiN7000 includes various network interfaces for flexible integration into the operator's backbone.

The WiN7000 is supported by WiNetworks Power System - WiNPS – and by WiNetworks Management system – WiNMS.

1.3 Package Components and Unpacking

Check that the package contains:

1. WiN7000 Compact Base Station (cBST).
2. Integral 2 x omni-directional antennas (optional 90° or 120° single sector dual slant antenna including 2 x 1m antenna cables).
3. cBST pole/wall mounting kit hardware.
4. Antenna pole/wall mounting kit hardware.
5. Single Sector Power Supply (optional Multi Sector WiNPS).
6. 30m 48VDC + ETH WiN cable (optional 80m).
7. Internal GPS receiver and GPS antenna and 1m GPS antenna cable (optional IEEE1588 module).

In case of damage, contact the shipping company.

1.4 Safety Information

General

Read this User Manual and follow all operating and safety instructions.

The base station and antenna must be installed by a professional installer.

The power requirements are indicated on the product-marking label. Do not exceed the described limits.

Power supply Requirements

The power supply unit should be safety-certified according to national rules Class 2 power supply with a maximum output current of 10A.

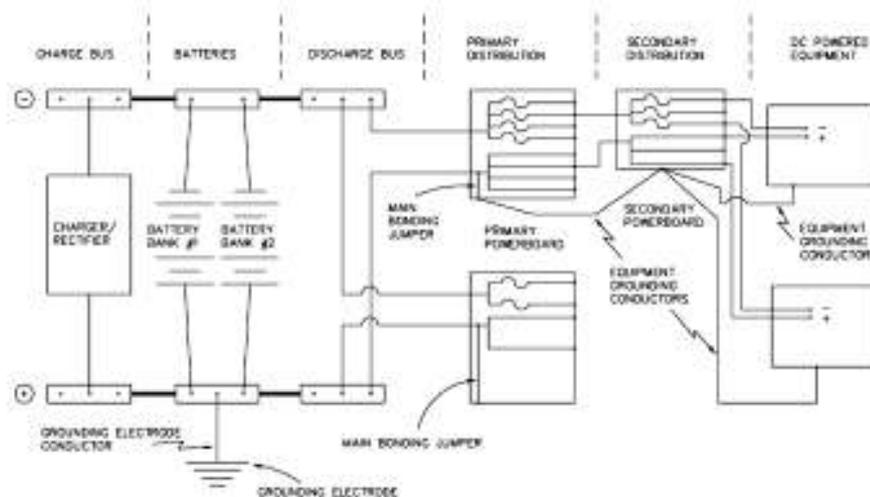
The output voltage of the power supply should not exceed 60VDC.

The output voltage should not be below 42VDC.

The disconnecting device is defined for the following modes of power connections:

- The appliance coupler of the AC/DC power supply is regarded as the main disconnecting device for the base station power when connected to the power through an AC/DC power supply.
- Circuit breaker double poles, rated 10Amp 60Vdc, shall be defined as a disconnecting device when the base station is connected to the power through batteries from a central office.

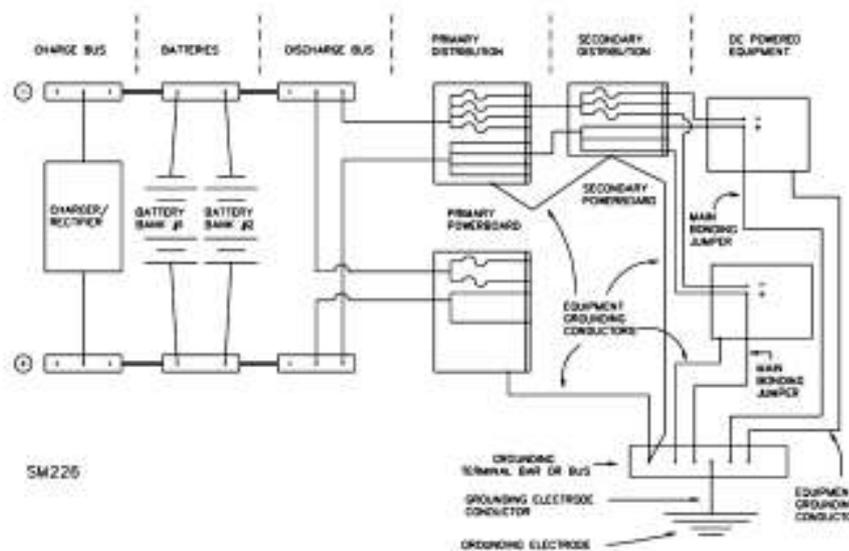
The unit is considered connected to a centralized DC power system. That is the reason that the power line should be grounded. The unit should be permanently connected to Ground with 16AWG cable or less. See figures below showing two method for power grounding (from the UL 60950-1 standard; acc. to UL 60950-22). When the unit is connected to a centralized DC Power System, the "+" side of the supply should be grounded, as per UL60950-1 and UL 60950-22 requirements, as shown in the diagrams below.



SM225

For the purpose of applying this figure, grounded and grounding are equivalent to earthed and earthing, respectively.

Figure NAB.1 – Typical centralized d.c. power system – plant and distribution source-grounded d.c. power system



SM226

For the purpose of applying this figure, grounded and grounding are equivalent to earthed and earthing, respectively.

Figure NAB.2 – Typical centralized d.c. power system – plant and distribution d.c. power system grounded at the equipment location

Equipment Installation

The equipment should be installed in accordance with the National Electrical Code (NEC), ANSI/NFPA 70, the Canadian Electrical Code (CEC), Part 1, CSA C22.1; and when applicable, the National Electrical Safety Code IEEE C2. And unless marked or otherwise identified, the Standard for the Protection of Electronic Computer/Data Processing Equipment, ANSI/NFPA 75.

RF Exposure

WiN7000 is compliant with the requirements set forth in CFR 47 section 1.1307, addressing RF Exposure from radio frequency devices as defined in OET Bulletin 65. The outdoor base station should be positioned more than 0.6 feet (20 cm) from humans.

Lightning Protection

When WiN7000 is installed in an outdoor location, all indoor components (Ethernet, power supply) should be connected through a lightning protector.

The purpose of the lightning protection is to protect people and equipment located indoors from lightning that might strike WiN7000 or its outdoor cables. Therefore, the lightning protector device should be installed indoors, as close as possible to the point where the cables enter the building. The lightning protector can also be installed outdoors, as long as the cables that go from it indoors are well protected from lightning between the box and the building entrance.

Power Cord Protection

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

Servicing

Do not open the cover of this product and attempt service unless instructed by a WiNetworks certified technician. Refer all repairs to qualified service personnel. Removing the covers or modifying any part of this device voids its warranty.

WiNetworks does not endorse or support the use of proprietary third-party outdoor cable assemblies that were not supplied by WiNetworks.

Keep out of electric power lines.

You can be killed if the antennas are in close proximity to electric power lines. Carefully read and follow all instructions in this manual. By nature of the installation, you may be exposed to hazardous environments and high voltage. Use caution when installing the outdoor system.

Antenna Grounding Requirements

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

Outdoor Grounding System

Verify that the base station is grounded.

The system must be properly grounded to protect against power surges and accumulated static electricity. It is the installer responsibility to install this device in accordance with the local electrical codes.

User ports and power supply

If length of communication lines outdoor exposed wiring greater than 40 m (140 feet) is applicable, these lines must be treated as TNV-1 circuits. The installer must ensure that the power supply and network ports are designed for full compliance with TNV-1 telecommunication network.

Caution

To reduce the risk of fire , use only no. 26AWG or larger telecommunication line cord.

NOTE:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Changes or modifications to this equipment not expressly approved by WiNetworks Ltd. could void the user's authority to operate the equipment.

2

Product Description

2.1 Introduction

The WiN7000 base station is an IEEE 802.16-2005 compliant wireless device designed for the deployment of point-to-multipoint (PMP) network architectures.

The WiN7000 base station is an outdoor device. Each Win-Max™ network segment is comprised of a WiN7000 base station and one or more WiMAX Forum 802.16e Wave 2 Certified subscribers. Each subscriber registers and establishes a bi-directional data link with the sector controller of the base station.

WiN7000 base station is part of the 802.16e Access Service Network (ASN). It functions as a central hub or concentrator, connected to a Core Services Network (CSN) through the Access Service Network Gateway (ASN-GW), managing wireless links for fixed, nomadic and mobile subscribers. The WiN7000 base station enforces the Quality of Service (QoS) settings by controlling all uplink and downlink traffic scheduling, providing non-contention based traffic with predictable transmission characteristics.

2.2 IEEE 802.16e Mobile WiMAX Compliance

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

The WiN7000 base station is compliant to IEEE 802.16-2005 WiMAX forum Wave 2 profile.

Note

802.16e standards are subject to amendment, and Win-Max™ product family design compliance applies to a specific revision of the standard. The Win-Max™ product family does not support mesh communication (direct subscriber-to-subscriber).

WiNetworks is an active member of the WiMAX Forum™ and participates in interoperability testing in the WiMAX Forum.

2.3 Block Diagram

WiN7000 consists of the following modules:

1. Base-Band Board – including the WiMAX 16e MIMO Base-Band SoC plus the network interface (Gb-ETH Switch) plus the analog front-end that interface to the RF module.
2. Timing Module – Clock source for the BST modules. Can be either GPS receiver or IEEE1588 (IP packet sync).
3. CPU Module – High performance CPU with its memories, that runs the WiMAX 16e MAC plus the Layer 3 - Networking stacks that runs above the WiMAX MAC. The CPU is responsible for the management (control, configuration and maintenance) of all the BS modules.

4. 2 x RF Board – Each board consists of single transmit/receive module that modulate the analog WiMAX signal input from the Base-Band modem to the high frequency RF output. Several RF modules exist - each supporting different frequency band.
5. 2 x PA Board – Power Amplifier module that amplifies the RF signal from the RF output to the desired transmit output power. Several modules exist, supporting the different frequencies and several transmit levels.
6. Power Supply – DC/DC power supply. Converts the 48VDC to the various voltages that are feeding the Digital and the RF modules.
7. Chassis: 140W power dissipating aluminum box.
8. Antennas: Two Antennas to support the MIMO schemes. Several antennas option exists (e.g. External 65/90/120 Sectors, Integral Omni).

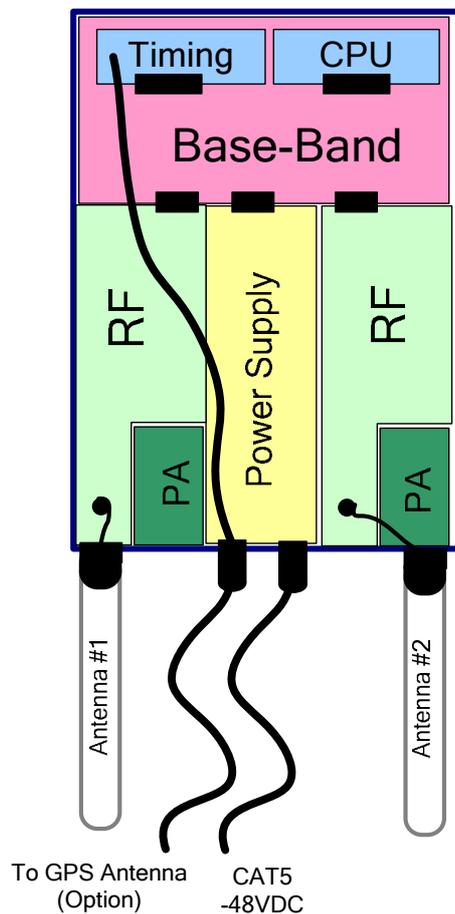


Figure 2-1: WiN7000- Block Diagram

2.4 Features

2.4.1 Mobile WiMAX Wave 2 MIMO Features

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

In point-to-multipoint systems employing MIMO, each base station antenna transmits a different data stream and each subscriber terminal receives various components of the transmitted signals with each of its subscriber antennas as illustrated in the figure below. By using appropriate algorithms, the subscriber terminal is able to separate and decode the simultaneously received data streams.

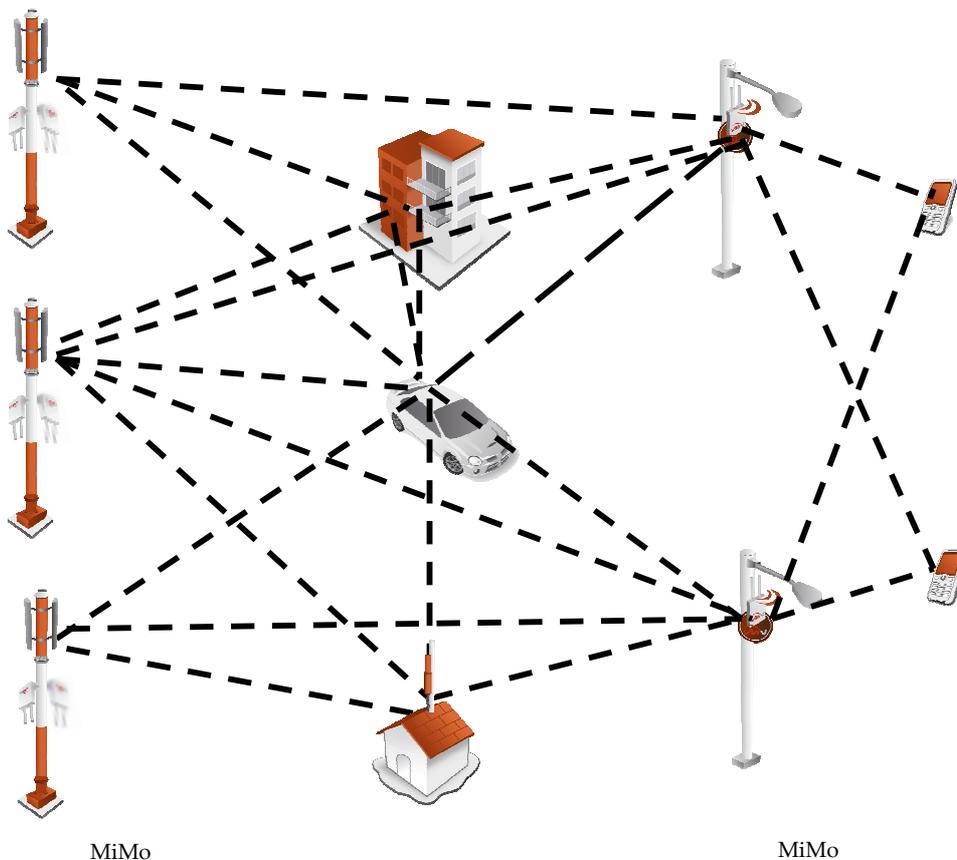


Figure 2-2: MiMo Antenna System

2.4.1.1 Space-Time Coding

Space-time coding (STC) is a technique for implementing transmission diversity. Mobile WiMAX uses transmit diversity in the downlink direction to provide spatial diversity that enhances the signal quality to a specific subscriber located anywhere within the range of the antenna beam. Although providing less signal gain than beam-forming, transmit diversity is more robust for mobile users since it does not require prior knowledge of the path characteristics of a subscriber's particular frequency channel. One such STC technique, known as the Alamouti Code, was published in 1998[4] and has been incorporated into the WiMAX 16e standard.

2.4.2 Security

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

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

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

There are two major differences between the standards. The first difference is that the security mechanism of the IEEE 802.16-2004 is based on the DOCSIS standard. In the 802.16e-2005 many changes have been made in the security mechanisms. The second difference is in the flexibility of SS's connection characteristics with the BST. The IEEE 802.16-2004 only supports fixed access. In fixed access, an SS cannot mitigate to the air interface of a new Base Station (BST) without performing the network entry again after a connection termination. The IEEE 802.16e-2005 supports mobile access. Mobile access enables an SS to move between various BST cells while keeping the connection established.

There are five primary aspects of WiMAX security that should be considered when designing a security plan for a WiMAX network. These range from mitigation techniques at the physical layer to improved wireless authentication and encryption to intrusion protection and data transport security. At each level, choices in implementation and security levels can be made; although in the case of the physical layer options are limited.

2.4.2.1 Physical Layer Security

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

Since most WiMAX network services are delivered over licensed bands (currently 3.5 GHz internationally and 2.5 GHz both internationally and in the US), this offers spectrum relatively quiet from accidental interference. Accidental interference in licensed spectrum cannot always be completely discounted as there is a possibility of second and third harmonic interference waves, for example, from much lower frequency signals if those are in close proximity to the WiMAX antenna systems or that cross them with a signal close enough in physical proximity to locally overload the WiMAX signal. In practice, this is rare.

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

While it may seem the physical layer is inherently most vulnerable as the security elements of WiMAX are located at higher layers, the fact is hackers can often find lower hanging fruit in terms of useful exploits higher in the stack, because as WiMAX supports multiple selections on what service providers can choose to implement in terms of authentication, sometimes the door can be left open for them by the choices made.

2.4.2.2 Authentication

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

A second, newer and much better choice, embraced by the Win-Max™ system, is the built in support for X.509 device certificates embedded with the use of extensible authentication protocol--transport layer security (EAP-TTLS) method, added with the 802.16e standard and WiMAX Forum.

Enter the EAP-TLTS authentication method. This technique allows both the subscriber and the base station to authenticate each other using an X.509 method for both, in addition to a subscriber authentication which is based on well-known subscriber authentication techniques such as PAP and MS-CHAP. MAC control headers are never encrypted in WiMAX, however with EAP carriers can choose to authenticate them (but they don't necessarily have to). This capability adds an additional layer of authentication confirmation. It's an operator specific guideline decision and is tunable in the Win-Max™ system.

2.4.2.3 Encryption

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

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

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

The downside to these heavy computing tasks (i.e. authentication and encryption) is that all of this requires processor cycles, which may affect the performance of the system. Nevertheless, the Win-Max™ system and especially, the SS and BST which are the entities that take active role in heavy security-related computations, were built bottom to top with a design goal of offloading heavily computing tasks from the host processor to a specific circuit. Consequently, no performance degradation is neglected.

2.4.2.4 Third-Party Intrusion Protection

We examined WiMAX authentication schemes, which are a major component of a secure network. And we also spoke of data encryption. Clearly, WiMAX possesses solid tools already built in. But there are considerations beyond just good security that can drive a migration to third party intrusion detection and protection tools---namely business case elements. Intrusion protection is however, not data protection. These are two different classes of solution. Certainly a good third party intrusion protection can monitor and secure a network's authentication. However, many solutions also offer worm protection, Trojan horse protection, defenses against viruses, backdoor exploits and denial of service attacks to name a few. Some of these elements are almost a business necessity for a wireless service provider and may justify the cost of an additional security suite initially. For other companies, a migration strategy to enhanced tools makes the most cost effective sense.

A good place to start is examining market and service scenarios. If your customer base is highly sensitive to data integrity (financial sector or hospital customers) third party intrusion prevention systems can help segment customers from each other better as well as secure them from outside attack.

Or in another example, a mobile network that offers just Internet access and voice may wish to abrogate responsibility for data encryption and use session initiation protocol (SIP) signaling for its VoIP and WiMAX native authentication tools.

Referring to encryption, clearly an AES supported data encryption system gives WiMAX excellent security in this regard. However, additional solutions that meet customer needs

such as virtual private networks may enhance the business model and provide additional source of revenue.

In the following two clauses, two revolutionary applications targeted at specific market segments are described. These applications of WiMAX for DBS & DVB-T operators and WiMAX for Cable operators distinguish WiNetworks from other players in the WiMAX industry.

Network Access Providers can easily provide fast Internet and advanced data service to their deployed network by using the WiNetworks WiMAX-based technology solution.

2.4.3 Time Division Duplexing (TDD)

The WiN7000 base station uses time division duplexing (TDD) to transmit and receive on the same RF channel. This is a non-contention based method for providing an efficient and predictable two-way PMP cell deployment. All uplink and downlink transmission scheduling is managed by the base station. The base station sends data traffic to subscribers, polls for grant requests, and sends grant acknowledgements based on the total of all traffic to all subscribers.

2.4.4 Coding Rate

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

2.4.5 Modulation

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

2.4.6 Error Code Correction

Error correction techniques have been incorporated into WiMAX to reduce the system signal to noise ratio requirements. Strong Reed Solomon FEC, convolutional encoding, and interleaving algorithms are used to detect and correct errors to improve throughput. These robust error correction techniques help to recover erroneous frames that may have been lost due to frequency selective fading or burst errors. Automatic repeat request (ARQ) is used to correct errors that cannot be corrected by the FEC, by having the erroneous information resent. This significantly improves the bit error rate (BER) performance for a similar threshold level.

The WiN7000 supports two Forward Error Correction (FEC) types: CC and CTC.

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

Convolutional Turbo Code (CTC) error correction is supported for all traffic rates. The CTC has better performance than the CC.

2.4.7 Time Synchronization

When operating two or more collocated base stations, transmitter operations **MUST** be synchronized to minimize inter-sector interference and inter sites interferences due to the TDD use. Each base station sector has a GPS receiver or optionally IEEE1588 compliant synchronization module. External GPS antenna must be connected to the GPS port located on the connector panel when a GPS receiver option is used.

2.5 Deployment Models

The base station supports point to multipoint (PMP) deployment scenario.

2.5.1 PMP Deployment

When deployed in a PMP configuration the base station establishes bi-directional links to more than one subscriber. PMP deployments typically use a wide beam (sector) antenna at the base station and a narrow beam antenna at the subscriber. Service flows are used to police service-level agreements for each subscriber.

2.5.2 Non Line-of-Sight

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

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

2.5.3 Channelization

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

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

2.6 Service Flows

Service flows are a key feature of the 802.16e standard.

A service flow represents a unidirectional data flow. Transmitting bidirectional traffic requires that two service flows be defined: one for the uplink, and another for the downlink. These service flows can have different QoS settings.

The base station allows multiple service flows to be configured for each subscriber in a sector. This allows service providers to offer different services, and segregate traffic flows having different QoS requirements.

A service flow is partially characterized by the following attributes:

1. A 32-bit Service Flow ID (SFID) is assigned to all existing service flows. The SFID serves as the principal identifier for the Service Flow and has an associated direction.
2. A 16-bit Connection ID (CID) is associated with each active SFID (connection active).
3. A set of QoS parameters specifying the required resources. The principal resource is bandwidth, but the specification may also include latency requirements.
4. A set of QoS parameters defining the level of service being provided.

2.6.1 Service Flow Classification

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

2.6.2 Dynamic Service Addition

Service flows are defined and stored in the base station. For each service flow to be established, the base station sends a setup message to the subscriber specifying the required set of QoS parameters. The subscriber responds to each request by accepting or rejecting the setup message.

A service flow may be pre-provisioned or can be dynamically created and deleted without service outage. This is useful for supporting multiple subscribers in a single sector. New subscribers can be added and existing subscribers can be removed or have service levels modified.

Setup messages are sent by the base station following any subscriber power-cycle, loss and recovery of the wireless link to a subscriber, or any service flow add/delete operation at the base station.

2.6.3 Default Service Flows

Default UL/DL service flows are created automatically for each registered subscriber.

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

2.6.4 Scheduling

The base station scheduling algorithm uses two scheduling passes. On the first pass, the scheduler attempts to allocate bandwidth to meet the minimum rates for all active service flows. If there is available bandwidth remaining at the end of the first pass, the scheduler executes a second pass and attempts meet all specified maximum rates. During both passes, bandwidth allocations are assigned based on the following order of assessment:

1. Priority of the scheduling service type, from highest to lowest (rtPS first, and then BE).
2. Traffic Priority setting when multiple service flows have the same service type.

Wireless transmission bandwidth is optimized by granting allocations based only on traffic available for immediate transmission: only the required bandwidth is allocated, and idle service flow channels do not receive any bandwidth allocation

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

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

Real-Time Polling Service (rt-PS)

The base station schedules a continuous regular series of transmit opportunities for the subscriber to send variable size data packets. The grant size is based on the current data transfer requirement. Typical applications include streaming MPEG video or VOIP with

silence suppression. This is efficient for applications that have a real-time component and continuously changing bandwidth requirements.

Extended Real-Time Polling Service (ert-PS)

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

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

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

Best Effort (BE)

The base station schedules transmit opportunities for the subscriber to send traffic based on unused bandwidth after all higher-level traffic-scheduling requirements are serviced.

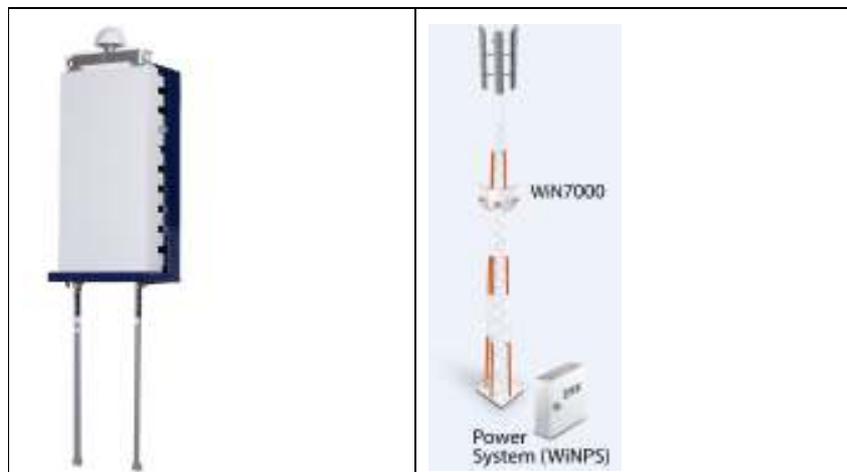
Typical applications may include Internet access and email. Best effort service flows can be assigned a priority of 0 to 7.

Unsolicited Grant Service (UGS)

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

2.7 Physical Description

The WiN7000 outdoor base station is packed in a waterproof metal housing. Mounting bracket and mounting kit supplied with the equipment support ease of installation at various sites.



WiN7000 with 2 Omni-directional Antennas	WiN7000 with External Antennas
--	--------------------------------

Figure 2-3: WiN7000 Outdoor Base Station Mounted – General View

The WiN7000 housing holds the connection panel detailed below.



Figure 2-4: WIN7000 – Top View

Dimensions: 60cm x 27cm x 10cm

Weight: <15 Kg

The interconnection panel holds the external connectors used to connect the equipment to the network, power supply and antennas as illustrated below. The interconnection panel holds 6 connectors. Detailed description of these connectors can be found in Section 4 of this document.



Figure 2-5: WiN7000 Interconnection Panel

3

Mounting

3.1 General

When choosing mounting locations for the antenna, consider the available mounting structures and antenna clearance. WiN7000 should be mounted downward to provide better weather protection.

The cBST is equipped with a mounting kit, which allows for several mounting options such as the following examples:

1. Poles
2. Towers
3. Walls

The following antenna options are provided:

1. 2 x Integrated Omni-directional antenna (default)
2. External Sector dual slant $\pm 45^\circ$ antenna (optional)

The following figure illustrates various mounting options.

		
<p>Pole Installation 1 Base Station with integrated 2 x omni-directional antennas</p>	<p>Tower Installation 3 Base Stations with 3 external sector antennas</p>	<p>Wall Installation 1 Base Station with integrated 2 x omni-directional antennas</p>

3.2 Site Survey

Due to variations in component configuration, placement, and physical environment, each installation is unique. Before installing the WiN7000, perform a site survey to determine the optimum placement of units for maximum range, coverage, and network performance. Consider the following factors when performing a site survey:

- Data rates—Sensitivity and range are inversely proportional to data bit rates. The maximum radio range is achieved at the lowest workable data rate. A decrease in receiver threshold sensitivity occurs as radio data rate increases.
- Antenna type and placement—Proper antenna configuration is a critical factor in maximizing radio range. As a rule, range increases in proportion to antenna height and gain.
- Physical environment—Clear or open areas provide better radio range than closed or filled areas. The less cluttered the operating environment, the greater the range.
- Electric power considerations
- Regulations (Max Power, EIRP)

Most wireless networks include many CPEs and BSTs installed in various locations in an overlapping radio-cell pattern. It is important to select carefully each CPE's location and radio channels. Therefore, a site survey becomes an essential first step before physically deploying the WiMAX solution.

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

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

Recommended Site Requirements

It is highly recommended that the WiN7000 BSTs be mounted near the edge of the roof of a tall building. The WiN7000 BSTs should be pointed in the direction of the area to be covered. To provide maximum coverage, multiple WiN7000 BSTs can be installed on the same rooftop. However, it is important to leave some distance between each unit in order to prevent interference between the units themselves. When choosing the ideal location, it is also important to take into consideration the overall area topology.

3.3 Pole Mounting

Select a mounting location. You can attach the WiN7000 to any pipe or pole with diameter 1.75" to 10"

3.4 Wall Mounting

Select a mounting location. You can attach the WiN7000 to any wall that can support the load of the WiN7000 cBST.

3.5 Tower Mounting

Select a mounting location. You can attach the WiN7000 to any tower that can support the load of the WiN7000 cBST. The tower mounting is analogous to wall mounting.

4

Installation Procedures

4.1 Safety Hazards



Warning:

Installing WiN7000 can pose a serious hazard. Be sure to take precautions to avoid the following:

Exposure to high voltage lines during installation

Falling when working at heights or with ladders

Injuries from dropping tools

Contact with AC wiring (power system connection)

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

4.2 Installation Tools

1. Screwdriver
2. Wrench
3. Driller
4. Hammer

4.3 Installing the WiN7000

Important

The equipment should be installed in accordance with the National Electrical Code (NEC), ANSI/NFPA 70, the Canadian Electrical Code (CEC), Part 1, CSA C22.1; and when applicable, the National Electrical Safety Code IEEE C2. And unless marked or otherwise identified, the Standard for the Protection of Electronic Computer/Data Processing Equipment, ANSI/NFPA 75.

The installation involves the WiN7000 device and the mounting bracket. The mounting bracket should be installed first, followed by WiN7000, which should be inserted into it, as explained below.

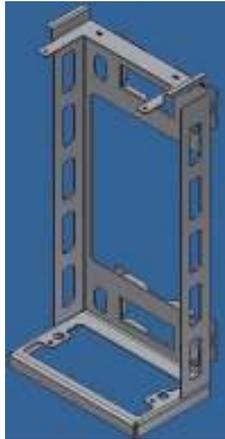


Figure 4-1: Mounting Bracket

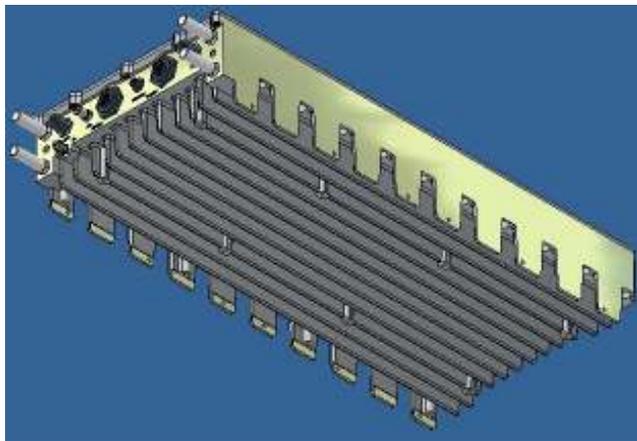


Figure 4-2: WiN7000

Use the connecting panel on the lower side of the WiN7000 to attach cables to the device. See Section 4.3.4 for details

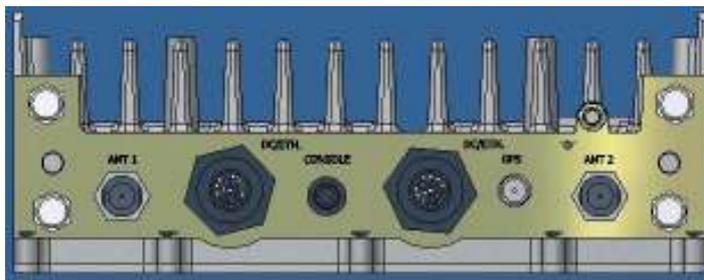


Figure 4-3: Connecting Panel

4.3.1 Pole Mount

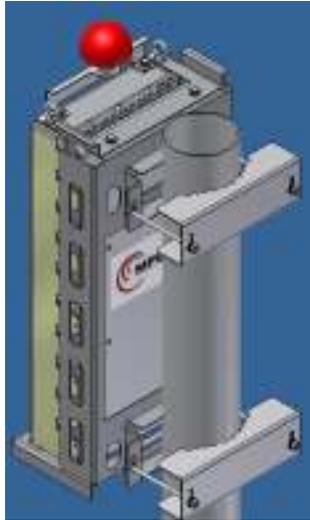


Figure 4-4: Pole Mount: Base station fully mounted – rear view

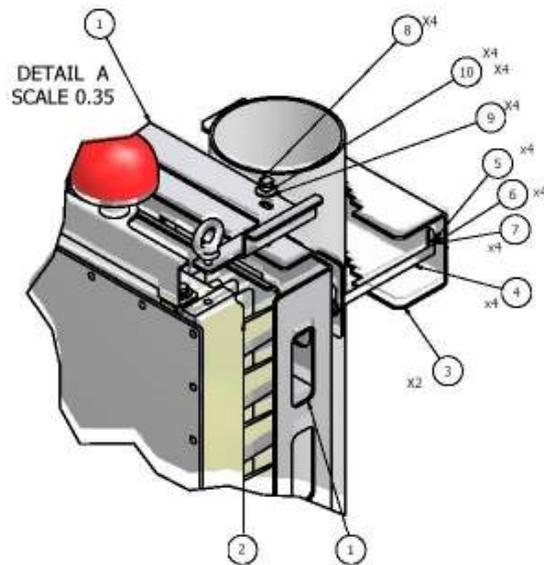


Figure 4-5: Pole Mount: upper connections

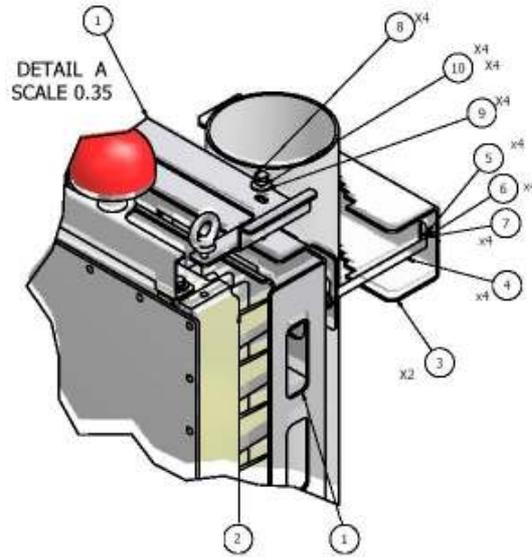


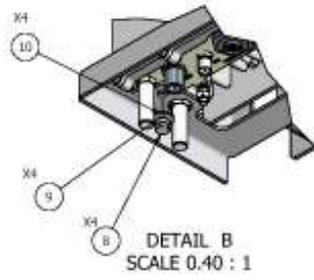
Figure 4-6: Pole Mount: lower connections

The following table lists the required parts.

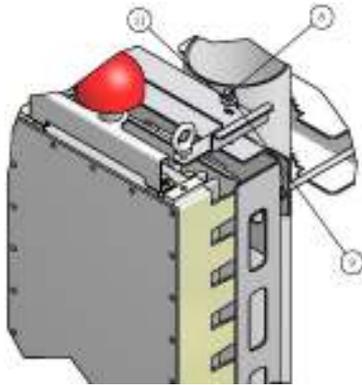
Parts List			
ITEM	QTY	PART NUMBER	DESCRIPTION
1	1	MPH00480	mount for win
2	1		MPH004700-WINNETWORKS RADIO ASSEMBLY
3	2	MPH00508	MOUNTING BRACKET
4	4	MSH00011	SCREW 5/16 HEX CAP X 6"
5	4	MNH12106	NUT NF5/16 HEX
6	4	MWH12110	WASHER FLAT 5/16
7	4	MWH12111	WASHER SPRING 5/16
8	4	MSH12510	SCREW NC1/4 X 1/2 HEX 10.8
9	4	MWH12109	WASHER FLAT NC1/4
10	4	MWH12210	WASHER SPRING NC 1/4
11	1	pole	pole

To install the Win7000 on a pole:

1. Select a mounting location on the pole.
2. Attach the mounting bracket at this location using the fastening brackets and the MSH00011 screws.
3. Lift the base station by its round bolts (ears) and place it on the mounting bracket's base.



4. Attach the top mounting bracket with the two bolts.



4.3.2 Wall Mount

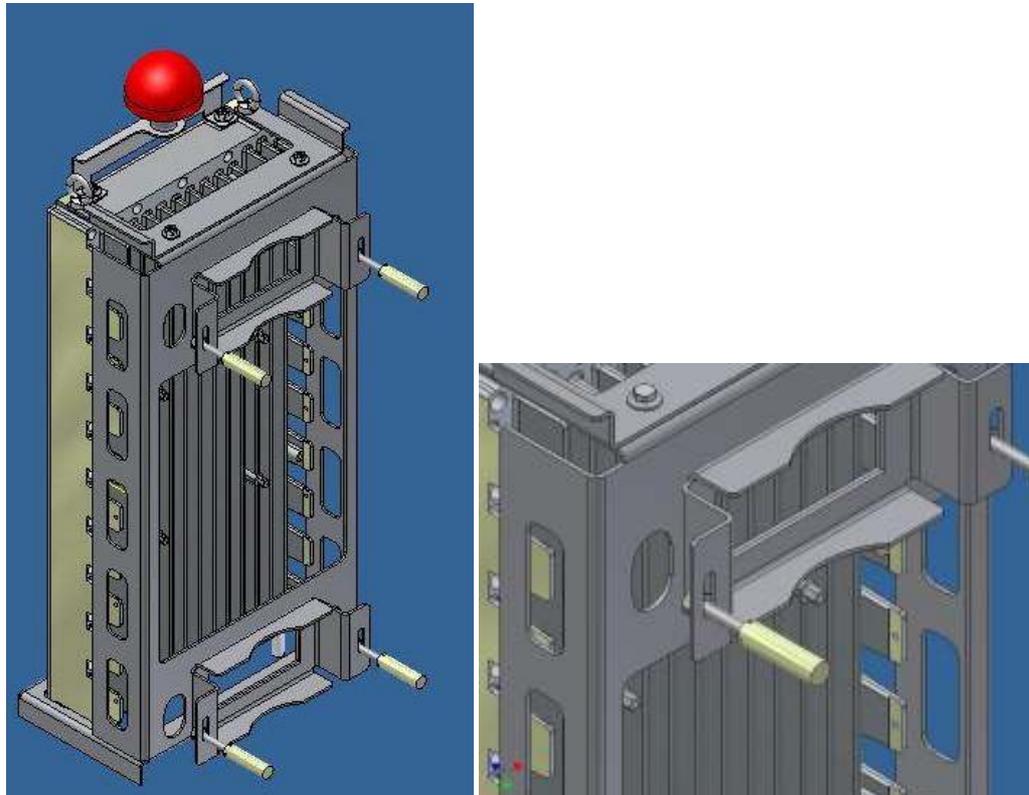


Figure 4-7: WiN7000 – Wall Mount

To install the WiN7000 on a wall:

1. Select a mounting location on the wall.
2. Place the mounting bracket on the wall and mark the location of four holes (two at the top and two at the bottom).
3. Drill the four holes for the fastening inserts (use 5/16 inch drill).
4. Insert the fastening inserts type NC ¼ into the holes.
5. Insert four flat washers, four spring washers, four screws type NS1/4 X ½ HEX via the holes on the mounting bracket.
6. Attach the mounting bracket at this location.
7. Fasten the screws.
8. Hold the WiN7000 by the ears on both sides and slide it into the mounting bracket with care.
9. The ears should match the ridge of the mounting bracket.

10. Insert the nuts (at both sides of the mounting bracket) until it matches the treads of the WiN7000 enclosure.
11. Insert the nuts and fasten them using a wrench,

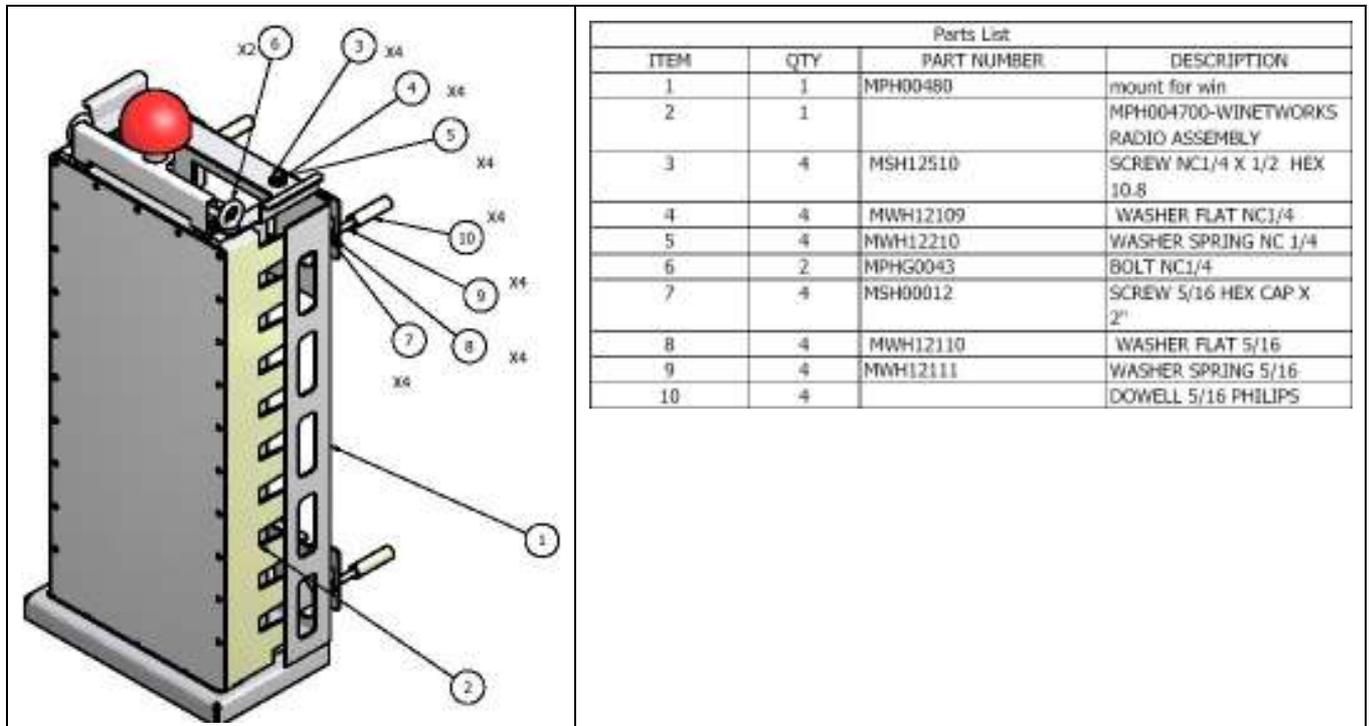


Figure 4-8: WiN7000 –Wall Mount - Assembled

4.3.3 Tower Mount

Follow the same procedure as wall mounting. Make sure that the tower can hold the load of the cBST.

4.3.4 Cable Connections

The following illustration shows the connectors on the lower panel of the WiN7000.

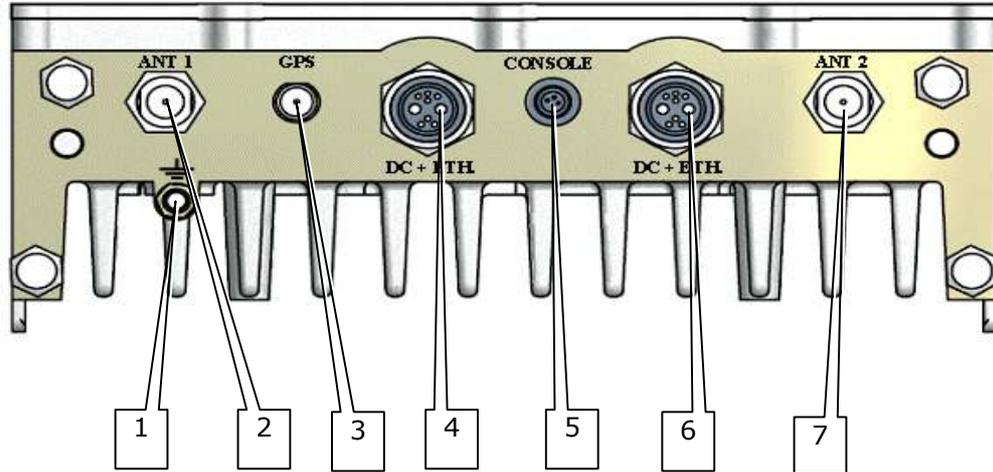


Figure 4-9: Interconnection Panel

Table 4-1: List of Connectors and Cables

No.	Design.	Connector Type	Cable Type	Function	Connected to
1	GND	2 screws ETSI	#10 AWG bare copper wire	Grounding	Central earth ground, Tower or pole chassis
2	ANT1	N type Female	RG 214/U	Connected to external antenna or screw omni-directional antenna	Antenna
3	GPS	TNC Female		Base Station Synchronization	GPS antenna
4	DC + ETH		Proprietary WiN cable	48 VDC/ Return / 5A + Ethernet Cat5	power supply + Network/Router/Switch
5	Console	3-pin	RS-232	Low level CLI for technicians	PC
6	DC + ETH		Proprietary WiN cable	48 VDC/ Return / 5A + Ethernet Cat5	Optional Multi sector base station Daisy Chaining
7	ANT2	N type Female	RG 214/U	Connected to external antenna or screw omni-directional antenna	Antenna

4.3.5 Power Cable

The pin-out of the power cable is shown below:



Pin Number	Type
1	NC
2	48VDC (RTN)
3	+TX Ethernet
4	- TX Ethernet
5	+RX Ethernet
6	48VDC (+)
7	NC
8	NC
9	- RX Ethernet

Figure 4-10: Power Cable Pin-out

4.3.6 Console Cable

Important

The console connector should be closed in normal condition and may be used only occasionally by an authorized technician.

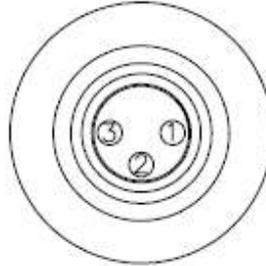
The chassis has a 3-pin maintenance female connector, used by a technician to connect a “console”.

The port is used by a maintenance person to communicate with the processor when the normal management interfaces cannot be used. The console port is based on RS-232 serial standard and support a standard terminal connection.

The technician can configure and monitor the base station through CLI (Command Language Interface) for low level debug.

The connector is shown in the following figure:

Figure 4-11: Console Connector



The maintenance connector pin out is listed in the following table:

Table 4-2: Maintenance connector

Pin Number	Type
1	TX
2	RX
3	GND

Cable type: 3 wires 28AWG

Cable connectors: DB9F, proprietary 3 pin console connector

Cable length: 2m

The cable is supplied by Winetworks.

4.3.7 Antenna Cable

Important

The part of antenna that is connected to the central pin of antenna connector should be covered by isolation material which is sufficiently resistant to degradation by ultra-violet (UV) radiation.

4.4 Power Connections

WiN7000 is supplied with +48/-48VDC via an external power system.

The power system type can be indoors or outdoors.

The power system can be supplied by WiNetworks (WiNPS) or by the operator.

Refer to power system's user manual for specific power connection to the main (AC) local power outlet.

Connect the WiNPS power system DC + ETH output to the WiN cable connector (supplied by WiNetworks).

Connect the other side of the WiN cable connector to the DC + ETH connector of WiN7000.

For more information, please refer to WiNPS specification and user manual.

The illustration below shows the physical connection between the WiN7000 cBST, the power system and to the AC power source.

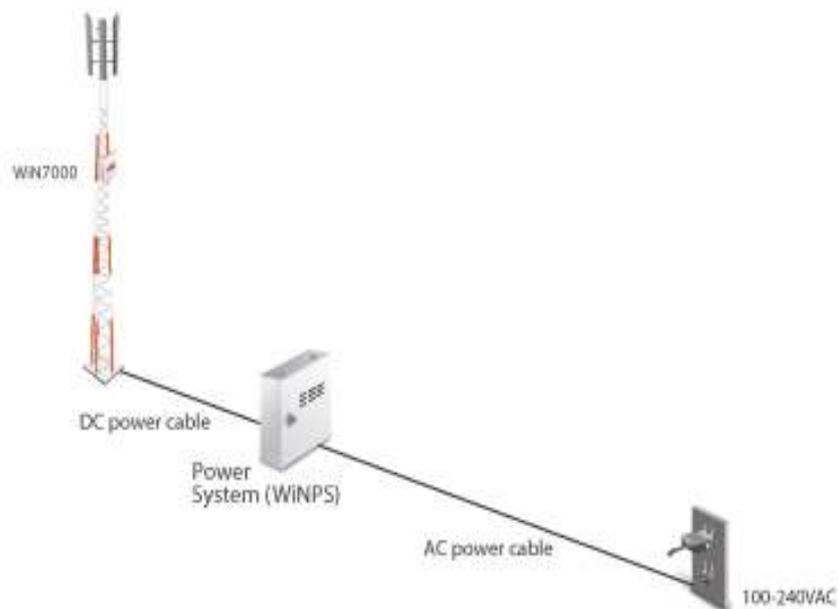


Figure 4-12: cBST Power Connection

4.5 Multi-sector Base Station Daisy Chain

The cBST supports daisy chain architecture for low-cost modular multi-sector base station sites.

The cBST chassis has 2 x Power and Ethernet (marked: DC + Eth) combo connections supporting a multi-sector base station daisy chain architecture.

The two combo connections have the same functionality and both can serve as input to the base station or output from the base station towards the next daisy chained base station. The chassis has no means of protection (fuses, switches etc.) for the power channeled to the chained unit.

One combo connector should be connected to the power source and the Ethernet aggregator (WiNPS). The other combo connector in the first BS should be connected to the combo connector on the other BS, and so on.

The maximum length of all parts of the daisy chain cables should not exceed 100m.

Figure 4-13 shows the physical daisy chain connection between 3 x WiN7000 cBSTs. The length of A + B + C should not exceed 100m.

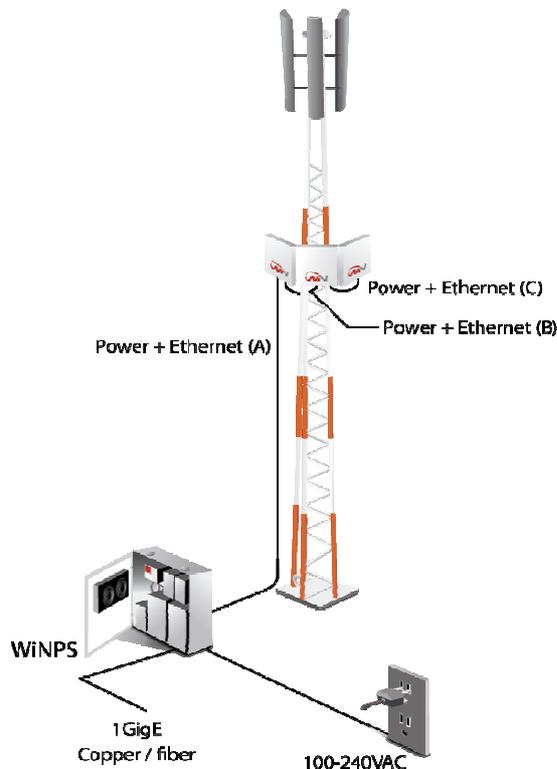


Figure 4-13: cBST Daisy Chain Connection

5

Equipment Configuration and Monitoring

5.1 Configuring WiN7000

5.1.1 Basic Configuration

WiN7000 cBST can be monitored and controlled with a standalone PC or through a management system (WiNMS) using the backhaul interface.

1. Use your Web browser to access 192.168.100.100.
2. In the Login window, enter username= vendor, password= vendorpass.
3. Choose the Private tab and select "setIPAddr" to set the data and management IP addresses.

Field Name	Type	Description	Value
Management	ENUM	in-band / out-of-band	out-of-band
Data_Type	ENUM	Static / Dynamic	Static
Data_IpAddress	STRING	Enter Ip Address	15.0.0.2
Data_NetworkMask	STRING	Enter Network Mask	255.255.255.0
Data_DefaultGateWay	STRING	Enter DefaultGateWay	15.0.0.1
Management_IpAddress	STRING	Enter Ip Address [Only for out_of_band management]	192.168.0.100
Management_NetworkMask	STRING	Enter Network Mask [Only for out_of_band management]	255.255.255.0
Management_DefaultGateWay	STRING	Enter DefaultGateWay [Only for out_of_band management]	
DefaultRouterMac	STRING	Enter the Default Router MAC (i.e. 00:11:22:33:44:55)	

Figure 5-1: setIPAddr Screen

The base station has a data and a management interface, each having a dedicated IP address. In Management, enter 0 (in-band – the management IP is included in the data network), or 1 (out of band, management IP external to the data network).

Note

In "out of band" mode, the Management IP address must be from the same IP address block as the IP address of the SNMP Server (WiNMS). In addition, the Auto Manager IP address must be from the same IP block as the IP address of the Management Interface.

In Data_Type, specify whether the Data IP address is static (0) or dynamic (1). The Management IP address is always static.

If you selected to work with static IP addresses, in the Data_... and Management_... fields enter the relevant information.

4. Check the entered information through the "showIPAddr" menu.
5. Choose the Mac tab and select "setMacUI".
6. In the frequency field set the frequency of the uplink transmission (CPE to base station) in KHz.

Parameter	Type	Range	Description
rng-backoff-start	INT	[0->15]	initial ranging backoff start
rng-backoff-end	INT	[0->15]	initial ranging backoff end
p-rng-backoff-start	INT	[0->15]	periodic ranging backoff start
p-rng-backoff-end	INT	[0->15]	periodic ranging backoff end
lwr-backoff-start	INT	[0->15]	request backoff start
lwr-backoff-end	INT	[0->15]	request backoff end
reservation-timeout	INT	[1->32]	reservation timeout after sending a bandwidth request
frequency	INT		frequency of the UL in KHz
permutation-base	INT	[0->62]	Uplink Permutation base parameter (ULPermBase in the standard)
subchannel-bitmap	STRING		Uplink Subchannel Bitmap (hex) - 0 to activate all subchannels
ranging-code-group-start	INT	[0->255]	Start of the ranging code range (parameter S)

Figure 5-2: setMacUI Screen

Leave all other fields blanks (default).

Note

The frequency of the UL should match the frequency of the DL configuration

7. Select the "setMacDI" command.

Parameter	Type	Range	Description
tx-power	INT		BS transmission power (dBm)
init-ranging-max-rx-power	INT		Initial ranging Max. Received Signal Strength at BS (dBm)
frequency	INT		frequency of the DL in KHz (Invalid in license-exempt operators)
version	ENUM		802.16 version
bsRestartCount	INT	[0->255]	BS restart count
bs-id	STRING		BS ID (MAC Address)
luc0-fec-code	ENUM		the system fec-code (QPSK)
luc1-fec-code	ENUM		the LLC 1 fec-code
luc2-fec-code	ENUM		the LLC 2 fec-code
luc3-fec-code	ENUM		the LLC 3 fec-code
luc4-fec-code	ENUM		the LLC 4 fec-code

Figure 5-3: setMacDI Screen

In the frequency field, set the same frequency as the uplink frequency for downlink transmissions (base station to CPE).

In the tx-power field, set the transmission power (in dBm).

Leave all other fields blanks (default).

Note

The frequency of the UL should match the frequency of the DL configuration

8. Choose "SetMacFrame", to set the bandwidth of the channel.



Figure 5-4: SetMacFrame Screen

Follow these steps:

- a. In the started field set the value to "0" to stop the WIMAX protocol messages.
- b. Then, in the bandwidth field set the bandwidth of the channel to one of the pre-defined values.
- c. Lastly, in the started field set the value to "1" to start the transmission.
- d. Leave all other fields blanks (default).

Note

The frequency and bandwidth configuration should be the same in both cBST and CPE

9. SNMP management: (in the Tools tab).

Select "addSNMPAccess". Set the Read community to "public" and the Write community to "private".

Figure 5-5: addSNMPAccess Screen

In User Level, select 1 (Manager) to grant Manager rights to users wishing to work with SNMP. Choose the User Level (1-Manager), and press "CALL".

Select "addAuthorizedManager" and set the IP address of the computer authorized to access SNMP.

Figure 5-6: addAuthorizedManager Screen

You can define more than one authorized computer: Click the Call button and enter another IP address. Repeat this step as many times as needed.

10. From the Tools tab, select the restart command and click on the Call button to reboot the base station.



Figure 5-7: Restart Screen

5.1.2 Monitoring

1. The "showSs" command is designed to display read-only information about a CPE. Select the SS tab and then select the "showSs" command.



Figure 5-8: showSs Screen

2. Do one of the following:

Just click on Call to see all of the CPEs connected to the base station.

You can access the details of a specific CPE by entering its MAC address or its CID, and clicking on Call.

3. Enter 1 in the verbose field to see the full details of the CPEs. Enter 0 to see concise details.

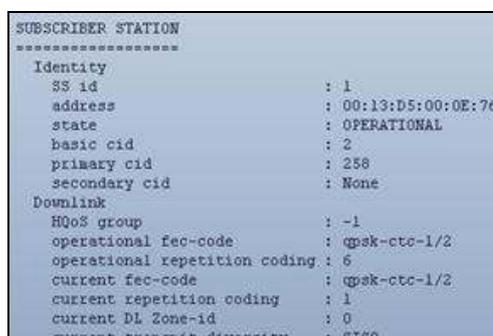


Figure 5-9: Verbose CPE query

4. Use the "showSsPhyStatUI" and "showSsPhyStatDI" commands (SS menu) to display physical statistics on the uplink and on the downlink respectively.

Figure 5-10: showSsPhyStatUI screen

5. Do one of the following:

Just click on Call to see the physical statistics of all of the CPEs connected to the base station.

You can access the physical statistics of a specific CPE by entering its MAC address or its CID, and clicking on Call.

```

SS UL PHYSICAL STATISTICS
=====
RANGING STATISTICS
Slots quantity (Sp)           : 1
Frequency (Hz)                : 28
Power per subcarrier (dBm)    : -99.76
Max. RSSI on the burst (dBm)  : -85.96
subchannel quantity on the burst : 1
CINR (dB)                     : 26.45
FEC code                      : qpsk-ctc-1/2
Repetition factor             : 1

```

Figure 5-11: showSsPhyStatUI, showSsPhyStatDI physical statistics display

6. The status of the service flows can be monitored using the "showSF" command.

Figure 5-12: showSF Screen

7. Do one of the following:

Just click the Call button to display a list of SFs.

Enter an sfID or a CID to focus on a specific SF.

Note

Entering 1 in the verbose field displays detailed information. Enter 0 to display concise information.

5.2 Configuring WiN7000 for MIMO

The Multiple In, Multiple Out technology allows the base station and the CPEs to process incoming and outgoing signals from multiple transmitters and receivers simultaneously in order to increase bandwidth without expanding the available resources. This section explains how to configure the base station for MIMO.

The system can work in MIMO and non-MIMO mode simultaneously.

1. First, you need to enable MIMO. Select the "AddDLZone" command.

Parameter	Value	Description
after-zone-id	INT [0->6]	Insert the new zone after the one with the console specified
use-all-subchannels	INT [0->1]	use all subchannels (also to default)
dl-permibus	INT [0->31]	DL Permibus (0Cell by default)
pbsz-id	INT [0->2]	PBSZ ID. (segment number by default)
stc	ENUM	STC Type values are: none stc-2
matrix-indicator	ENUM	Matrix Indicator (relevant only when using STC) values are: matrix-a matrix-b

Call

Figure 5-13: addDLZone command screen

You can define multiple zones.

Specify the stc and the matrix-indicator and click on the Call button. This creates a zone and automatically assigns the next available number in after-zone-id (the first zone carries the number 0). If you need to define more zones, repeat this step.

2. You need to specify the resources to be allocated to MIMO mode (to a zone). In the private tab, select the dmsbSetZoneProperties command.

Parameter	Value	Description
zone-id	* INT [0->7]	the DL zone id
min-slot	* INT [0->100]	minimal number of slot for the zone
max-slot	* INT [0->100]	maximal number of slot for the zone

Submit

Figure 5-14: addDLZone command screen

In zone-id enter the sequence number of the zone to which you want to allocate resources for MIMO mode.

In min-slot and max-slot fields specify the minimum and maximum number of slots to allocate to MIMO. Entering 100 means that your system will work in MIMO mode only.

3. In the ss tab select setSsPhyDl and set the relevant parameters for transmissions on the downlink.

5.3 Configuring the ASN Gateway

The ASN gateway is the point of access of the base station to the wide area network. Traffic to and from the base station passes through the ASN gateway.

The ASN gateway also mediates between the base station and the authentication server. It passes registration requests to the authentication server and returns results to the base station.

This section explains how to configure the ASN gateway.

1. Under the tools tab select setIPAddr and make sure that the data IP address and the physical IP address of the ASN gateway are in the same subnet.
2. Select SetOperationMode.

Field	Type	Value
OperationMode	ENUM	standalone
AsnIpAddress	STRING	Enter Ip Address
AuthenticationEnable	ENUM	NULL Authentication / RRM2 Authentication

Figure 5-15: SetOperationMode command screen

In OperationMode enter 1 (ASN gateway).

In AsnIpAddress enter the virtual template (IP address) of the ASN gateway (currently 192.168.103.1).

In AutthenticationEnable specify whether you want the ASN gateway to pass requests to the authentication server.

3. After clicking the Call button, the base station resets itself. Make sure that the reset procedure has succeeded and that the base station is in working order (the base station resets itself also after changing the mode from ASN gateway to Standalone).
4. Use the ShowOperationMode command to display the operation details of the ASN gateway.



Figure 5-16: ShowOperationMode command screen

5.4 Monitoring

1. Check if any CPE is up by choosing "showSs" in the "SS" tab.
2. Leaving all the fields blank will show a list of associated SS
3. Choose a specific CPE by writing its MAC address and the value "1" in the "verbose" field.
4. The CPE DL and UL RF parameters can be seen in "showSsPhyStatUI", and "showSsPhyStatDI", in the SS menu.
5. Define the specific CPE ID or MAC address in the relevant field.
6. The status of the service flows can be monitored in the "showSF" menu.
7. Leaving the fields blank will show a list of SFs. It is possible to choose a specific SF by choosing its sfid or bcid, and the value "1" in the "verbose" field.

6

Management

6.1 General

The WiN7000 cBST can be monitored and controlled with a standalone PC or through a management system (WiNMS) using the backhaul interface. The monitoring and control capabilities are similar in both cases but the interface may be different. This chapter describes the monitoring and control capabilities.

The local PC can connect to the internal web server using HTTP.

The management of the WiN7000 cBST device uses SNMP. The WiN7000 cBST has a standard MIB II and propriety MIB.

There are no local displays on the BS. All the indications will have to be monitored via the management system (WiNMS).

6.2 SW Download/Upgrade

The software can be loaded into the WiN7000 cBST using one of the following methods:

- Using a local PC (connected to the nearby switch) that has an FTP server running on it;
- Through remote SNMP (over the backhaul interface), using the WiNMS.

The WiN7000 cBST supports a complete rollback option to be used in case the upgrade fails.

1. In the HostIpAddress field, enter the FTP server IP address.
2. In the FileDirectory field, enter the directory in which the new SW files are located.
This directory should contain a <filename>.pkg file.
3. In the PackageFileName field, enter in the file name of the .pkg file.
4. Enter in the username and password of the FTP server in the appropriate fields.
5. Click the "call" button.
6. Wait for the upgrade process to complete.

6.3 Web-Based Management

The monitored and controlled parameters are available through a web interface.

Please refer to the Equipment Configuration and Monitoring chapter for a description of the basic configuration and monitoring screens.

For details see cBST WEB Manager chapter.

6.4 SNMP Management

Two MIBs are available in the WiN7000 cBST:

- The standard MIB II (RFC 1213)
- The private MIB

Table 6-1 describes the cBST Managed Parameters

Table 6-1: BS Parameters

Parameter	Description	MIB Type	Remarks
Location site + Contact details		MIB II	
Cell ID		Private	
Data Interface Status	Activity (Connected/Disconnected), Speed (10/100/1000), Duplex (Full/Half), IP Address,	MIB II	
Temperature	temperature inside the cBST case	Private	
Software Version	all Modules software's versions	Private	
Uptime	on time from power up	Private	
Number of registered CPEs		Private	
CPE MAC Addresses		Private	
CPE Type	Fix CPE ODU, PC Card, Self installed	Private	
Radio Status	Transmit: On/Off Frequency: configured radio frequency Configured BW/FFT Transmit power	Private	
TX Counter	Number of transmit packets	Private	
RX Counter	Number of receive packets	Private	

7

cBST WEB Manager

12. Click the Submit button.

7.4 Commands by Functional Area

This section presents the commands classified by functional areas. Each area corresponds to a tab in cBST WEB Manager.

7.4.1 Security

createStaticSa	Creates a static Security Association.
deleteStaticSa	Deletes a static Security Association.
resetSsAuth	Resets authorization for an MS, PKM V1 only.
showPkm	Displays PKM settings.
showPkmCs	Displays PKM settings related to crypto suites.
showSa	Displays security association.
showSsAuth	Displays MS authorization.

7.4.2 Logs

addLogFilter	Adds an MS to a log filter.
showLog	Displays the logging state for the specified module.
removeLogFilter	Removes an MS from a log filter.
setLogFilter	Enables or disables the filter log.
clearLogFilter	Clears all MS from a log filter.
showLogFilter	Displays MS in a log filter.

7.4.3 Misc

phyPing	Pings an MS.
showMacAddress	Displays the Station MAC address.
showVersion	Displays the system version.

7.4.4 UnicastServiceFlow

changeSf	Changes a service flow in the local service flow database.
createSf	Creates a service flow.
deleteSf	Deletes a service flow.
setSfEnable	Enables or disables a service flow in the local service flow database.
showSf	Displays information about a given service flow.

7.4.5 SS

createProvSf	Adds an MS to a provisioned service flow.
deleteProvSf	Deletes all provisioned service flows for an MS.
deregisterSs	De-registers an MS.
resetSs	Resets an MS.
setSsPhyDI	Configures MS downlink parameters.
setSsPhyUI	Sets MS uplink physical parameters.
showCaps	Displays global capabilities.
showProvSf	Displays the provisioned Service Flows.
showSs	Displays MS information.
showSsCaps	Displays the negotiated capabilities of an MS.

7.4.6 Statistics

resetPacketFlow	Resets the counters holding the statistical data shown by showPacketFlow.
showPacketFlow	Displays the quantity of packets flowing on the downlink and the uplink, as well as the packet flow rate.
showSsPhyStatsDI	Displays downlink MS physical statistics.
showSsPhyStatsUI	Displays uplink MS physical statistics.

7.4.7 MacFrame

addDIZone	Adds a downlink zone.
removeDIZone	Removes a downlink zone.
setMacDI	Changes the downlink channel descriptor configuration.
setMacFrame	Changes the frame channel descriptor configuration.
setMacUI	Changes the uplink channel descriptor configuration.
setSchedulerTdd	Configures the TDD split.
showMacDI	Displays the current downlink channel descriptor configuration.
showMacFrame	Displays the frame channel descriptor content.
showMacUI	Displays the uplink channel descriptor configuration.
showSchedulerMac	Displays the MAC scheduler configuration.

7.4.8 FWD

resetFwdEntries	Removes the entries stored in the Forwarding Table.
-----------------	---

7.4.9 Config

setTimeSync	Timeout for synchronization attempt.
showTimeSyncLockStatus	Indicates whether the base station is synchronized.
showTimeSyncParams	Shows the configured values of setTimeSync .

7.4.10 Private

cmdHelp	Displays all the commands and their description.
sniffShowState	Shows the current parameters controlling the packet sniffer.
pkmbShowPkm	Shows the current configuration controlling PKM.

7.4.11 Other

addAuthorizedManager	Adds a user authorized to access the cBST Web Manager and issue commands at administrator level.
AddIpAddress	Assigns an IP address to one of the system's network interface cards.
addSsToMcastSf	Adds an MS to a multicast service flow.
AddUser	Adds a user authorized to access the cBST Web Manager and issue commands at user level.
changeFwdFilter	Changes a filter in the forwarding database.
changeNeighborBs	Changes a Neighbor BS in the database.
createFwdArEntry	Creates an entry in the Address Resolution table.
createFwdEntry	Adds a static entry in the forwarding database.
createFwdFilter	Adds a new filter in the forwarding database.
createNeighborBs	Creates a neighbor BS.
createSc	Creates a service class.
DeleteAllSnmpAccess	Removes all SNMP access permissions.
deleteAuthorizedManager	Deletes an authorized administrator that has been added using the addAuthorizedManager command.
DeleteChangesFile	Deletes the changes file. See UpdateChangesFile. You may want to delete it so that at the next reset the base station reads only the configuration file.
deleteFwdArEntry	Removes an Address Resolution entry.
deleteFwdEntry	Removes a forwarding entry.
deleteFwdFilter	Removes a forwarding filter.
DeleteIpAddress	Deletes an IP address assigned using the addIpAddress command.
deleteNeighborBs	Deletes a neighbor BS from the database.
deleteSc	Deletes a service class.
enableFwdFilters	Enables or disables the filtering functionality.
FileDownload	Copies a file from the network to the base station's Flash memory.
FileList	Displays the files currently stored in the base station's Flash memory.

FileUpload	Copies a file from the base station's Flash memory to the network.
removeSsFromMcastSf	Removes an MS from a multicast service flow.
resetFwdStats	Resets the forwarding statistics.
Restart	Restart the base station.
RunMainPkgFile	Software upgrades are supplied in packages containing the upgrade files and installed on the base station's flash memory. This command runs the package defined as primary package.
RunSecondaryPkgFile	Same as RunMainPkgFile but runs the package defined as secondary.
setFwdPort	Configures the setting of the port.
setIpAddr	Modifies an IP address assigned with addIpAddress.
setLinkAdaptationDI	Configures DL link adaptation.
setMcastPhyDI	Sets multicast service flow PHY parameters.
setQosDI	Configures downlink QoS.
setQosHRateDI	Configures a DL HQoS parameter set.
setQosHrateSsDI	Associates an MS to a DL HQoS parameters set.
setQosHrateSsUI	Associates an MS to a UL HQoS parameters set.
setQosHRateUI	Configures a UL HQoS parameter set.
setQosRedDI	Enables and disables the downlink RED and sets the maximum RED latency.
setQosRedDIProfile	Configures the downlink RED drop profile.
setQosShapingDI	Enables and disable DL shaping.
SetSecondaryAsMain	Switches the definition of the main and secondary base station software packages. The secondary becomes main and the main becomes secondary.
showFwdAgeingTimeout	Displays entry timeout.
showFwdArEntry	Displays the address resolution forwarding entry.
showFwdEntries	Displays forwarding entries.
showFwdFilter	Displays forwarding filters.
showFwdInterface	Displays forwarding interface configuration.
showFwdPort	Displays port configuration.

showFwdStats	Displays forwarding statistics.
showIpAddr	Displays an IP address assigned with addIpAddress.
showLinkAdaptationDI	Displays DL link adaptation parameters.
showMcastPhyDI	Displays multicast service flow physical parameters.
showMcastSfList	Displays the list of multicast service flows.
showMcastSsList	Displays the list of MS registered to a multicast service flow.
showMii	Displays the MII configuration.
showNeighborAdvertisement	Displays neighbor advertisement parameters.
showNeighborBs	Displays a neighbor BS descriptor from the handover database.
ShowPkgFiles	Lists the files contained in the main and secondary packages.
showQoSDI	Displays the downlink QoS parameters.
showQoSRateDI	Displays a downlink hierarchical QoS parameter set.
showQoSRateUI	Displays an uplink hierarchical QoS parameter set.
showRfRx	Displays the RF frequency in Rx.
showRfTx	Displays the RF frequency in Tx.
ShowTrap	Lists the SNMP traps currently defined.
SoftwareUpgrade	Copies the upgrade package from the network to the flash memory of the base station.
SoftwareUpgradeStatus	Shows the current status of the upgrade performed via the SoftwareUpgrade command.
SysUptime	Shows the time that elapsed since the last time the base station has been reset.
TrapConfig	Allows you to define SNMP traps.
TrapEnable	Enables traps defined via the TrapConfig command.
TrapGetActive	Sends from the base station all active traps.
TrapIpAddress	Specifies the IP address to which traps are sent.
UpdateChangesFile	When you modify the base station configuration, the changes are written to a separate changes file. The next time the base station resets, it also reads the changes file. This command allows you to apply the changes made after the last reset (instead of resetting the station).

UpdateSnmpAccess	Updates the SNMP user authorizations with the details of the newly added users.
UserLogIn	Logs the user in to the base station.
UserLogOut	Logs the user out of the base station.

7.5 Command Reference

The following is an alphabetic reference to all cBST WEB Manager commands.

activatePsc

Other tab.

Activates a Power Saving Class.

Parameters

pscId

Power saving class identifier.

Integer in the range [0..255].

Required parameter.

ssId

MS identifier.

Integer in the range [0..65535].

startFrameDelay

Start frame delay in frame quantity.

Integer in the range [0..255].

Required parameter.

addAuthorizedManager

Other tab.

Adds a user authorized to access the cBST Web Manager and issue commands at administrator level.

Parameters

IpAddress

Manager IP address.

addChannelToScanner

Other tab.

Adds a new channel to the scanning list.

Parameters

bandwidth

Radio channel bandwidth.

Possible values: [3.5MHz | 5MHz | 7MHz | 8.75MHz].

frequency

A valid RF frequency.

Integer, expressed in kHz.

Required parameter.

Example for 2.5 GHz: frequency=2500000

duration

Frame duration.

Possible value: [5ms]

id

Channel ID.

Integer in the range [0..128].

addDcdTrigger

Other tab.

Adds a DCD trigger.

Parameters

metric

Metric used for trigger. Enum in [CINR | RSSI | RTD].

This is a required parameter.

duration

Averaging duration in frames number. Integer in [1..255].

This is a required parameter.

value

Value used for trigger. This parameter is metric-dependant. Refer to

IEEE802.16e section for encoding description.

This is a required parameter.

function

Function used for trigger.

Enum in [NBS_GREATER_ABS_VALUE | NBS_LESS_ABS_VALUE | NBS_GREATER_REL_VALUE | NBS_LESS_REL_VALUE | SBS_GREATER_ABS_VALUE | SBS_LESS_ABS_VALUE].

This is a required parameter.

action

Action to be performed. Enum in [REPORT | HANDOVER | SCANNING].

This is a required parameter.

addDlZone

Other tab.

Adds a downlink zone.

Parameters

after-zone-id

Insert the new zone after this one.

Integer.

use-all-subchannels

Use all the subchannels.

Integer with the following values:

The default status is disabled.

dl-permbase

Downlink permbase.

Integer in range [0..31].

By default, the value of this parameter is the IdCell number.

prbs-id

PRBS identifier.

Integer in range [0..2]

By default, the value of this parameter is the segment number.

stc

STC Type.

Possible values: [none | stc-2].

matrix-indicator

Matrix indicator. This parameter is only relevant when using STC.

Possible values: [matrix-a | matrix-b].

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

[0] Disabled.

[1] Enabled.

AddIpAddress

Other tab.

Assigns an IP address to one of the system's network interface cards.

Parameters

Specify the IP address, the network mask and the default gateway.

addLogFilter

Logs tab.

Adds an MS to a log filter.

Parameters

mac

Selects a mobile station with the given MAC address.

cid

Selects a mobile station with the given CID.

Integer in the range [1..65535].

addPagingGroup

Other tab.

Adds a paging group.

Parameters

id

Paging group ID.

Integer in the range [0..65535].

Required parameter.

cycle

Paging group cycle.

Integer in the range [0..65535].

Required parameter.

offset

Paging group cycle.

Integer in the range [0..65535].

Required parameter.

interval

Paging group interval.

Integer in the range [2..5].

Required parameter.

addSsToMcastSf

Other tab.

Adds an MS to a multicast service flow.

Parameters

macSs

MAC address of the selected mobile station.

String.

Exclusive required parameter.

cidSs

Basic CID of the selected, already registered, mobile station.

Integer in the range [1..65535].

Exclusive required parameter.

sfidMcast

SFID of the selected service flow.

Integer.

Exclusive required parameter.

cidMcast

CID of the selected service flow.

Integer in the range [1..65535].

Exclusive required parameter.

addSsToStaticSa

Other tab.

Adds an MS to a static Security Association.

Parameters

cidSs

Selects the mobile station with this CID. Integer in range [1..65535].

Required parameter.

said

SAID of the static SA. Integer.

Required parameter.

addUlZone

Other tab.

Adds an uplink zone.

Parameters

after-zone-id

Inserts the new zone after the one with the zoneId specified.

Integer in the range [0..6].

use-all-subchannels

Enables the use of all subchannels, concerns PUSC only.

Integer with the following values:

ul-permbase

Uplink permbase.

Integer in the range [0..127].

The default value of this parameter is the uplink permbase in the UCD.

subchannel-rotation

Enable subchannel rotation.

Integer in range [0..1]. Default value is 1 (true).

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

AddUser

Other tab.

Adds a user authorized to access the cBST Web Manager and issue commands at user level.

Parameters

User Name

Enter the new user's username.

Password

Enter the new user's password.

Verify Password

Enter the password again.

User Level

Select the user's authorization level.

changeFwdFilter

Other tab.

Changes a filter in the forwarding database.

Parameters

name

Name of the filter, previously used for createFwdFilter.

String.

Required parameter.

enable

Status of the filter.

Possible values: [disable, enable].

action

Action.

Possible values: [filter, forward].

priority

Priority.

Integer in the range [0..255].

Filter priority: filters with higher numerical value priorities are evaluated before those with lower numerical values.

port

Port name.

Possible values:

direction

Direction of the filter.

Possible values:

LOCAL Local control/management plane.

RFI Radio Frequency Interface

NSI Network-Side Interface; the MII or the local host interface.

PFGA Packet Flow Generator and Analyzer software module.

[tx] Transmitting to the WiMAX interface (egress).

ethsa

Source MAC address.

ethda

Destination MAC address.

dscprm

Type of Service/Differentiated Services Code Point field range mask.

etherType

Protocol encapsulated in the Ethernet frames.

proto

Protocol encapsulated in the IP diagrams.

ipsrc

Source IP address.

String.

ipdst

Destination IP address.

String.

spr

Source TCP/UDP port range.

Example: 31233 - 31234.

dpr

Destination TCP/UDP port range.

Example: 31233 - 31234.

changeNeighborBs

Other tab.

Changes a Neighbor BS in the database.

Parameters

handle

Handle of the BS in the database.

Integer. This is a required parameter.

mac

Neighbor BS MAC address.

String.

fa-index

Neighbor BS Frequency Assignment index.

Integer in [0..255]

preamble-index

Neighbor BS Preamble index.

Integer in [0..113]

changeSf

Other tab.

UnicastServiceFlow tab.

Changes a service flow in the local service flow database.

Parameters

sfid

SFID of the service flow to change in the database.

Integer.

Exclusive required parameter.

cid

Connection identifier of the service flow to change in the database.

Integer in the range [0..65535].

Exclusive required parameter.

state

State of the service flow.

Possible values [provisioned | admitted | active]

maxrate

Maximum rate of the service flow in bits per second.

Integer.

minrate

Minimum rate of the service flow in bits per second.

Integer.

maxlatency

Maximum latency of the service flow in milliseconds.

Integer.

priority

Traffic priority of the service flow.

Integer in the range [0..7].

grant-interval

Grant period for UGS/eRTPS, in ms.

Integer.

polling-interval

Polling period for rtPS and nrtPS, in ms.

Integer.

delete-all-classifier

Deletes all classifiers of the service flow.

Integer with the following values:.

classifier1

First classifier.

classifier2

Second classifier.

classifier3

Third classifier.

classifier4

Fourth classifier.

clearLogFilter

Logs tab.

Clears all MS from a log filter.

Parameters

None.

clearScannerChannels

Other tab.

Resets all scanner channels.

Parameters

None.

clearSnifferFilters

Other tab.

Clears all sniffer filters.

Parameters

None.

cmdHelp

Private tab.

Displays all the commands and their description.

Parameters

commandName

'Module::command' name to display the usage

createFwdArEntry

Other tab.

Creates an entry in the Address Resolution table.

Parameters

mac

String. Ethernet MAC address.

This is a required parameter.

ip

String. IP Address

This is a required parameter.

createFwdEntry

Other tab.

Adds a static entry in the forwarding database.

Parameters

mac

MAC address.

Required parameter.

port

Port that you use to access the above MAC address.

Required parameter.

Possible values:

If the MAC address is a multicast or broadcast address, you can use a comma-separated list of ports. Do not use the space character in the list.

cid

CID of the MS, in case of RFI interface.

Integer in the range [0..65535].

createFwdFilter

Other tab.

Adds a new filter in the forwarding database.

Parameters

name

Name of the filter.

String.

Required parameter.

enable

State of the filter.

Possible values: [disable | enable].

action

Action.

Possible values: [filter | forward].

priority

Priority.

Integer in the range [0..255].

Filter priority: filters with higher numerical values are evaluated before those with lower numerical values.

port

Port name.

Required parameter.

Possible values:

direction

Direction of the filter.

LOCAL Local control/management plane.

RFI Radio Interface

NSI Network-Side Interface; the MII or the local host interface.

NSI is replaced with MII in host mode over MII.

SDIO interface might exist in host mode over SDIO.

PFGA Packet Flow Generator and Analyzer software module.

Required parameter.

Possible values:

ethsa

Source MAC address.

ethda

Destination MAC address.

dscprm

Type of Service/Differentiated Services Code Point field range mask.

etherType

Protocol encapsulated in the Ethernet frames.

proto

Protocol encapsulated in the IP diagrams.

ipsrc

Source IP address.

String.

ipdst

Destination IP address.

String.

spr

Source TCP/UDP port range.

Example: 31233 - 31234.

dpr

Destination TCP/UDP port range.

Example: 31233 - 31234.

createHandoverMs

Other tab.

Provisions an MS for handover.

Parameters

mac

MAC address of the MS.

String.

Required parameter.

createMcastSf

Other tab.

Creates a multicast service flow.

Parameters

sfid

SFID of the service flow.

Unique ID.

Integer.

Exclusive required parameter.

mac

Associates the created SF with the specified MAC address.

String.

Exclusive required parameter.

maxrate

Maximum rate of the service flow in bits per second.

Integer.

minrate

Minimum rate of the service flow in bits per second.

Integer.

priority

Traffic priority of the service flow.

Integer in the range [0..7].

longFsn

Specifies whether to enable the long 11-bit FSN subheader.

Integer with the following values:.

The default status is enabled.

fragmentation

Specifies whether fragmentation is enabled on the connection.

[0] Disabled.

[1] Enabled.

Integer with the following values:

The default status is enabled.

phs

Specifies whether PHS is enabled on the connection.

Integer with the following values:.

packing

Specifies whether packing is enabled on the connection.

Integer with the following values:.

crc

Specifies whether IEEE 802.16 CRC is enabled on the connection.

Integer with the following values:.

said

Security Association ID of the service flow.

Integer.

encryption

Encryption type.

Enumeration, possible values: [des, aes]. Default value is aes.

createNeighborBs

Other tab.

Creates a neighbor BS.

Parameters

mac

Neighbor BS's MAC address.

frequency

Neighbor BS's frequency in MHz.

preamble-index

Neighbor BS's preamble index

subchannel-bitmap

Uplink subchannels bitmap (hex). Enter 0 to activate all subchannels.

dcdCount

Neighbor BS's DCD count.

ucdCount

Neighbor BS's UCD count.

ip

Neighbor BS's IP address.

createProvSf

SS tab.

Adds an MS to a provisioned service flow.

Parameters

mac

MAC address.

String.

Required parameter.

sfid

SFID of the provisioned service flow.

Unique integer.

Required parameter.

direction

Direction of the provisioned service flow.

Enumeration, possible values: [uplink | downlink].

Required parameter.

maxrate

Maximum rate of the provisioned service flow.

Integer in bits per second.

minrate

Minimum rate of the provisioned service flow.

Integer in bits per second.

maxlatency

Maximum latency of the service flow.

Integer in milliseconds.

priority

Traffic priority of the provisioned service flow.

Integer in the range [0..7].

scheduling

Type of scheduling.

Possible values: [besteffort | nrtps | rtps | ugs].

grant-interval

Grant period for UGS.

Integer in milliseconds.

polling

Polling period for RTPS and nRTPS.

Integer in milliseconds.

longFsn

Enables the long FSN subheader (11 bits).

Integer with the following values:

The default status is enabled.

broadcast-bwr

Enables the broadcast bandwidth requests on the connection.

Integer with the following values:

The default status is enabled.

multicast-bwr

Enables the multicast bandwidth requests on the connection.

Integer with the following values:

The default status is enabled.

piggyback-bwr

Enables the piggyback bandwidth requests on the connection.

Integer with the following values:

[0] Disabled.

[1] Enabled.

The default status is enabled.

fragmentation

Enables the fragmentation on the connection.

Integer with the following values:

The default status is enabled.

phs

Enables the PHS on the connection.

Integer with the following values:

The default status is disabled.

packing

Enables the packing on the connection.

Integer with the following values:

The default status is enabled.

crc

Enables the 802.16 CRC on the connection.

Integer with the following values:

The default status is enabled.

arq

Enables the ARQ feature.

Integer with the following values:

[0] Disabled.

[1] Enabled.

The default status is disabled.

arq-window-size

ARQ window size in block quantity.

Integer in the range [1..1024]. Default value is 512.

arq-block-size

ARQ block size in number of bytes.

Integer in the range [4..10], must be a power of 2. Default value is 256.

arq-transmitter-delay

ARQ transmitter delay in ms.

Integer in the range [1..655]. Default value is 35 ms.

arq-receiver-delay

ARQ receiver delay in ms.

Integer in the range [1..655]. Default value is 35 ms.

arq-block-lifetime

ARQ block lifetime in ms.

Integer in the range [0..655]. Default value is 250 ms.

arq-sync-loss-timeout

ARQ Sync Loss Timeout in ms.

Integer in the range [0..655]. Default value is 300 ms.

arq-rx-purge-timeout

ARQ Rx purge timeout in ms.

Integer in the range [0..655]. Default value is 150 ms.

harq

Enables the Hybrid ARQ feature.

Integer with the following values:

The default status is disabled.

harq-acids

Bitmap of Hybrid ARQ ACIDs to use

Integer in the range [0..65535]. Default value is 0xFFFF.

harq-latency

Maximum latency for Hybrid ARQ retransmissions in ms.

Integer in the range [0..1000]. Default value is 0 ms.

harq-pdu-sn

H-ARQ PDU SN type to use.

Possible values are [none | short | long]

[0] Disabled.

[1] Enabled.

classifier1

First classifier.

Required parameter.

classifier2

Second classifier.

classifier3

Third classifier.

classifier4

Fourth classifier.

createPsc

Other tab.

Creates a Power Saving Class.

Parameters

pscId

Identifier of the Power Service Class.

Integer in range [0..63].

ssId

MS identifier.

Integer in range [0..65535].

direction

Direction of the associated service flow.

Possible values: [undefined, downlink, uplink]. Default value is undefined.

tir

Traffic Indication required flag.

Possible values: [0..1]. Default value is 1 (true).

ttwf

Traffic triggered waking flag.

Possible values: [0..1]. Default value is 0 (false).

initSleepWindow

Initial Sleep window, in frame quantity.

Integer in range [0..255].

Required parameter.

listenWindow

Listening window, in frame quantity.

Integer in range [0..255].

Required parameter.

finalSleepWindowBase

Final Sleep window base, in frame quantity.

Integer in range [0..1023].

Required parameter.

finalSleepWindowExp

Final Sleep window exponent.

Integer in range [0..7].

Required parameter.

cidQty

CID quantity.

Integer in range [0..7].

Required parameter.

cidList

CID list.

String.

startFrameDelay

Start frame delay (in number of frames).

Integer in range [0..255].

Required parameter.

createSc

Other tab.

Creates a service class.

Parameters

scid

Unique ID of the service class.

Maximum 32-bit integer defined by the user, must be unique.

Required parameter.

name

Unique name of the service class.

String defined by the user, must be unique.

Required parameter.

scheduling

Type of scheduling (uplink only): [besteffort | nrtps | rtps | ugs]

priority

Traffic priority of the service class.

Integer, default value is 0.

max-sustained-rate

Maximum sustained rate of the service class, in bit/s.

Integer, default value is 0.

max-traffic-burst

Maximum traffic burst of the service class.

Integer, default value is 0.

min-reserved-rate

Minimum reserved rate of the service class.

Integer in bits per second.

tolerated-jitter

Minimum rate of the service flow.

Integer in bits per second.

max-latency

Maximum latency of the service class, in bit/s.

Integer in bits per second.

grant-interval

Grant period for UGS in ms. (not available in the current release of S-Cube)

Integer.

polling-interval

Polling period for RTPs and nRTPs in ms.

Integer.

createSf

UnicastServiceFlow tab.

Creates a service flow.

Parameters

sfid

Unique ID of the service flow.

Maximum 32-bit integer defined by the user, must be unique (within a given MS).

Required parameter.

bcid

Basic connection ID for this service flow.

Integer in the range [0..65535].

direction

Direction of the service flow.

Enumeration, possible values: [uplink | downlink].

Required parameter.

state

State of the service flow.

Possible values [provisioned | admitted | active]

maxrate

Maximum rate of the service flow.

Integer in bits per second.

minrate

Minimum rate of the service flow.

Integer in bits per second.

createSf S-Cube 4.4.0

maxlatency

Maximum latency of the service flow in milliseconds.

Integer.

priority

Traffic priority of the service flow.

Integer in the range [0..7].

serviceClass

Service Class Name.

String.

scheduling

Type of scheduling: [besteffort | nrtps | rtps | ugs]

grant-interval

Grant period for UGS/eRTPS in ms. (Not available in the current release of S-Cube).

Integer.

polling-interval

Polling period for RTPs and nRTPs in ms.

Integer.

broadcast-bwr

Enables broadcast BWR on the connection.

Integer with the following values:.

The default status is enabled.

multicast-bwr

Enables multicast BWR on the connection.

Integer with the following values:.

The default status is enabled.

piggyback-bwr

Enables piggyback BWR on the connection.

Integer with the following values:

[0] Disabled.

[1] Enabled.

The default status is enabled.

fragmentation

Enables fragmentation on the connection.

Integer with the following values:

The default status is enabled.

phs

Enables PHS is enabled on the connection.

Integer with the following values:

The default status is disabled.

packing

Enables packing on the connection.

Integer with the following values:

The default status is enabled.

crc

Enables IEEE 802.16 CRC on the connection.

Integer with the following values:

The default status is enabled.

arq

Enables the ARQ feature.

Integer with the following values:

[1] Enabled.

[0] Disabled.

The default status is disabled.

arq-window-size

ARQ window size in block quantity.

Integer in the range [0..1024]. The default value is 512.

arq-block-size

ARQ block size in byte quantity.

Power of two integer in the range [4..10]. The default value is 8.

arq-transmitter-delay

ARQ transmitter delay in ms.

Integer in the range [0..655]. The default value is 35.

arq-receiver-delay

ARQ receiver delay in ms.

Integer in the range [0..655]. The default value is 35.

arq-block-lifetime

ARQ block lifetime in ms.

Integer in the range [0..655]. The default value is 250.

arq-sync-loss-timeout

ARQ Sync Loss Timeout in ms.

Integer in the range [0..655]. The default value is 0.

arq-rx-purge-timeout

ARQ Rx purge timeout in ms.

Integer in the range [0..655]. The default value is 250.

harq

Enables the HARQ feature.

Integer with the following values:

harq-acids

Bitmap of HARQ ACIDs to use.

Integer in the range [1..65535].

Default value is 0xFFFF.

harq-latency

Maximum latency for HARQ retransmissions in milliseconds.

Integer in the range [0..1000].

[0] Disable.

[1] Enable. Default value.

Default value is 0.

harq-pdu-sn (enum: none, short, long): HARQ PDU SN type to use

classifier1

First classifier.

Required parameter.

classifier2

Second classifier.

classifier3

Third classifier.

classifier4

Fourth classifier.

createSnifferFilter

Other tab.

Adds a filter to the sniffer.

Parameters

cid

The CID of the actual connection on which you want to sniff packets. The CID can be any kind of CID, for example basic CID, primary CID, or data CID.

Integer in the range [0..65535]

error

Specifies whether to sniff only packets with errors.

Integer with the following values:

[0] Do not sniff only packets with errors.

[1] Sniff only packets with errors.

type

Specifies whether you want this filter to sniff data or MAC packets.

Enumeration, possible values: [data | mac]. Default value is mac.

mac-filter

Sniffs MAC management packets with the specified type.

Filter, syntax is as follows:

mac-filter=(**[+-]**NAME**[*]**)**+**

Name: MAC management names, To select from possible string values, perform the following steps:

1. In the directory /src/cbe, open the file cbeMisc.cc.
2. Search for the following line: Sniffer interface.
3. Select from the MAC filter values in the list.

Example: mac-filter=**+**DL_MAP-UL_MAP**+**DCD-UCD

See also IEEE 802.16e-2005, Table 14, for a list of MAC filter string values.

Note: Sequans uses only underscores [**_**] in MAC filter string values, whereas the IEEE standard uses underscores and hyphens [**-**].

Examples:

Sequans: UL_MAP, MOB_NBR_ADV

IEEE: UL-MAP, MOB_NBR-ADV

The default value is `-*`, in other words no sniffing.

direction

Specifies a transmission or reception filter.

Possible values:

The default value is `rx`.

createStaticSa

Security tab.

Creates a static Security Association.

Parameters

saId

Selects the SAID. Integer in range [0..65535].

Required parameter.

encryption

Encryption type.

Possible value: [aes-keywrap]. The default value is `aes-keywrap`.

deactivatePsc

Other tab.

Deactivates a Power Saving Class for an MS.

Parameters

pscId

Power Saving Class identifier.

Integer in range [0..255].

Required parameter.

ssId

MS identifier.

Integer in range [0..65535].

DeleteAllSnmpAccess

Other tab.

Removes all SNMP access permissions.

Parameters

deleteAuthorizedManager

Other tab.

Deletes an authorized administrator that has been added using the addAuthorizedManager command.

Parameters

IpAddress

Enter the manager's IP address.

DeleteChangesFile

Other tab.

Deletes the changes file. See UpdateChangesFile. You may want to delete it so that at the next reset the base station reads only the configuration file.

Parameters

None.

deleteFwdArEntry

Other tab.

Removes an Address Resolution entry.

Parameters

id

IP Address.

String. This is a required parameter.

deleteFwdEntry

Other tab.

Removes a forwarding entry.

Parameters

mac

MAC address to be deleted.

String.

Required parameter.

deleteFwdFilter

Other tab.

Removes a forwarding filter.

Parameters

name

The name of the filter that you want to remove.

String.

Required parameter.

deleteNeighborBs

Other tab.

Deletes a neighbor BS from the database.

Parameters

handle

Neighbor BS's handle in the database.

deletePagingGroup

Other tab.

Removes a paging group.

Parameters

id

Paging group ID.

Integer in the range [0..65535].

Required parameter.

offset

Paging group offset.

Integer in the range [0..65535].

Required parameter.

deleteProvSf

SS tab.

Deletes all provisioned service flows for an MS.

Parameters

mac

MAC address of the MS.

String.

Required parameter.

deletePsc

Other tab.

Deletes a Power Saving Class.

Parameters

pscId

Identifier of the PSC.

Integer in range [0..63].

Required parameter.

deleteSc

Other tab.

Deletes a service class.

Parameters

name

Name of the service class.

String.

Required parameter.

deleteSf

UnicastServiceFlow tab.

Deletes a service flow.

Parameters

sfid

ID of the service flow to be deleted.

Integer.

Required parameter.

cid

Connection identifier for this service flow.

Integer in the range [0..65535].

Required parameter.

deleteSnifferFilter

Other tab.

Deletes a sniffer filter.

Parameters

id

Identifier of the sniffer filter to delete.

Integer in the range [0..65535].

Required parameter. The ID of a filter is automatically attributed. You can find it by calling the showSniffer command.

deleteStaticSa

Security tab.

Deletes a static Security Association.

Parameters

said

Selects the SAID. Integer in range [0..65535].

Required parameter.

deregisterSs

SS tab.

De-registers an MS.

Parameters

mac

MAC address of the selected MS.

String.

Exclusive required parameter.

cid

CID of the selected MS.

Integer in range [0..65535].

Exclusive required parameter.

action

Selects the message action code.

Enumeration, possible values:

[leave | transmit | listen | return | terminate].

disableLog

Other tab.

Disables trace logging for a software module.

Parameters

name

Selects the software module for which you want to disable logging traces.

Refer to the list of software modules in the S-Cube Architecture Guide.

String.

Required parameter.

name has the following syntax:

module/submodule

where:

module

Selects the module for which you want to disable logging traces. You can set this parameter to *.

String.

submodule

Optional parameter reserved for Sequans internal use. This parameter selects the software submodule for which you want to disable logging software traces.

You can set this parameter to * to indicate all logs.

String.

disableSniffer

Other tab.

Disables packet sniffing.

Parameters

None.

enableFwdFilters

Other tab.

Enables or disables the filtering functionality.

Parameters

enable

State of the filtering feature.

Enumeration, possible values: [disable, enable].

Required parameter.

enableLog

Other tab.

Enables trace logging for a software module.

Parameters

name

Selects the software module for which you want to enable logging traces.

Refer to the list of software modules in the S-Cube Architecture Guide.

Required parameter.

String.

name has the following syntax:

module/submodule

where:

module

Selects the module for which you want to enable logging traces. You can set this parameter to *.

String.

submodule

Optional parameter reserved for Sequans internal use. This parameter selects the software submodule for which you want to enable logging software traces. You can set this parameter to *.

String.

enableSdc

Other tab.

Enables Switched Diversity Combining.

SQN1110 only.

Parameters

state

Requires state for SDC.

Enum in range [disable | enable].

Required parameter.

enableSniffer

Other tab.

Enables packet sniffing.

Parameters

qty

Quantity of packets to sniff.

Integer, default value infinite.

FileDownload

Other tab.

Copies a file from the network to the base station's Flash memory.

Parameters

HostIpAddress

Select the base station's IP address.

FileDirectory

Select the original location of the file.

FileName

Select the file.

UserName

Specify the username needed to perform the operation.

Password

Specify the password needed to perform the operation.

FileList

Other tab.

Displays the files currently stored in the base station's Flash memory.

Parameters

None.

FileUpload

Other tab.

Copies a file from the base station's Flash memory to the network.

Parameters

HostIpAddress

Select the base station's IP address.

FileDirectory

Select the destination directory.

FileName

Select the file.

UserName

Specify the username needed to perform the operation.

Password

Specify the password needed to perform the operation.

filterLog

Other tab.

Filters logging.

Parameters

+

Specifies that the specified module or set of modules should be logged

-

Specifies that the specified module or set of modules should not be logged

module

Selects the software module for which you want to start logging traces.

Refer to software modules list in document S-Cube User Guide.

String.

Required parameter.

submodule

Optional parameter reserved for Sequans internal use. This parameter selects the software submodule that starts logging its software traces.

String.

Wildcard character.

modifyProvisionedPsc

Other tab.

Update parameter of a Power Saving Class.

Parameters

direction

Direction of the associated service flow.

Possible values: [undefined, downlink, uplink]. Default value is undefined.

tir

Traffic Indication required flag.

Possible values: [0..1]. Default value is 1 (true).

ttwf

Traffic triggered waking flag.

Possible values: [0..1]. Default value is 0 (false).

initSleepWindow

Initial Sleep window, in frame quantity.

Integer in range [0..255].

listenWindow

Listening window, in frame quantity.

Integer in range [0..255].

finalSleepWindowBase

Final Sleep window base, in frame quantity.

Integer in range [0..1023].

finalSleepWindowExp

Final Sleep window exponent.

Integer in range [0..7].

cidQty

CID quantity.

Integer in range [0..7].

Required parameter.

cidList

CID list.

String.

modifyPsc

Other tab.

Modifies the parameters of a Power Saving Class.

Parameters

pscId

PSC identifier.

Integer in range [0..255]. Required parameter.

direction

Direction of the associated service flow.

Possible values: [undefined, downlink, uplink].

initSleepWindow

Initial Sleep window, in frame quantity.

Integer in range [0..255].

listenWindow

Listening window, in frame quantity.

Integer in range [0..255].

finalSleepWindowBase

Final Sleep window base, in frame quantity.

Integer in range [0..1023].

finalSleepWindowExp

Final Sleep window exponent.

Integer in range [0..7].

cidQty

CID quantity.

Integer in range [0..7].

cidList

CID list.

String.

performHandover

Other tab.

Performs a small cell jump to a neighbor BS.

Parameters

bs-index

BS index in neighbor database.

Integer in the range [0..268435455].

Required parameter.

phyPing

Misc tab.

Pings an MS.

Parameters

grant-length

Minimal length of the grant, in number of slots.

Integer in the range [1..40]. Default value is 10.

cid

Selects a mobile station with the given CID.

Integer in the range [1..65535].

Required parameter.

pkmbShowPkm

Private tab.

Shows the current configuration controlling PKM.

Parameters

None.

removeChannelFromScanner

Other tab.

Removes a channel from the scanning list.

Parameters

id

Channel ID, representing the index of the channel to remove from the scanning list.

Integer in the range [0..128].

Required parameter.

removeDcdTrigger

Other tab.

Removes a DCD trigger.

Parameters

metric

Index of the trigger to remove. Integer in [0..15].

Required parameter.

removeDlZone

Other tab.

Removes a downlink zone.

Parameters

zone-id

The identifier of the zone to remove.

Integer in the range [1..7].

Required parameter.

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

removeLogFilter

Logs tab.

Removes an MS from a log filter.

Parameters

mac

Selects a mobile station with the given MAC address.

Required parameter.

cid

Selects a mobile station with the given CID.

Integer in the range [1..65535].

Required parameter.

removeSsFromMcastSf

Other tab.

Removes an MS from a multicast service flow.

Parameters

macSs

MAC address of the selected mobile station.

String.

Required parameter.

cidSs

CID of the selected mobile station.

Integer in the range [1..65535].

Required parameter.

sfidMcast

SFID of the selected multicast service flow.

Integer.

Required parameter.

cidMcast

CID of the selected multicast service flow.

Integer in the range [1..65535].

Required parameter.

removeSsFromStaticSa

Other tab.

Removes an MS from a static Security Association.

Parameters

cidSs

Selects the MS with the given connection ID.

Integer in the range [1..65535].

Required parameter.

saId

SAID of the static SA.

Integer.

Required parameter.

removeUplinkZone

Other tab.

Removes an uplink zone.

Parameters

zone-id

The zone ID of the zone to remove.

Integer in the range [1..7].

Required parameter.

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

requestPowerModeChange

Other tab.

Request a power control mode change.

Parameters

cid

CID of the selected mobile station.

Integer in the range [1..65535].

Required parameter on the BS.

mode

New power control mode.

Possible values: [closed-loop | open-loop].

resetFwdEntries

FWD tab.

Removes the entries stored in the Forwarding Table.

Parameters

None.

resetFwdStats

Other tab.

Resets the forwarding statistics.

Parameters

None.

resetPacketFlow

Statistics tab.

Resets the counters holding the statistical data shown by showPacketFlow.

resetSa

Other tab.

Resets a Security Association.

Parameters

said

Selects the security association ID.

Integer range [0..65535].

Required parameter.

bcid

Specifies the MS by its base connection ID.

Integer in the range [0..65535].

send-tek-invalid

Specifies the action when resetting. The action is sent with the message parameter.

Integer with the following values:.

message

Specifies the message to send with a TEK invalid.

String. This parameter does not support spaces.

resetSs

SS tab.

Resets an MS.

Parameters

No parameters for the MS.

For the BS:

mac

Selects a mobile station by its MAC address.

String.

Required parameter.

cid

Selects a mobile station by its base connection ID.

Integer in the range [0..65535].

Required parameter.

action

Selects the message type.

Possible values:

[local | send-reset-command | send-ranging-abort]

resetSsAuth

Security tab.

Resets authorization for an MS, PKM V1 only.

Parameters

mac

MAC address of the MS for which you want to reset the authorization.

String.

Required parameter.

cid

Base connection ID of the MS for which you want to reset the authorization.

Integer in the range [0..65535].

Required parameter.

action

BS specific.

Specifies the action when resetting the MS authorization.

Possible values:

[none | invalidate-auth | send-auth-invalid | auth-invalidate-teks]

message

BS specific.

Message to send with send-auth-invalid action.

Restart

Other tab.

Restart the base station.

Parameters

None.

RunMainPkgFile

Other tab.

Software upgrades are supplied in packages containing the upgrade files and installed on the base station's flash memory. This command runs the package defined as primary package.

Parameters

None.

RunSecondaryPkgFile

Other tab.

Same as RunMainPkgFile but runs the package defined as secondary.

Parameters

None.

setCaps

Other tab.

Sets the global capabilities.

Parameters

pkm-version

Sets the requested authorization policy.

Enumeration, possible values: [none | pkm-v1 | pkm-v2]

pkm-cmac-0

Enables the support of CMAC0.

Integer with the following values:

pkm-cmac

Enables the support of CMAC.

Integer with the following values:

arq

Sets ARQ support.

Enumeration, possible values: [disabled | enabled]

arq-supported-ack

Bitmap of supported ACK types.

Integer in the range [0..15].

rx-qam64

Sets Rx QAM64 support, MS only.

Enumeration, possible values: [disabled | enabled]

tx-qam64

Sets Tx QAM64 support, BS only.

[0] Disabled.

[1] Enabled.

[0] Disabled.

[1] Enabled.

Enumeration, possible values: [disabled | enabled]

rx-stc

Sets Rx STC support.

Enumeration, possible values: [disabled | enabled]

phs

Sets PHS support.

Enumeration, possible values: [disabled | enabled]

ertps

Sets eRTPS support. Enum in [disabled | enabled]

rx-ctc

Sets Rx CTC support.

Enumeration, possible values: [disabled | enabled]

tx-ctc

Sets Tx CTC support.

Enumeration, possible values: [disabled | enabled]

rx-harq

Enables Rx chase combining Hybrid ARQ support.

Integer with the following values:

tx-harq

Enables Tx chase combining Hybrid ARQ support.

Integer with the following values:

rx-max-data-per-frame

Sets Rx maximum MAC level data per frame in bytes, floored to a 256

multiple. This parameter is for MS only.

Integer in the range: [0..16776960]. A value of 0 means infinite.

tx-max-data-per-frame

Sets Tx maximum MAC level data per frame in bytes, floored to a 256

multiple. This parameter is for MS only.

pcinr-preamble

Enables the support of PCINR measurement on preamble.

[0] Disabled.

[1] Enabled.

pcinr-pilot

Enables the support of PCINR measurement on pilot subchannel.

Integer with the following values:

[0] Disabled.

[1] Enabled.

ecinr-preamble

Enables the support of ECINR measurement on preamble.

Integer with the following values:

ecinr-pilot

Enables the support of ECINR measurement on pilot subchannel.

Integer with the following values:

concurrent-cqi

Enables the support of concurrent Channel Quality Indicator (CQI) report.

Integer with the following values:

collaborative-sm

Enables the support of collaborative spatial multiplexing.

Integer with the following values:

disabling-of-subc-rotation

Disables the support of subchannel rotation.

Integer with the following values:

[0] Suppression of subchannel rotation is supported.

[1] Suppression of subchannel rotation is not supported.

setDebugAsicOutput

Other tab.

Configures the ASIC debug output signals.

Parameters

output

Output signal identification.

Enumeration

Supported BS values: [none | rxFft | rxChannelEstimation | rxAdc | rxCic | txIfft | txDac].

Supported MS values: [none | rxFft | rxTimingSynchro | rxAdc | rxCic | txIfft | txDac].

Required parameter.

chanId

Channel Selection.

Integer with the following values: [0 | 1]

mac-domain

MAC domain. This parameter is for BS only.

Integer in range [0..2]. Default value is 0.

setDefaultMacDomain

Other tab.

Defines the default MAC domain.

Parameters

mac-domain

MAC domain.

Integer, use value 0.

setFwdAgeingTimeout

Other tab.

Sets the fwdtimeout entry.

Parameters

timeOut

Timeout in ms.

Integer in [900000..2147483647]

setFwdPort

Other tab.

Configures the setting of the port.

Parameters

port

Port name.

String.

Required parameter.

frame-type

Acceptable frame type.

Enumeration, possible values: [any, vlan].

pvid

Port VLAN ID.

Integer in the range [0..4095].

prio

VLAN priority. Integer in the range [0..7].

default-dest

Default destination. This value must be different from port.

String.

replyToArp

Reply to ARP requests.

Enumeration, possible values: [no, yes].

setHandover

Other tab.

Configures handover trigger.

Parameters

mode

Enables scanning and handover triggers.

Enumeration, possible values: [off|scan|scan-and-handover]

scan-threshold

Serving BS CINR threshold in dB to scan neighbor BS.

Float.

handover-threshold

Serving BS CINR threshold in dB to perform handover.

Float.

handover-hysteresis

CINR hysteresis margin in dB to perform handover.

Float.

setHarqCategory

Other tab.

Declares an HARQ category.

Parameters

dl-category

DL HARQ category to declare.

Integer in the range [1..4].

ul-category

UL HARQ category to declare.

Integer in the range [1..4].

setIdleMode

Other tab.

Starts idle mode.

Parameters

duration

Duration of idle mode in milliseconds.

Integer in the range [1000..1000000].

setIpAddr

Other tab.

Modifies an IP address assigned with addIpAddress.

Parameters

setLinkAdaptationDI

Other tab.

Configures DL link adaptation.

Parameters

mode

Mode of link adaptation.

Possible values: [manual | automatic]

protection

CINR protection against implementation CINR in dB.

Float.

hysteresis

CINR hysteresis when upgrading the FEC code, in dB.

Float.

report-period

This parameter only applies to the MS.

Period of downlink operation burst profile reporting, in ms.

Integer in range [20..30000].

report-enable

This parameter only applies to the MS.

Enables the periodic report.

Integer with the following values:

manual-mimo-mode

Manual selection of the MIMO mode.

[0] Disabled.

[1] Enabled.

Enum in [matrix-a-pusc-fusc | matrix-a-adjacent-subchannel |

matrix-b-pusc-fusc | matrix-b-adjacent-subchannel |

matrix-c-pusc-fusc | matrix-c-adjacent-subchannel |

antenna-option-0-a1 | antenna-option-1-a2 |

antenna-option-2-a3 | antenna-option-3-b1 |

antenna-option-4-b2 | antenna-option-5-b3 |

antenna-option-6-b4 | antenna-option-7-b5 | reserved-b6 |

closed-loop-1 | closed-loop-2 | closed-loop-3 |

closed-loop-4]

fec-code

This parameter only applies to the MS.

FEC of the operational downlink burst profile.

Possible values: [qpsk-cc-1/2 | qpsk-cc-3/4 | qam16-cc-1/2 |
qam16-cc-3/4 | qam64-cc-1/2 | qam64-cc-2/3 | qam64-cc-3/4 |
qpsk-ctc-1/2 | qpsk-ctc-3/4 | qam16-ctc-1/2 |
qam16-ctc-3/4 | qam64-ctc-1/2 | qam64-ctc-2/3 |
qam64-ctc-3/4 | qam64-ctc-5/6].

repetition

This parameter only applies to the MS.

The repetition coding.

Possible values: [1 | 2 | 4 | 6].

setLinkAdaptationUI

Other tab.

Defines UL link adaptation parameters.

Parameters

mode

Link adaptation mode.

Value in range [manual | automatic].

protection

CINR protection in dB against implementation CINR.

Float.

hysteresis

CINR hysteresis in dB when upgrading the FEC code.

Float.

setLogFilter

Logs tab.

Enables or disables the filter log.

Parameters

enable

Enables the log filter.

Integer with the following values:

setMacDI

MacFrame tab.

Changes the downlink channel descriptor configuration.

Parameters

tx-power

BS transmission power in dBm.

Integer.

init-ranging-max-rx-power

Maximum Received Signal Strength at the BS during initial ranging in dBm.

Integer.

frequency

Frequency of the downlink in kHz.

Integer.

version

Version of the IEEE 802.16 specification: [V1 | V2 | V3 | V4]

bsRestartCount

BS restart count. Integer in [0..255]

bs-id

Specifies the MAC Address of the BS.

String.

iuc0-fec-code

The system FEC code.

Enumeration, see coding described in the Note below.

iuc1-fec-code

FEC code of IUC 1.

Enumeration, see coding described in the Note below.

iuc2-fec-code

FEC code of IUC 2.

Enumeration, see coding described in the Note below.

iuc3-fec-code

FEC code of IUC 3.

Enumeration, see coding described in the Note below.

iuc4-fec-code

FEC code of IUC 4.

Enumeration, see coding described in the Note below.

iuc5-fec-code

FEC code of IUC 5.

Enumeration, see coding described in the Note below.

iuc6-fec-code

FEC code of IUC 6.

Enumeration, see coding described in the Note below.

iuc7-fec-code

FEC code of IUC 7.

Enumeration, see coding described in the Note below.

iuc8-fec-code

FEC code of IUC 8.

Enumeration, see coding described in the Note below.

iuc9-fec-code

FEC code of IUC 9.

Enumeration, see coding described in the Note below.

iuc10-fec-code

FEC code of IUC 10.

Enumeration, see coding described in the Note below.

iuc11-fec-code

FEC code of IUC 11.

Enumeration, see coding described in the Note below.

iuc12-fec-code

FEC code of IUC 12.

Enumeration, see coding described in the Note below.

harq-max-retries

Maximum number of HARQ retransmissions. Integer in [0..255].

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

Note: FEC codes are represented by an enumeration with the following possible values:

[qpsk-cc-1/2, qpsk-cc-3/4, qam16-cc-1/2, qam16-cc-3/4,
qam64-cc-1/2, qam64-cc-2/3, qam64-cc-3/4, qpsk-ctc-1/2,
qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2,
qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6, none]

setMacFrame

MacFrame tab.

Changes the frame channel descriptor configuration.

Parameters

started

Channel start state.

Integer with the following values:

bandwidth

Channel bandwidth.

Possible values:

[3.5MHz | 5MHz | 7MHz | 8.75MHz | 10MHz].

Note: bandwidth=8.75MHz is the only value supported in the current release.

cp

G-ratio of the cyclic prefix start.

Possible values: [1/4 | 1/8 | 1/16 | 1/32].

Note: cp=1/8 is the only value supported in the current release.

duration

Frame duration.

Possible values: [5ms, 10ms].

fft-size

FFT size.

Enumeration, possible values: [512, 1024] .

[0] Stop

[1] Start

[5ms] SQN1110 SoC ASIC

[10ms] Preliminary FPGA on QSNx110-P Board

Note: fft-size=1024 is the only value supported in the current release.

preamble-index

Preamble index, which determines the PUSC segment.

Integer in the range [0..113].

subchannel-bitmap

Subchannel bitmap.

Integer in the range [1..63].

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

setMacUI

MacFrame tab.

Changes the uplink channel descriptor configuration.

Parameters

i-rng-backoff-start

Initial ranging back-off start.

Integer in the range [0..15].

i-rng-backoff-end

Initial ranging back-off end.

Integer in the range [0..15].

p-rng-backoff-start

Periodic ranging back-off start.

Integer in the range [0..15].

p-rng-backoff-end

Periodic ranging back-off end.

Integer in the range [0..15].

bwr-backoff-start

Bandwidth request back-off start.

Integer in the range [0..15].

bwr-backoff-end

Bandwidth request back-off end.

Integer in the range [0..15].

reservation-timeout

Reservation timeout after sending a Bandwidth Request .

Integer in the range [1..32].

frequency

Frequency of the uplink in kHz.

Integer.

permutation-base

Uplink permutation base parameter, UIPermBase in the IEEE 802.16e-2005 standard.

Integer in the range [0..69].

subchannels-bitmap

Uplink subchannels bitmap.

Hexadecimal string; [0] activates all subchannels.

ranging-code-group-start

Start of the ranging code range.

Parameter S, see the IEEE 802.16e-2005 standard.

Integer in the range [0..255].

ranging-code-irng-qty

Quantity of I-RNG code.

Parameter N, see the IEEE 802.16e-2005 standard.

Integer in the range [1..20].

ranging-code-prng-qty

Quantity of P-RNG code.

Parameter M, see the IEEE 802.16e-2005 standard.

Integer in the range [1..64].

ranging-code-bwr-qty

Quantity of BWR code.

Parameter L, see the IEEE 802.16e-2005 standard.

Integer in the range [1..64].

ranging-code-ho-qty

Quantity of HO code.

Parameter O, see the IEEE 802.16e-2005 standard.

Integer in the range [1..64].

max-harq-rep

Maximum number of Hybrid ARQ retransmissions.

Integer in the range [0..255].

harq-max-retries

Maximum number of HARQ retransmissions. Integer in [0..255].

tx-report-threshold

Tx report threshold, in dB.

Enum in [0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | infinite]

tx-report-period

Tx report period, in frames number.

Enum in [1 | 2 | 4 | 8 | 16 | 32 | 64 | 128 | 256 | 512 | 1024 | 2048 | 8192 | 16384 | infinite]

tx-report-alpha

Tx report alpha ratio.

Enum in [1/16 | 2/16 | 3/16 | 4/16 | 5/16 | 6/16 | 7/16 | 8/16 | 9/16 | 10/16 | 11/16 | 12/16 | 13/16 | 14/16 | 15/16 | 16/16]

ffb-fec-code

FEC code of IUC 0, fast feedback. See coding described in the Note below.

iuc1-fec-code

FEC code of IUC 1. See coding described in the Note below.

iuc2-fec-code

FEC code of IUC 2. See coding described in the Note below.

iuc3-fec-code

FEC code of IUC 3. See coding described in the Note below.

iuc4-fec-code

FEC code of IUC 4. See coding described in the Note below.

iuc5-fec-code

FEC code of IUC 5. See coding described in the Note below.

iuc6-fec-code

FEC code of IUC 6. See coding described in the Note below.

iuc7-fec-code

FEC code of IUC 7. See coding described in the Note below.

iuc8-fec-code

FEC code of IUC 8. See coding described in the Note below.

iuc9-fec-code

FEC code of IUC 9. See coding described in the Note below.

iuc10-fec-code

FEC code of IUC 10. See coding described in the Note below.

Note: FEC codes are represented by an enumeration with the following possible values:

[qpsk-cc-1/2, qpsk-cc-3/4, qam16-cc-1/2, qam16-cc-3/4, qam64-cc-1/2, qam64-cc-2/3, qam64-cc-3/4, qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6, none]

subchannel-rotation

Enables subchannel rotation on the first Zone.

Integer in range [0..1]. Default value is 1 (true).

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

setMcastPhyDI

Other tab.

Sets multicast service flow PHY parameters.

Parameters

sfidMcast

SFID of the multicast service flow.

Integer.

Exclusive required parameter.

cidMcast

CID of the multicast service flow.

Integer in the range [1..65535].

Exclusive required parameter.

fec-code

FEC code.

Enumeration, possible values:[qpsk-cc-1/2, qpsk-cc-3/4, qam16-cc-1/2, qam16-cc-3/4, qam64-cc-1/2, qam64-cc-2/3, qam64-cc-3/4, qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6].

Required parameter

repetition

The repetition coding.

Enumeration, possible values:[1 | 2 | 4 | 6].

zone-id

The downlink zone ID.

Integer in the range [0..7].

mimo-kind

The MIMO matrix type.

Possible values: [siso | matrix-a | matrix-b].

setMii

Other tab.

Sets MII link configuration.

Parameters

speed

Maximum link speed, possible values: [10 | 100].

10: Maximum link speed is 10 Mbps

100: Maximum link speed is 100 Mbps

duplex

Duplex mode [half-duplex | full-duplex]

mtu

Maximum Transfer Unit. Integer in [1526..2048]

setNeighborAdvertisement

Other tab.

Configures neighbor advertisement.

Parameters

enable

Enables database advertisement.

Integer with the following values:

period

Advertisement period in ms.

Integer in the range [1000...10000].

setPkm

Other tab.

Configures PKM settings.

Parameters

auth-lifetime

Lifetime in seconds that the BS assigns to a new authorization key (PKMv1 only).

Integer in the range [0..6048000]. The default value is 7 days, that is value 6048000.

tek-lifetime

Lifetime in seconds that the BS assigns to a new traffic encryption key (TEK).

Integer in the range [0..604800]. The default value is 12 hours, that is value 43200.

auth-grace-time

Default authorization key grace time, in seconds.

Integer in the range [0..3024000].

tek-grace-time

Default encryption key grace time, in seconds.

Integer in the range [0..302399].

auth-wait-timeout

Default authorization wait timeout, in seconds.

Integer in the range [0..30].

reauth-wait-timeout

Default reauthorization wait timeout, in seconds.

Integer in the range [0..30].

operational-wait-timeout

Default operational wait timeout, in seconds.

Integer in the range [0..10].

rekey-wait-timeout

Default rekey wait timeout, in seconds.

Integer in the range [0..10].

auth-reject-wait-timeout

Default authorization reject wait timeout, in seconds.

Integer in the range [0..600].

setPkmCs

Other tab.

Configures PKM settings related to crypto suites.

Parameters

algo

The data encryption algorithm of the crypto-suite.

Possible values: [none | none-des | des | aes-keywrap].

Required parameter.

rank

New rank of the crypto suite. Integer in the range [1..1000]. The default value is 0.

enabled

Enabled status of a supported crypto-suite.

Integer with the following values:

By default, the specified crypto-suite is disabled.

setProvisionedPsc

Other tab.

Sets PSC configuration.

Parameters

direction

Direction of the associated service flow.

Possible values: [undefined, downlink, uplink]. Default value is undefined.

tir

Traffic Indication required flag.

Possible values: [0..1]. Default value is 1 (true).

ttwf

Traffic triggered waking flag.

Possible values: [0..1]. Default value is 0 (false).

initSleepWindow

Initial Sleep window, in frame quantity.

Integer in range [0..255].

Required parameter.

listenWindow

Listening window, in frame quantity.

Integer in range [0..255].

Required parameter.

finalSleepWindowBase

Final Sleep window base, in frame quantity.

Integer in range [0..1023].

Required parameter.

finalSleepWindowExp

Final Sleep window exponent.

Integer in range [0..7].

Required parameter.

cidQty

CID quantity.

Integer in range [0..7]. Default value is 0, for all the CIDs of the MS.

cidList

CID list.

String.

setQoSDI

Other tab.

Configures downlink QoS.

Parameters

above-minrate-mode

Mode when above the minimum rate:

[roundrobin | strict | weightedFair]

where:

roundrobin All DL CIDs are served by the BS one by one in a sequential manner.

Strict Traffic is allocated first to service flows associated with the highest priority class.

Weighted Fair Scheduling per service flow.

Each scheduling class "i" is associated with a weight wamr(i).

For all CID with traffic, bandwidth BW_i is allocated to CID of traffic priority "i", so that the ratio BW_i/wamr(i) remains equal, under congestion.

This is a required parameter.

below-minrate-mode

Mode when below the minimum rate:

[roundrobin | strict | weightedFair]

Same definitions as for above-minrate-mode (understanding wamr instead of wamr).

This is a required parameter.

above-minrate-fairness

Fairness type when above the minimum rate: Integer [0..100], balance between byte and resource fairness.

0=byte fairness only, 100=resource fairness only

below-minrate-fairness

Fairness type when below the minimum rate: Integer [0..100], balance between byte and resource fairness.

0=byte fairness only, 100=resource fairness only.

wamr0 – wamr7

Weight for priorities 0 – 7 above the minimum rate. Integer range [1..255]. The default value of wamrn is 1.

wbmr0 – wbmr7

Weight for priorities 0 – 7 below the minimum rate. Integer range [1..255]. The default value of wbmrn is 1.

setQosHRateDI

Other tab.

Configures a DL HQoS parameter set.

Parameters

hrate-index

Index of the parameter set.

Integer in the range [0..255].

Required parameter.

instant-maxrate

MS instantaneous downlink maximum data rate, in bits/s.

Integer in the range [0..100000000]. 0 means None. Default value is 0.

longterm-maxrate

MS long term downlink maximum data rate, in bits/s.

Integer in the range [0..100000000]. 0 means None. Default value is 0.

longterm-initial-credit

Long-term initial credit, in seconds.

Integer in the range [1..86400]. Default value is 1.

setQosHrateSsDI

Other tab.

Associates an MS to a DL HQoS parameters set.

Parameters

mac

Selects the MS with the given MAC address.

String.

Exclusive required parameter.

cid

Selects the MS with the given CID.

Integer in the range [1..65535].

Exclusive required parameter.

hrate-index

Index of the parameter set.

Integer in the range [-1..255]. Value -1 means None.

Required parameter.

setQosHrateSsUI

Other tab.

Associates an MS to a UL HQoS parameters set.

Parameters

mac

Selects the MS with the given MAC address.

String.

Required parameter.

cid

Selects the MS with the given CID.

Integer in the range [1..65535].

Required parameter.

hrate-index

Index of the parameter set. Integer in range [-1..255]. Value -1 means None.

Required parameter.

setQosHRateUI

Other tab.

Configures a UL HQoS parameter set.

Parameters

hrate-index

Index of the parameter set.

Integer in the range [0..255].

Required parameter.

instant-maxrate

MS instantaneous Uplink maximum data rate, in bits/s.

Integer in the range [0..100000000]. 0 means None.

longterm-maxrate

MS long term Uplink maximum data rate, in bits/s.

Integer in the range [0..100000000]. 0 means None.

longterm-initial-credit

Long-term initial credit, in seconds.

Integer in the range [1..86400].

setQosRedDI

Other tab.

Enables and disables the downlink RED and sets the maximum RED latency.

Parameters

latency

Maximum DL RED latency in milliseconds. This parameter represents the maximum buffering time of a downlink packet in the scheduler.

Integer in the range [0..5000].

enable

Enables or disables the downlink RED algorithm.

Integer with the following values:

setQosRedDIProfile

Other tab.

Configures the downlink RED drop profile.

Parameters

l0 – l7

Latency (l) for points 0 – 7, expressed as a percentage.

Integer in the range [0..100].

p0 – p7

Drop probability (p) for points 0 – 7, expressed as a percentage.

Integer in the range [0..100].

setQosRedUIDefault

Other tab.

Configures congestion control in the uplink for SF without maximum latency.

Parameters

latency

Maximum RED latency in milliseconds.

Integer in the range [0..5000].

setQosRedUIDefaultProfile

Other tab.

Configures the uplink RED drop profile for SF without maximum latency.

Parameters

l0 – l7

Latency (l) for points 0 – 7.

Percentage integer in the range [0..100].

p0 – p7

Drop probability (p) for points 0 – 7.

Percentage integer in the range [0..100].

setQosRedUIMaxLatencyProfile

Other tab.

Configures the uplink RED drop profile for SF with non-null maximum latency.

Parameters

l0 – l7

Latency (l) for points 0 – 7.

Percentage integer in the range [0..100].

p0 – p7

Drop probability (p) for points 0 – 7.

Percentage integer in the range [0..100].

setQosShapingDI

Other tab.

Enables and disable DL shaping.

Parameters

enable

Enables or disables the downlink shaping function.

Integer with the following values:

The default status is enabled.

Required parameter.

setQosUI

Other tab.

Configures uplink QoS.

Parameters

above-minrate-mode

Mode when above the minimum rate: [roundrobin | strict | weightedFair]

where:

below-minrate-mode

Mode when below the minimum rate: [roundrobin | strict | weightedFair]

Where:

- | | |
|--------------|---|
| Roundrobin | All DL CIDs are served by the BS one by one in a sequential manner. |
| Strict | Traffic is allocated first to service flows associated with the highest priority class. |
| weightedFair | Scheduling per service flow. |

Each scheduling class “i” is associated with a weight $wamr(i)$.

For all CID with traffic, bandwidth BW_i is allocated to CID of traffic priority “i”, so that the ratio $BW_i/wamr(i)$ remains equal, under congestion.

above-minrate-fairness

Fairness type when above the minimum rate: Integer [0..100], balance between byte and resource fairness.

0=byte fairness only, 100=resource fairness only

below-minrate-fairness

Fairness type when below the minimum rate: Integer [0..100], balance between byte and resource fairness.

0=byte fairness only, 100=resource fairness only.

wamr0 – wamr7

Weight for priorities 0 – 7 above the minimum rate. Integer range [1..255]. The default value of wamrn is 1.

wbmr0 – wbmr7

Weight for priorities 0 – 7 below the minimum rate. Integer range [1..255]. The default value of wbmrn is 1.

setScanning

Other tab.

Configures periodic scanning.

Parameters

enable

Enables periodic scanning.

Integer with the following values:

period

Scanning period in ms.

Integer in the range [50..10000].

duration

Averaging duration in ms.

Integer in the range [10..10000].

window

Averaging window in ms.

Integer in the range [10..10000].

setSchedulerMac

Other tab.

Configures the MAC scheduler.

Parameters

ucd-period

Period in ms of the periodic UCD message sending. Integer.

ucd-repeat

Quantity of UCD message notification before UCD change.

Integer in the range [1..5].

dcd-period

Period in ms of the periodic DCD message sending.

Integer.

dcd-repeat

Quantity of DCD message notification before DCD change.

Integer in the range [1..5].

ertps-inactive

Behavior of inactive eRTPS (zero bytes requested).

Enum in [no-grant | rtps]

ss-max-distance

Maximum distance of an MS, in meters.

Integer in the range [0..70000].

compressed-map

Enables MAP compression.

Enumeration, possible values: [none | dl | dl-ul].

diuc0-repetition

DL-MAP, UL-MAP, UCD, DCD repeat quantity.

Enumeration, possible values: [1 | 2 | 4 | 6].

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

setSchedulerTdd

MacFrame tab.

Configures the TDD split.

Parameters

split

Size of the downlink sub-frame as a percentage of the frame being split.

Integer range [0..100].

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

SetSecondaryAsMain

Other tab.

Switches the definition of the main and secondary base station software packages. The secondary becomes main and the main becomes secondary.

Parameters

None.

setSfEnable

UnicastServiceFlow tab.

Enables or disables a service flow in the local service flow database.

Parameters

sfid

SFID of the service flow.

Integer.

cid

CID of the service flow.

Integer in the range [0..65535].

enable

Specifies whether the selected service flow is enabled or disabled in the service flow database.

Integer with the following values:

Required parameter.

setSnifferParams

Other tab.

Set debug sniffer parameters.

Parameters

dumpDescr

Enables or disables the packet descriptor dump debug feature.

Integer with the following values:

setSsPhyDI

SS tab.

Configures MS downlink parameters.

Parameters

mac

Selects a mobile station by its MAC address.

String.

Exclusive required parameter.

cid

Selects a mobile station by its connection ID.

Integer in the range [0..65535].

Exclusive required parameter.

fec-code

FEC code.

Enumeration, possible values: [qpsk-cc-1/2, qpsk-cc-3/4, qam16-cc-1/2, qam16-cc-3/4, qam64-cc-1/2, qam64-cc-2/3, qam64-cc-3/4, qpsk-ctc-1/2, qpsk-ctc-3/4, qam16-ctc-1/2, qam16-ctc-3/4, qam64-ctc-1/2, qam64-ctc-2/3, qam64-ctc-3/4, qam64-ctc-5/6]

repetition

The repetition coding.

Enumeration, possible values: [1 | 2 | 4 | 6]

zone-id

The downlink zone identifier.

Integer in the range [0..7].

map-id

The MAP identifier. integer in the range [0..3] with the following signification:

0 DL-MAP

1 First sub-MAP

2 Second sub-MAP

3 Third sub-MAP

mimo-kind

The MIMO Matrix type.

Possible values: [siso | matrix-a | matrix-b].

harq-fec-code

HARQ FEC code. Enum in [qpsk-cc-1/2 | qpsk-cc-3/4 | qam16-cc-1/2 | qam16-cc-3/4 | qam64-cc-1/2 | qam64-cc-2/3 | qam64-cc-3/4 | qpsk-ctc-1/2 | qpsk-ctc-3/4 | qam16-ctc-1/2 | qam16-ctc-3/4 | qam64-ctc-1/2 | qam64-ctc-2/3 | qam64-ctc-3/4, qam64-ctc-5/6]

harq-repetition

The HARQ repetition coding. Enum in [1 | 2 | 4 | 6]

harq-max-retries

Maximum number of HARQ retransmissions. Integer in [0..255]

setSsPhyUI

SS tab.

Sets MS uplink physical parameters.

Parameters

mac

MAC address of the mobile station.

Exclusive required parameter.

cid

Connection ID of the mobile station.

Integer in the range [0..65535].

Exclusive required parameter.

fec-code

FEC code.

Possible values: [qpsk-cc-1/2 | qpsk-cc-3/4 |

qam16-cc-1/2 | qam16-cc-3/4 | qam64-cc-1/2 | qam64-cc-2/3 | qam64-cc-3/4 | qpsk-ctc-1/2 | qpsk-ctc-3/4 | qam16-ctc-1/2 | qam16-ctc-3/4 | qam64-ctc-1/2 | qam64-ctc-2/3 | qam64-ctc-3/4 | qam64-ctc-5/6].

repetition

The repetition coding.

Enumeration, possible values: [1 | 2 | 4 | 6]

max-channel

The maximum channel quantity for Uplink bursts.

Integer in the range [1..35].

zone-id

The uplink zone identifier.

Integer in the range [0..7].

harq-fec-code

The Hybrid ARQ FEC code.

Enumeration, possible values: [qpsk-cc-1/2 | qpsk-cc-3/4 | qam16-cc-1/2 | qam16-cc-3/4 | qam64-cc-1/2 | qam64-cc-2/3 | qam64-cc-3/4 | qpsk-ctc-1/2 | qpsk-ctc-3/4 | qam16-ctc-1/2 | qam16-ctc-3/4 | qam64-ctc-1/2 | qam64-ctc-2/3 | qam64-ctc-3/4 | qam64-ctc-5/6]

harq-repetition

The Hybrid ARQ repetition coding.

Enumeration, possible values: [1 | 2 | 4 | 6]

harq-max-retries

Maximum number of HARQ retransmissions. Integer in [0..255].

setTimeSync

Config tab.

Timeout for synchronization attempt

Parameters

TimeSync Stop timeout

Enter the TimeSyncStop timeout in seconds.

TimeSync Fatal timeout

Enter the fatal timeout in seconds.

showCaps

SS tab.

Displays global capabilities.

Parameters

supported

Displays supported capabilities.

Integer with the following values:

configured

Displays configured capabilities.

Integer with the following values:

showDcdTrigger

Other tab.

Displays DCD trigger settings.

Parameters

None

showDhcp

Other tab.

Displays DHCP client configuration.

Parameters

None

showFwdAgeingTimeout

Other tab.

Displays entry timeout.

Parameters

None.

showFwdArEntry

Other tab.

Displays the address resolution forwarding entry.

Parameters

None.

showFwdEntries

Other tab.

Displays forwarding entries.

Parameters

None.

showFwdFilter

Other tab.

Displays forwarding filters.

Parameters

name
Name of the filter.
String.

showFwdInterface

Other tab.
Displays forwarding interface configuration.

Parameters

None

showFwdPort

Other tab.
Displays port configuration.

Parameters

port
Name of the port.
String.
Required parameter.

showFwdStats

Other tab.
Displays forwarding statistics.

Parameters

None.

showHandover

Other tab.
Displays handover trigger parameters.

Parameters

None.

showHoAveragingParam

Other tab.

Displays HO averaging parameters.

Parameters

None.

showIpAddr

Other tab.

Displays an IP address assigned with addIpAddress.

Parameters

None.

showLinkAdaptationDI

Other tab.

Displays DL link adaptation parameters.

Parameters

None.

showLinkAdaptationUI

Other tab.

Displays UL link adaptation parameters.

Parameters

None.

showLog

Logs tab.

Displays the logging state for the specified module.

Parameters

name

Selects the software module for which you want to show logging state.

Refer to the list of software modules in the S-Cube Architecture Guide.

String.

Required parameter. Uses the following syntax:

module/submodule

where:

module Selects the module for which you want to show logging state.

This can be set to *.

String.

Submodule Optional parameter reserved for Sequans internal use. This parameter selects the software submodule for which you want to show logging state. This can be set to *.

String.

showLogFilter

Logs tab.

Displays MS in a log filter.

Parameters

None.

showMacAddress

Misc tab.

Displays the Station MAC address.

Parameters

None.

showMacDI

MacFrame tab.

Displays the current downlink channel descriptor configuration.

Parameters

None.

showMacFrame

MacFrame tab.

Displays the frame channel descriptor content.

Parameters

None.

showMacStatsRx

Other tab.

Displays RF interface reception or management statistics.

Parameters

data

Integer with the following values:

mgt

Integer with the following values:

showMacUI

MacFrame tab.

Displays the uplink channel descriptor configuration.

Parameters

None.

showMcastPhyDI

Other tab.

Displays multicast service flow physical parameters.

Parameters

sfidMcast

Multicast service flow identifier.

Integer.

cidMcast

CID of the multicast service flow.

Integer in range [1..65535].

showMcastSfList

Other tab.

Displays the list of multicast service flows.

Parameters

verbose

Specifies whether to show detailed information.

Integer with the following values:

showMcastSsList

Other tab.

Displays the list of MS registered to a multicast service flow.

Parameters

cid

CID of the selected service flow.

Integer in the range [1..65535].

Exclusive required parameter.

sfid

SFID of the selected service flow.

Integer in the range [1..65535].

Exclusive required parameter.

verbose

Specifies whether to show detailed information.

Integer with the following values:

showNeighborAdvertisement

Other tab.

Displays neighbor advertisement parameters.

Parameters

None.

showNeighborBs

Other tab.

Displays a neighbor BS descriptor from the handover database.

Parameters

verbose

Specifies whether to show detailed information about the neighbor BS.

Integer with the following values:

showNeighborBsStat

Other tab.

Displays statistics of a neighbor BS.

Parameters

frequency

Neighbor BS RF frequency in kHz.

Integer in the range [1000000..10000000].

preamble-index

Neighbor BS Preamble index.

Integer in the range [0..113].

showPacketFlow

Statistics tab.

Displays the quantity of packets flowing on the downlink and the uplink, as well as the packet flow rate.

Parameters

None.

showPagingGroup

Other tab.

Displays paging groups registered at the BS.

Parameters

pgId

Paging group ID.

Integer in the range [0..65535].

ShowPkgFiles

Other tab.

Lists the files contained in the main and secondary packages.

Parameters

None.

showPkm

Security tab.

Displays PKM settings.

Parameters

None.

showPkmCs

Security tab.

Displays PKM settings related to crypto suites.

Parameters

None.

showProvisionedPsc

Other tab.

Displays the Power Saving Class characteristics.

Parameters

None.

showProvSf

SS tab.

Displays the provisioned Service Flows.

Parameters

mac

MAC address.

String.

Required parameter.

verbose

Specifies whether to show detailed information.

Integer with the following values:

showPsc

Other tab.

Displays the Power Saving Class information.

Parameters

pscId

power Saving Class identifier.

Integer in range [0..63].

ssId

MS identifier.

Integer in range [0..65535]. This parameter applies only to the BS.

verbose

Integer in range [0..1].

showQoSdI

Other tab.

Displays the downlink QoS parameters.

Parameters

None.

showQosHrateDI

Other tab.

Displays a downlink hierarchical QoS parameter set.

Parameters

hrate-index

Parameter set index.

Integer in the range [0..255].

showQosHrateUI

Other tab.

Displays an uplink hierarchical QoS parameter set.

Parameters

hrate-index

Parameter set index.

Integer in the range [0..255].

showQosUI

Other tab.

Displays UL QoS configuration.

Parameters

None.

showRfRx

Other tab.

Displays the RF frequency in Rx.

BS and MS

Parameters

mac-domain

MAC domain. This parameter applies to the BS only

Integer in range [0..2]. Default value is 0.

showRfTx

Other tab.

Displays the RF frequency in Tx.

Parameters

mac-domain

MAC domain. This parameter applies to the BS only

Integer in range [0..2]. Default value is 0.

showSa

Security tab.

Displays security association.

Parameters

said

Selects the SA identifier.

Integer in the range [0..65535].

bcid

On the BS, specifies the MS by its base connection ID.

Integer in the range [0..65535].

verbose

Specifies whether to show detailed information.

Integer with the following values:

showSaAuthorizedSs

Other tab.

Displays MS list authorized on a security association.

Parameters

said

Selects the said.

Integer in the range [0..65535].

showSc

Other tab.

Displays the service class information.

Parameters

scid

SCID of the service class for which you want to display information.

Integer in the range [1..65535].

verbose

Specifies whether to show detailed information.

Integer with the following values:

showScanner

Other tab.

Displays the scanning list.

Parameters

None.

showScanning

Other tab.

Displays periodic scanning parameters.

Parameters

None.

showSchedulerMac

MacFrame tab.

Displays the MAC scheduler configuration.

Parameters

mac-domain

MAC domain.

Integer in range [0..2]. Default value is 0.

showSf

UnicastServiceFlow tab.

Displays information about a given service flow.

Parameters

verbose

Specifies whether to show detailed information.

Integer with the following values:

sfid

Selects the SF with its SFID.

Integer.

cid

Selects the SF with its CID.

Integer in the range [0..65535].

showSniffer

Other tab.

Displays the sniffer state and filters.

Parameters

None.

showSs

SS tab.

Displays MS information.

Parameters

mac

Selects the mobile station with the specified MAC address.

String.

cid

Selects the mobile station with the specified CID.

Integer in the range [0..65535].

verbose

Specifies whether to show detailed information.

Integer with the following values:

showSsAuth

Security tab.

Displays MS authorization.

Parameters

mac

Selects the mobile station with the specified MAC address.

cid

Selects the mobile station with the specified CID.

Integer in the range [0..65535].

verbose

Specifies whether to show detailed information.

Integer with the following values:

showSsCaps

SS tab.

Displays the negotiated capabilities of an MS.

Parameters

mac

Selects the mobile station with the specified MAC address.

String.

cid

Selects the mobile station with the specified CID.

Integer in the range [0..65535].

requested

Displays requested capabilities.

Integer with the following values:

operational

Displays negotiated operational capabilities.

Integer with the following values:

showSsHarqStats

Other tab.

Displays HARQ statistics for a MS.

Parameters

bcid

Basic CID of the MS for which you want to display statistics.

Integer in the range [0..65535].

Exclusive required parameter.

showSsPhyStatsDI

Statistics tab.

Displays downlink MS physical statistics.

Parameters

For the mobile station, this command has no parameters.

For the base station, this command has the following parameters:

mac

Selects a mobile station by its MAC address.

String.

cid

Selects a mobile station by its connection ID.

Integer in the range [0..65535].

alpha

Averaging parameter for global request in 1/32 dB.

Integer in the range [1..16].

type

Type of CINR to be reported.

Possible values: [pcinr | ecinr].

report-type

Feedback Type.

Possible values: [preamble | zone].

permutation

Zone Permutation.

Possible values: [pusc-sc-0 | pusc-sc-1 | fusc | optional-fusc | safety-channel | amc].

measure-type

Measurement type.

Possible values: [pilot | data].

zone-type

Zone type.

Possible values: [non-stc | stc | aas | stc-dedicated-pilots].

prbs-id

Zone PRBD_ID.

Integer in the range [0..3].

major-group-bitmap

PUSC Major group bitmap.

Integer in the range [0..63].

reuse

Preamble use.

Possible values: [1 | 3]. Default value is 1.

cinr-alpha

Averaging parameter for Physical CINR request in 1/16 dB.

Integer in the range [1..16].

showSsPhyStatsUI

Statistics tab.

Displays uplink MS physical statistics.

Parameters

mac

MAC address of the MS for which you want to display statistics.

String.

Exclusive required parameter.

cid

Connection ID of the MS for which you want to display statistics.

Integer in the range [0..65535].

Exclusive required parameter.

showTime

Other tab.

Displays the system current time.

Parameters

None.

showTimeSyncLockStatus

Config tab.

Indicates whether the base station is synchronized.

Parameters

None.

showTimeSyncParams

Config tab.

Shows the configured values of [setTimeSync](#).

Parameters

None.

showTod

Other tab.

Displays the client TOD.

Parameters

None.

ShowTrap

Other tab.

Lists the SNMP traps currently defined.

Parameters

TrapName

Select the name of the trap to show.

showVersion

Misc tab.

Displays the system version.

Parameters

None.

sniffShowState

Private tab.

Shows the current parameters controlling the packet sniffer.

Parameters

None.

startSs

Other tab.

Starts the IEEE 802.16e MAC software.

Parameters

None.

stopSs

Other tab.

Stops the IEEE 802.16e MAC software.

Parameters

None.

SysUptime

Other tab.

Shows the time that elapsed since the last time the base station has been reset.

Parameters

None.

TrapConfig

Other tab.

Allows you to define SNMP traps.

Parameters

TrapName

Specify the trap name.

Send

Select 1=Enable or 2=Disable.

Severity

Select 1=Critical 2=Major 3=Minor 4=Warning 5=Info.

Threshold

Enter the trap threshold (PA1Max: 0-1023 PA2Max: 0-1023 PA3Max: 0-1023 Temperature: 0-800).

CounterThreshold

Enter trap counter threshold.

CounterAutoReset

Select 1=Enable 2=Disable.

CounterReset

Select 1=Enable 2=Disable.

TrapEnable

Other tab.

Enables traps defined via the TrapConfig command.

Parameters

Trap

Select 1=Enable 2=Disable.

TrapGetActive

Other tab.

Sends from the base station all active traps.

Parameters

None.

TrapIpAddress

Other tab.

Specifies the IP address to which traps are sent.

Parameters

None.

UpdateChangesFile

Other tab.

When you modify the base station configuration, the changes are written to a separate changes file. The next time the base station resets, it also reads the changes file. This command allows you to apply the changes made after the last reset (instead of resetting the station).

Parameters

None.

UpdateSnmpAccess

Other tab.

Updates the SNMP user authorizations with the details of the newly added users.

Parameters

Read Community

Enter Read Community

Write Community

Enter Write Community

User Level

Enter User Level [0-Developer,1-Mng,2-Tech,3-User]

UserLogin

Other tab.

Logs the user in to the base station.

Parameters

User Name

Password

UserLogOut

Other tab.

Logs the user out of the base station.

Parameters

User Name

Password

Appendix A –Specifications

Radio and Modem:

Frequency	WiN7013-2: 1350 MHz to 1400 MHz WiN7025-2: 2496 MHz to 2690MHz WiN7035-2: 3400 MHz to 3600 MHz WiN7037-2: 3600MHz to 3720MHz
Radio Access Method	IEEE802.16-2005 (16e OFDMA)
Compatibility	WiMAX Forum Wave 2 Profile
Operation Mode	TDD
Channel Bandwidth	3.5Mhz, 5 MHz, 7Mhz, 10 MHz
Frequency Resolution	0.25 MHz
Number of Antenna ports	2
Antennas Connectors	2x N-Type, 50 ohm, lightning protected
Diversity Support	STC/MIMO
Output Power [P1dB]	2 x 45W;
Output Power (average)	36 dBm +/-1dB maximum
FFT/Modulation	512/1024 FFT points; QPSK, 16QAM, 64QAM
FEC	Convolution Code and Turbo Code
TPC	15dB
Synchronization	GPS

Network Interfaces:

Network	1. 37-60VDC 2. 10/100BaseT Half/full Duplex IEEE 802.3 CSMA/CD
ASN GW Compatibility	WiMAX Forum R6 Profile C Compatible with CISCO ASN-GW

Ordering Information:

Part Number	WiN70XX-2-Y-ZZE-W
XX – Frequency range	See frequency table for details
Y – Sync. Interface	G – GPS
ZZ – PA peak power [Watt]	45;

Configuration and Management:

Management	SNMP
SNMP Agent	SNMP ver 2 client: MIB II (RFC 1213), Private Win-Max MIBs
Software Upgrade	FTP
Remote Configuration	FTP

Mechanical:

Dimensions [HxWxD]	60cm x 27cm x 10cm
Weight	<15Kg

Power Interface:

Input	48VDC nominal (37-60VDC)
Power Consumption	140Watt maximum

Environmental:

Operating Temperature	-40°C to +55°C
Operating Humidity	5%-95% non condensing, Weather protected

Standards Compliance:

EMC	FCC part 15, subpart B, class A ETSI EN 301489-1/4
Safety	TUV-UL 60950-1 IEC 60950-1
Environmental	ETS 300 019: Part 2-1 T 1.2 & part 2-2 T 2.3 Part 2-4 T 4.1E
Enclosure	Type 3R (IP66)
Immunity	EN61000-4-2 EN61000-4-4 EN61000-4-5
Radio	ETSI EN302 326

List of Acronyms

AAA	Authentication Authorization Accounting
AES	Advanced Encryption Standard
AMC	Adaptive Modulation and Coding
API	Application Programming Interface
ASN	Access Service Network
ASP	Application Service Provider
ATPC	Automatic Transmit Power Control
BE	Best Effort
BPSK	Binary Phase Shift Keying
BST	Base Station
BWA	Broadband Wireless Access
cBST	Compact Base Station
CPE	Customer Premise Equipment
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
EAP	Extensible Authentication Protocol
ErtPS	Extended Real-Time Polling Service
FFT	Fast Fourier Transfer
FTP	File Transfer Protocol
FUSC	Fully Used Sub-Channelization
GW	Gateway
HA	Home Agent
HTTP	Hypertext Transport Protocol
ICMP	Internet Control Message Protocol
IDU	Indoor Units
IEEE	Institute of Electronic and Eclectic Engineers
IGMP	Internet Group Multicast Protocol

IMS	IP Multimedia System
IP	Internet Protocol
IPSec	IP Security
LAN	Local Area Network
LOS	Line-of-sight
MAC	Media Access Control
MAI	Multiple Access Interference
MAN	Metropolitan Area Network
MGCP	Media Gateway Control Protocol
MIMO	Multiple-Input, Multiple-Output
MIP	Mobile IP
MSG	Multi-Service Gateways
NAP	Network Access Provider
NMS	Network Management System
NLOS	Non-line-of-sight
nrtPS	Non-Real Time Polling Service
NSP	Network Service Provider
OAM	Operations and Maintenance
ODU	Outdoor Units
OFDM	Orthogonal Frequency Division Multiplexing
OFDMA	Orthogonal frequency division multiple access
PDA	Personal Digital Assistant
PMIP	Proxy Media IP
POP	Point of Presence
PPTP	Point-to-Point Tunneling Protocol
PUSC	Partially used sub-channelization
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency

rtPS	Real-Time Polling Service
SF	Service Flow
SIP	Session Initiation Protocol
SLA	Service Level Agreements
SNMP	Simple Network Management Protocol
SS	Subscriber Station
STC	Space-time coding
SU	Subscriber Unit
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
UGS	Unsolicited Grant Service
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WiMAX	Worldwide Interoperability for Microwave Access
Win-MAX™	WiNetworks WiMAX Product Family
WINMS	WiNetworks Network Management System