SOLECTEK
www.solectek.com

SkyWay-MAX

Operator's Guide

Solectek #1524604, rev 2.0

2 Operator's Guide

i. About this Guide

Congratulations on the purchase of your Solectek SkyWay MAX wireless system. This document has been supplied to assist with the turn up, commissioning and long-term management of a SkyWay MAX wireless system.

The following Solectek models are covered herein:

Outdoor Base Stations
ODB-3436
ODB-3537
ODB-3537H

Indoor Controllers
IC-100

Outdoor Subscriber Stations
ODS-3437

This document is divided into two sections. First, the document will walk through a typical network turn-up and commissioning sequence covering product configuration, pre-provisioning, installation and verification. Second, the document will review the detailed and advanced usage of the SkyWay MAX system to allow system tuning, long-term management and network scalability.

This document does not cover the physical installation of the SkyWay MAX devices. This information is presented in the following documents, available from your local reseller or directly from Solectek:

1524601: *SkyWay MAX Outdoor Base Station - Installation Guide*
1524602: *SkyWay MAX Outdoor Subscriber - Installation Guide*
1524603: *SkyWay MAX Indoor Base Station Controller - Installation Guide*

Similarly, this document does not cover the detailed planning processes required in developing a high-performance, scalable WiMAX network. Topics such as Network Planning, Frequency Planning/Reuse, RF coverage and QoS modeling are covered here in a summary fashion for introductory purposes only. Customers interested in additional information on these topics should contact Solectek's System Engineering group for further information.

ii. Legal Rights

Contents

I. Quick Launch

A. Assumptions

The following sections of this document assume that the SkyWay MAX Base Station Unit (BSU) and one or more Subscriber Stations (SS) have been physically installed and/or made available for bench Testing. For more information, consult the *SkyWay MAX Base Station Installation Guide* (Solectek part number 1524601).

Further, this guide assumes that network admission control is disabled and that all user traffic is supported on a single, network wide non-differentiated service, also referred to as 'open IP service.'

B. Before You Start

A minimum set of information must be gathered during the system planning process prior to network turn-up:

RF
Sector channel – for example: 3650 MHz
Sector bandwidth – for example: 7.0 MHz
RF frame length - for example 10 milliseconds
Network
IP Settings
Administrative Protocols – this is the list of IP/Ethernet protocols that must be supported on the SkyWay MAX network to allow the transport of basic services to the subscriber-side network(s). Examples include: DHCP, ARP, and PPPoE.

C. SkyWay MAX Manager

The Manager application is a Java-based program used for basic commissioning and management of a small to medium-sized SkyWay MAX network.

Designate a PC on the same IP subnet as the Base Station that will be used as the Manager PC, and ensure that there is no firewall installed that will block the operation of SNMP and SSH protocols. Obtain the version of the SkyWay MAX Manager application package (Solectek part number 1545901) that is compatible with your firmware release, and run the Setup program on the Manager PC. Contact Solectek Support if you are in any doubt about which version to use.

The same program can be used to manage either a BSU or an SS, so it may also be installed on a separate computer to facilitate configuration of SS units. Multiple sessions of SkyWay MAX Manager cannot be run on the same computer.

System Requirements

Microsoft Windows XP or XP Professional, SP2 or later
minimum 2 GHz processor (single core) minimum 1 GB of RAM
Java Runtime Environment version 1.6 or later

D. Base Station Turn-up

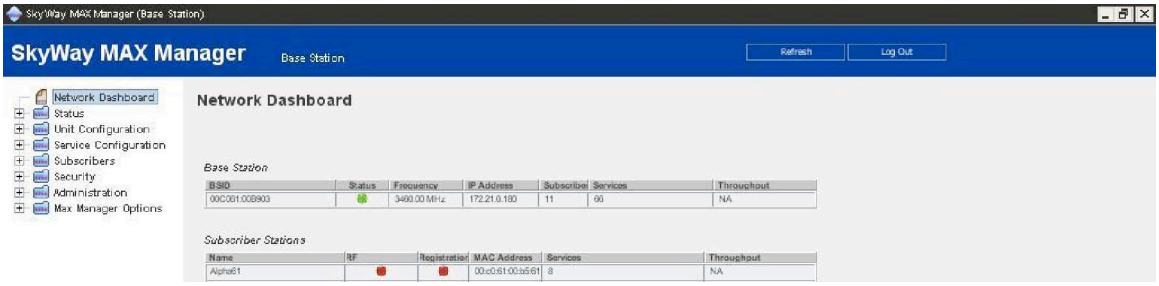
The Solectek BSU is shipped in an open access default configuration. Specifically, this means that all configurable security systems have been disabled, allowing initial network entry of SS units to be more straightforward.

Launch the Manager Application and log into the BSU using the appropriate IP address, Login and Password. See Appendix A for default access information.

Following a successful login, the Manager Application will display a Network Dashboard and, along the left side, a command Navigator.

Using the Navigator to access the necessary pages, the Minimum System Information collected in the previous section should be entered into the BSU configuration, as follows:

Unit Configuration : Port	Set appropriate RF Channel and Bandwidth. If desired, the BSID can be changed
Unit Configuration : Network	Set appropriate IP Address, Network Mask and Default Gateway.



Note: The Manager connection to the Base Station may be interrupted if changes are made to IP Settings. Re-launching of the Manager may be required.

E. Subscriber Provisioning

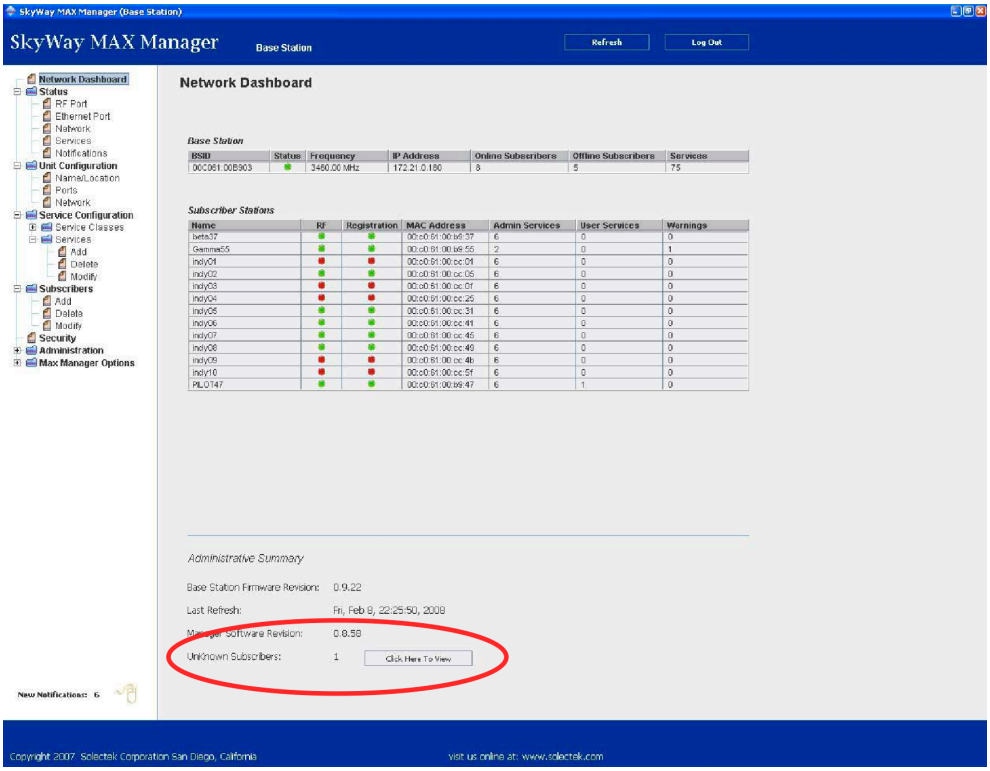
Like the BSU, the Solectek SS units are also shipped in an 'open' mode in which all configurable security features have been disabled. On the SS, this allows a fully 'plug-and-play' capability in which the SS can be deployed without pre-configuration of the SS, or pre-provisioning on the BSU.

This open mode implies the following:

- Base Station ID (BSID) Verification, used to define which set of BSUs the SS can connect to, is disabled. The SS will connect to the BSU first detected.
- Channel Plan File, used to limit the frequency search range of an SS, is set to the Factory Default set of frequencies (see Appendix).

F. Network Entry Process

Once the BSU and SS are powered and aligned, the SS will initiate the network entry process. Once an RF link has been established, the new SS will be added to the Manager Dashboard under the Administration section. Since the SS has not been pre-provisioned in the BSU, it is considered an unknown SS, as seen on the next page:

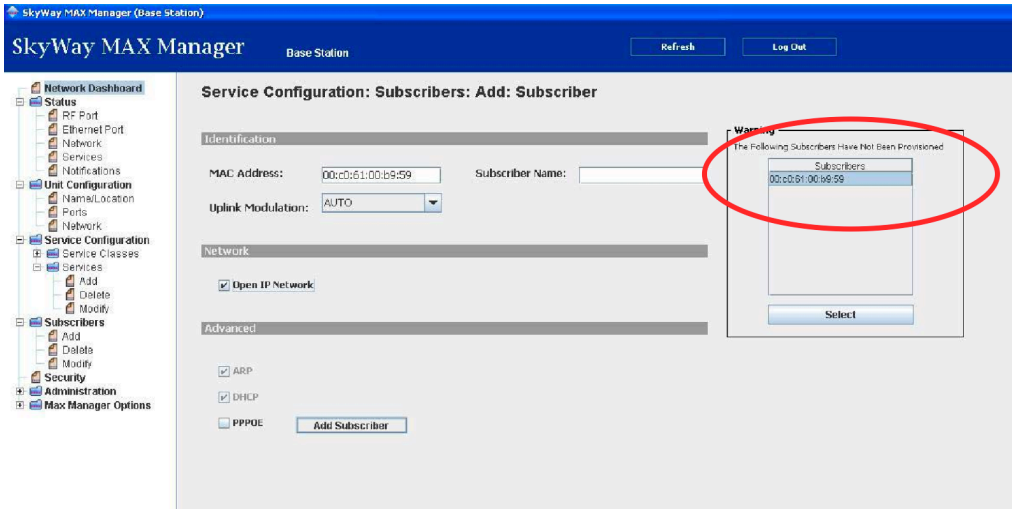


G. Getting Traffic Started

As will be covered in a subsequent section, the WiMAX protocol requires logical services to be created before network traffic can flow through the BSU and SS.

Once the SS has entered the BSU network, the Manager Application can be used to create a default set of services to allow basic traffic to be carried:

- From the Manager's Dashboard page, press the 'Click Here To View' button. This will lead to the Add Subscriber page, augmented with the current list of unknown SS units.
- From this page, the Administrative Services and an Open IP Service can be created.
- At a minimum, the ARP protocol must be added when provisioning a new SS. Open IP allows for one-click selection of common protocols for ease of initial turn up. DHCP and PPPoE are optional.
- At this point, the SS is provisioned and the network should be capable of passing basic traffic.



H. Basic Monitoring

Using the BSU Manager's Navigation Bar, the following screens can used to assess basic system status:

Dashboard	Used to summarize BSU and all connected SS parameters
Status : RF Port	Displays current RF port settings and packet counters
Status : Ethernet Port	Displays current Ethernet port settings and packet counters
Status : Network	Displays packet counter information per SS, and per Service
Status : Services	Displays service configuration and status, per SS
Status : Notifications	Lists Notification traps sent by BSU

This section ends the Quick Launch process. At this point, multiple SS units can be easily and quickly deployed and provisioned. However, there is a great deal of functionality and performance to be gained by implementing the processes and techniques described in the following sections of this Operator's Guide.

II. Network Entry Process

The Network Entry process is initiated as an SS attempts to find and join a BSU network. This section describes the RF and Security provisioning details managed during the Network Entry process that must be properly considered to set up a BSU sector.

The process moves through eight discrete steps in sequence:

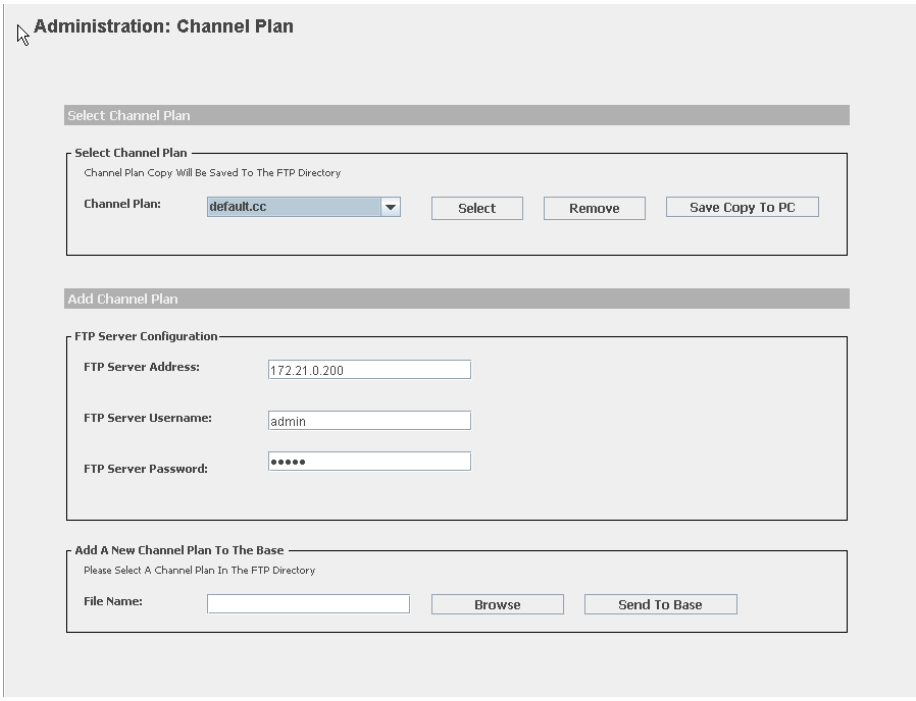
1. Synchronization: the SS detects the BSU and establishes communication
2. Ranging: the BSU adjusts for the time-of-flight delay in the signal and sets the SS transmit power
3. MAC ACL (optional): if ACL security is enabled, the BSU checks the MAC address of the SS and grants access if the MAC address appears on the list of authorized units
4. Capabilities: inform SS and BSU about basic characteristics of the system
5. Authorization: if certificate security is enabled, the BSU will verify that the SS unit's X.509 digital certificates are valid
6. Registration: the BSU issues the SS a Connection ID (CID)
7. Time: the BSU sets time of day on the SS unit, which has no time clock of its own
8. Provisioning: configured services are provisioned on the SS

A. RF Settings

The BSU defines the RF frequency used within a sector. The available channels are defined by a text file with a prescribed format, called a channel plan file, which is stored on the BSU. Each SkyWay MAX BSU is shipped with a default channel plan file. See the Appendix for a listing of default.cc, the default channel plan file and its formatting conventions.

The SS units scan the set of frequencies and bandwidths defined in its own local channel plan file. Like the BSU, the SS is shipped with a default channel plan file. If the desired frequency set differs from the default set or if a reduced scan time is desired, then a custom file can be created and uploaded to the SS. The channel plan file can contain a single channel, but it must match the channel selected on the BSU. If a custom file is needed on the SS, this operation should be performed prior to SS installation and turn-up.

Channel plan files can be uploaded on BSU and SS units using the Manager application. This functionality is accessed in the **Administration: Channel Plan** section.



Be sure to follow channel plan format conventions as noted in the Appendix.

B. Security

This section details the security elements of the SkyWay MAX system as they relate to Network Entry.

BSID Verification
The BSID is a unique, 6 octet (12 hex digit) identifier configured on each BSU at the factory. The first 3 octets have the fixed value of 00000B, an assigned Solectek identifier. The final 3 octets are, by default, the same value as the final 3 octets of the BSU's RF MAC address. These final 3 octets can be changed by the Operator (using hexadecimal digits 0-9, a-f) if desired.

When an SS is first powered up, and any time it is not connected to a network, the SS will scan the channels listed in its channel plan for a BSU sector wireless network to join. The BSID Verification feature ensures than an SS only attempts to join a BSU listed in its BSID table. To make initial provisioning simpler, the BSID verification feature is disabled by default. However, enabling this feature on the SS limits the risk of entry into an incorrect network. The BSID list is hosted on each SS, and can contain one or more BSIDs.

Each BS can have only one BSID, though any SS can have multiple BSIDs configured in its verification list
Remember, BSID verification enable/disable is an SS configuration parameter.

Access Control List (ACL)
A MAC based, Access Control List feature is available on the BSU. When enabled, the BSU must be provisioned with the RF MAC address of each SS to be granted network entry. Once the SS MAC address is added to the BSU, this SS will be tracked by the management system. If an SS attempts to join this BSU network without a corresponding ACL entry, it will be rejected.

The ACL feature is disabled by default. In this state, an SS that tries to join the network without a matching ACL MAC address, will be granted entry, but considered "unknown." Once services are defined for this SS, the unit will then be considered provisioned.

X.509 Digital Certificates

The X.509/PKM protocol set is an industry standard authentication method used to verify the credentials of an SS. When enabled, the SS credentials are validated by the BSU in a secure fashion. Rogue SS units, those not containing signed and validated X.509 digital certificates, are rejected from the BSU network.

This feature is managed by the BSU, and is disabled by default.

C. Open Mode vs. Pre-provisioning

When a system is configured in Open Mode (as shipped from the factory), SS units will join BSU networks as unknown subscribers.

Note that Open Mode allows the initial stages of network entry to proceed, resulting in the establishment of an RF connection. Intervention is required for network entry to proceed fully.

Both Administrative and User Services can then be added to desired unknown subscribers, making the SS fully provisioned.

When an SS is pre-provisioned in the BSU, all Network Entry and Services information about the SS is set up before the SS attempts to connect to the BSU. Once it is within RF range of a BSU, the SS enters the network and all pre-provisioned services are added to the system. Based upon these services, network traffic will begin flowing.

D. Registration

Once an RF connection has been established and access granted (if security systems are enabled), the SS is given a Connection ID (CID) by the BSU and service provisioning can then begin. An SS that does not complete the connection process successfully will continue to scan the channels indefinitely in an attempt to find a BSU sector that will allow it to enter.

E. Rate Limiter vs. WiMAX Mode

In order to simplify deployment for some operators, the system can be run in Rate Limiter mode. This will allow a Maximum Data Rate to be specified for each individual subscriber unit, but without the advanced traffic management and quality of service features of WiMAX. No prioritization of traffic types is possible in Rate Limiter mode: instead, uplink and downlink data rate limits on set a per-SS basis. This selection can be made under **Unit Configuration : Advanced**.

III. Services

A. Introduction

Traffic on a WiMAX/802.16 network passes between a BSU and SS over logical connections called services. Using services, an operator can filter, groom and prioritize network traffic allowing optimal performance and efficient use of wireless spectrum. For example, Voice over IP (VoIP) requires that latency and jitter to be minimized. Using WiMAX services, such traffic can be prioritized over traffic that is less sensitive to network conditions.

The critical operation of services can be explained as a two-stage process:

The first stage is classification. This filtering process only allows data packets onto a service if it meets certain criteria, such as source address or protocol type. SkyWay MAX classification methods include combinations of values present in common packet bit fields. See the Appendix for a complete list of available Ethernet and IPv4 classifiers.

The second stage involves the scheduling and transport of the packet across the wireless link. This process takes into account the QoS requirements of each active service as well as the current RF conditions. WiMAX service classes allow for consistent application of scheduling and QoS to multiple individual services. An understanding of the types of data the wireless system will carry - as well as a reasonable estimate of future growth and requirements - will help in defining services that will optimize performance for all the users of the system.

This section will discuss how traffic is classified on the SkyWay MAX system, how bandwidth is allocated via scheduling, and details the creation of services for data transport. A brief example will be given to illustrate how services can be designed.

B. Classification

Network traffic can only flow over a WiMAX service if it meets criteria defined by the operator. The classification process can be compared to a whitelist: data that does not match a classifier will not be allowed to pass on to a service. If a packet does not match any classifiers, the packet will be dropped. Classifiers are assigned to a single service and thus apply to a single subscriber and in a single direction (uplink or downlink).

Classifiers can be defined very narrowly to ensure that a certain type of traffic to or from a particular endpoint will be carried on a specific service. A very general classifier can be used to act as a sort of 'catch-all' so that traffic not otherwise classified will use a particular service.

C. Scheduling Types

WiMAX uses request and grant interactions between the SS and BS to provide deterministic access to the shared wireless link. WiMAX scheduling provides flexible service classes to prioritize bandwidth allocations on a per SS basis. Each WiMAX service class will use one of four possible scheduling types:

- **Unsolicited Grant Service (UGS):** provides pre allocated bandwidth grants for fixed-size packets on a regular basis and does not require SS requests, improving latency
- **real-time Polling Service (rtPS):** provides grants for variable-length packets on a periodic basis in real time, allows the SS to specify the size of the grant, optimizing throughput and latency
- **non real-time Polling Service (nrtPS):** polls on a regular basis, assuring that the SS can receive a grant for variable-length packets even in periods of high usage, improving throughput at the expense of latency
- **Best Effort (BE):** grants are provided when space is available, and an explicit request for bandwidth by the SS must be sent, received, allocated and granted before transmitting. BE is best for traffic without minimum throughput or latency requirements

It's important to select a scheduling type carefully to allow for efficient loading of the wireless link. For example, overuse of rtPS scheduling can result in reduced performance due to overhead, and UGS scheduling does result in allocated but unused bandwidth being lost.

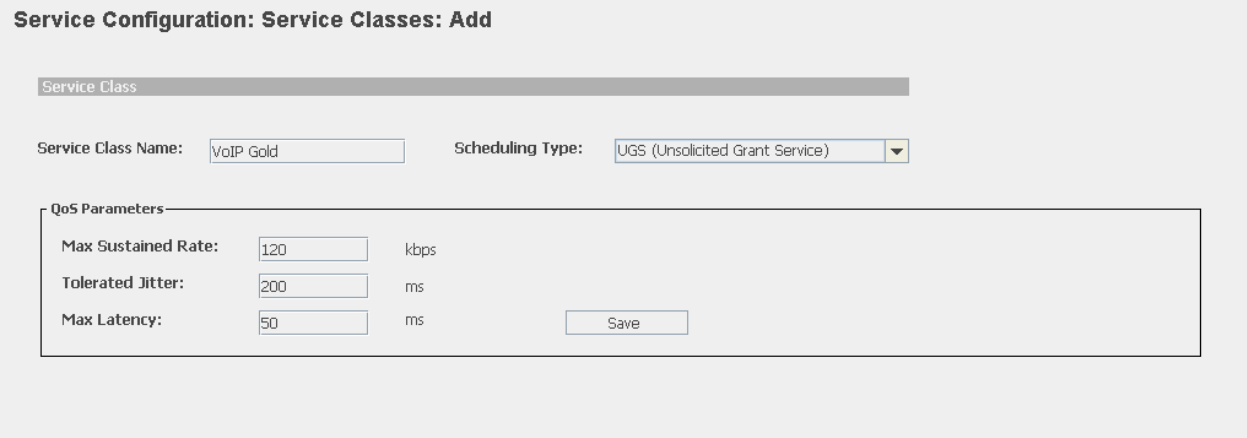
Summary of scheduling type operational considerations:

Scheduling Type	Impact on **Service**	Impact on **Media Access**	Impact on **Overhead**
UGS	Decreasing Latency	Increasing scheduling efforts	Decreasing efficiency
rtPS			
nrtPS			
BE	Increasing Latency	Decreasing scheduling efforts	Increasing efficiency

D. Service Classes

The WiMAX system supports the creation of service classes so that particular scheduling and QoS parameters can be applied to many services in a template fashion. This aids operators in implementing Service Level Agreements (SLAs) uniformly across the network. Multiple service classes can be created within a single BSU sector.

For example, for an Operator to deliver a given SLA, a set of QoS parameters could be defined with an appropriate scheduling type. These parameters would include the appropriate packet minimum and maximum throughput requirements, as well as maximum latency. A template service class can be created and named (e.g. "VoIP Gold") to capture all of these parameter values. For each subscriber with that SLA, then, this "Gold" class of service may be used to create a user service flow that will prioritize that traffic as needed.



Each class of service defines a particular scheduling method for putting data on the wireless link along with target and maximum metrics for the traffic it carries. In order to create service classes that will be of use for the life of the system, some forethought is advisable. Service classes that overallocate resources will not make efficient use of scarce bandwidth, which can result in less-than-optimal system performance as additional subscribers are added.

When a service class is created, the operator will define a minimum reserved data rate for each service assigned to that class. The BSU will attempt to provide bandwidth up to the minimum reserve rate, and then additional bandwidth subject to availability.

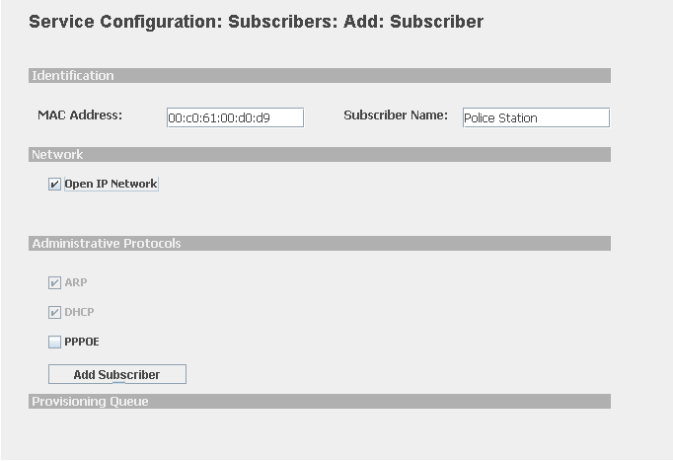
A maximum sustained traffic rate will also be specified in a service class definition. This is a physical-layer specification, and it should be understood that the actual performance experienced at an endpoint will be lower than the value set, due to overhead at higher layers, congestion on the wireless link and/or the endpoint's LAN, or other factors. The maximum sustained rate is meant as a rate-limiting throttle to improve allocation of bandwidth system-wide.

E. Services

As described above, services are required to carry network traffic across the wireless system. There are two types of services implemented in the SkyWay MAX system: administrative and user services. Administrative services are used to enable underlying protocols and to allow IP traffic to begin flowing with a minimum of configuration steps. User services bring the power and flexibility of WiMAX classification into play. Services can be defined as either unicast or multicast.

Administrative Services
IP networks require a number of administrative protocols running to provide basic functions such as Authorization (PPPoE), IP Address assignment (DHCP), IP address resolution (ARP), etc. Since all wireless traffic must be carried on an active service, each SS must be provisioned with a set of appropriate services to carry this traffic.

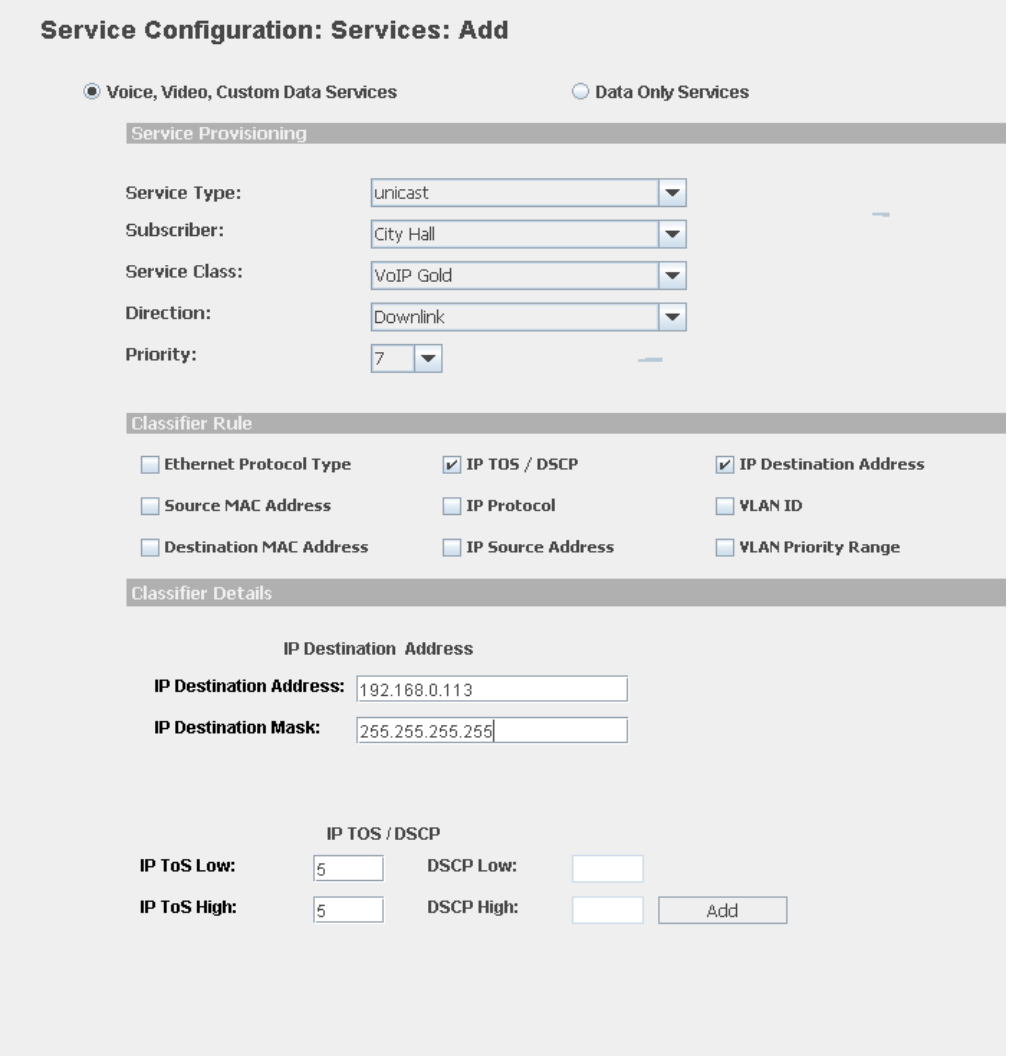
To accelerate the deployment of SS units, SkyWay MAX Manager provides a simplified method of adding such Administrative Services. When a subscriber unit is added to the system - either in Open Mode or pre-provisioned - the operator is provided a list of available administrative protocols. The 'Open IP' option allows the operator to select DHCP, ARP and IP services with a single click. Open IP is a Solectek-specific construct that allows the operator, using SkyWay MAX Manager software, to create services that will carry Ethernet ARP, DHCP, IP and (if needed) PPPoE traffic with a single click. The management system creates all of the necessary underlying services for traffic to begin flowing using Best Effort scheduling. The services are given a priority of 0, meaning they are last in the queue to be put on the wireless link.



Open IP provisioning is intended as a convenience for quick commissioning of new subscribers. It's not sufficient, in and of itself, for a high-performance WiMAX network. Rate limiting and prioritization of traffic is not possible when using Administrative Services. To make best use of limited wireless resources, therefore, and to deliver optimal network performance, it's advisable to create user services.

User Services
In contrast to Administrative Services, User Services transport application payload with custom QoS and Reserve Rate parameters. When defining a User Service, it must be assigned an existing service class. Considerations for choosing a class would include the type of network traffic being carried, SLAs, and the specifics of the wireless deployment (such as range, density, frequency re-use). At this time, a relative priority from 4 to 16 (separate from QoS priority, which is a class parameter) is also set. Finally, the service is tied to a classifier to define what types of data will be carried.

User services are defined by the operator on a per-subscriber, per-direction (i.e. uplink or downlink) basis. Each service is assigned a Service Flow ID (SFID). There are two categories of user data services that can be created on the SkyWay MAX system: **Voice, Video, Custom** or **Data Only** services. Voice, Video and Custom services allow for detailed specification of traffic in both the uplink and downlink direction, while Data Only services create a set of uplink and downlink flows for all traffic not otherwise classified.



Data Only Services

Provisioning a subscriber unit with Data Only services provides somewhat more flexibility than offered by Open IP. These services may be assigned any of the service classes available on the system, but only two classifiers are possible, IP gateway (***not*** the subscriber unit itself, but a CPE device, such as a wireless router directly attached to the SS) and VLAN ID. This limits the ability to specify types of traffic or individual endpoints beyond the gateway, and is best used for lower priority traffic: as a "catch-all" for application payload that is not otherwise classified and does not require uplink/downlink asymmetry. The priority of these services is fixed at 3; priority cannot be changed for either Open IP or Data Only services.

Voice, Video, Custom Data Services

This service category offers the most finely grained classification of traffic, with a wide range of 802.3, VLAN and IP parameters available to specify exactly which traffic will be carried on which service to and from which endpoint (a customer PC).

Well-designed classifiers support the optimal performance of the system. However, some level of knowledge of the configuration and capability of individual endpoints (e.g. personal computers, SOHO routers, or other attached network devices) is typically necessary. It's common for operators to manually assign IP addresses to PCs that are connected to subscriber units. If this is done statically, then Source and Destination IP addresses can be used as one of the classifiers. If DHCP will be used to assign IP addresses from a pool, on the other hand, it might be necessary to use the MAC address of the PC's network card as a classifier. Merely using the IP or MAC of the SS unit offers no benefit to the end user traffic.

Using a specific endpoint identifier (IP or MAC address), along with an additional classifier (such as IP protocol) allows particular types of traffic to be differentiated and targeted for prioritization. A service can be created specifically for the traffic type, and assigned to a class of service that has the mix of scheduling and QoS parameters appropriate for those needs. Up to four classifiers may be enabled per service flow.

F. Unicast and Multicast Services

Services can operate in either a unicast or multicast fashion. A unicast service defines a logical connection between the BSU and a single SS. A multicast service defines a connection between the BSU and a defined set of SS units. Multicast services are available in the downlink direction only.

The system has a set of permanent, reusable downlink multicast services that are used to implement Administrative Services:

SFID 3820, 3821: PPPoE
SFID 3822: ARP
SFID 3823: DHCP
SFID 3824: IP

G. Example

An operator is setting up a sector network expected to build out to 50 subscriber units. The service provider is marketing several tiers of service:

Basic Broadband	up to 512 kbps download, 128 kbps upload
Business Broadband	1024 kbps DL, 256 kbps UL
Premium Broadband	1024 kbps DL, 1024 kbps UL
Voice Service	64 kbps DL and UL each line

To implement these SLAs, several custom service classes will need to be set up, for both directions (uplink and downlink) of each plan. Then, the operator will create individual uplink and downlink services for each subscriber, using classification to specify which data will be carried on which service.

Since in this example "Basic Broadband" users will comprise the majority of services on the system, they could be configured with non real-time polling service (nrtPS) scheduling, with relatively fewer Premium and Business Broadband plan subscribers receiving priority real-time polling service (rtPS) flows. An important factor to remember when making these determinations is that real-time polling ensures priority access to the wireless link. If many subscribers are provisioned with such services, the prioritization is effectively defeated. It may be more efficient to use nrtPS scheduling to share bandwidth.

The total available bandwidth will vary depending on the RF conditions of the BSU sector. When the minimum reserved rate (MRR) for a given class of service is set, ensure that the sum of all MRRs on the number of services active at any given time should not exceed the available bandwidth. Otherwise, subscribers may be denied access to the network at peak usage times.

Remember that the parameters set for each class refer to the physical transmission of the bitstream over the wireless link, and do not take into account overhead inherent in higher-layer data protocols. As such, it may be advisable to take that overhead into account when setting Maximum Sustained Rate (MSR) parameters in order to reach targeted data rates.

Using multiple classifiers for a service is best practice. If two or more different services use the same classifiers, the SkyWay MAX convergence sublayer will assign an incoming frame to the first service that matches. No traffic will be assigned to the second.

While SkyWay MAX devices do not add or modify IP header information, the Differentiated Services Code Point (DSCP) field of each IP packet can be read by the BSU, and used to classify traffic. In this way, operators can rely on end-to-end QoS support from the core through the wireless link to the customer's network.

IV. Management Systems

The SkyWay MAX system provides a number of different management methods, suited for different network deployment and management scenarios. With the exception of the SS pre-provisioning process, most normal management functions are processed directly through the BSU.

A. Manager Application

The SkyWay MAX Manager Application is the most straightforward management tool for Solectek's WiMAX equipment. This Manager system is built on a Java platform and is installed and can be operated on a Windows PC.

Once installed and operational, the Manager can be pointed to any Solectek SkyWay MAX device, including BSUs, SS and compatible Indoor Controllers. The software provides full command and control of a device across pre-provisioning, turn-up and operation/maintenance processes.

Since the Manager host PC logs directly into the device being managed, this management tool is best suited for Host PCs with local access within an Operator's private network, and for managing small to medium networks.

Please refer to Solectek document 1556701, *SkyWay MAX Manager User Guide*, for more information on the features and operation of this tool.

B. EMS System

For medium- to large-scale networks, Solectek's EMS software is an ideal management solution. Hosted on a dedicated NOC server residing within an Operator's private network, the system provides multi-site network wide status and control. Please contact Solectek Sales or Technical Support for more information regarding availability of the EMS system.

C. SNMP

Solectek's BSU provides SNMP v2c read only, monitoring functionality through the use of both multiple MIBs: MIB II, 802.16f WIMAX MIB, and Solectek's private MIB.

SNMP functions can be mapped to an Operator's existing SNMP Management system or related NMS/EMS application.

MIBs are posted on Solectek's support portal, along with a helpful guide to relevant OIDs available in the Solectek MIB. Please contact support for portal access and registration info.

D. Telnet

Each network element (BSU, SS) can be accessed and managed through a command line interface (CLI) launched via a Telnet connection. See the *SkyWay MAX Telnet Command List* (Solectek part 1553501) for a detailed reference to the commands available.

Below are a small number of options not currently supported In the SkyWay MAX Manager, requiring use of the Telnet interface.

ssaclulmod and **ssacldlmod**: allows manual configuration of uplink and downlink modulation settings
uptime: elapsed time since last reset of the WiMAX Upper MAC layer software
get ethinfo: Ethernet interface status and counters
get ethcfg: Ethernet port speed/duplex configuration
get gps: GPS synchronization counter

E. Serial Console

Accessed via an accessory serial cable, an RS-232 Serial Console is available for the BSU only. It is recommended that this management connection be used only for bench testing and on-site debug work. Maximum console cable length per RS-232 is 100 feet. The commands available through the Serial Console are the same as those available from Telnet. See the *SkyWay MAX Telnet Command List* (Solectek part 1553501) for a detailed reference to the commands available.

V. RF System

A. Parameters

RSSI / CINR

The instantaneous RF received signal strength (RSSI) and Carrier-to-Interference & Noise Ratio (CINR) metrics are available in both the uplink and downlink direction. Both are important as indicators of the RF link quality. RSSI is an absolute measure, calibrated in dBm. CINR is a ratio, or relative measure, calibrated in dB.

Optimal RSSI & SS Power Control

During the network entry process, in a stage known as *ranging*, the SS must adjust its power so that the signal power received (RSSI) at the BSU equals the *Optimal RSSI*, a threshold stored in the BSU.

If the SS cannot reach the Optimal RSSI value, it may still be allowed on to the network, but can likely only support lower order modulations, that is, lower data rates. A typical window for minimum power received at the BS is ~15dB below the configured optimal RSSI value. Setting an optimal value lower than -78 dBm is generally not recommended.

Modulation

RF modulation, which determines the achievable data rate, is specified on a per-SS and per-direction basis. Each SS has both an uplink and downlink modulation setting. The available modulations and their corresponding forward error correction (FEC) coding rates are as follows:

Modulation	Coding Rate
AUTO	n/a
BPSK	1/2
QPSK	1/2
QPSK	3/4
QAM16	1/2
QAM16	3/4
QAM64	2/3
QAM64	3/4

The Auto Modulation feature provides a self-adjusting modulation dependent on the current RF link conditions, as measured by the CINR and RSSI. This process occurs independently per SS, and per direction. Note that recorded CINR and modulations automatically assigned nay not be fully optimized In the absence of traffic due to low sample rates for the system. Link maintenance has priority in such a case. Auto and Fixed modulation settings can be mixed within an RF network, or even an individual SS.

Multicast Modulation

Each downlink Multicast Service must also be assigned one of the modulation settings shown above. Once selected, the modulation setting applies to all SS units with membership in a particular Multicast Service. Thus the modulation should be

chosen conservatively enough so that all member SS units can remain connected to the service.

As an example, consider a situation where all SS units within a Multicast Service have sufficient link margin to support QAM64-2/3, except one SS which can only support QPSK-3/4. In order to retain service to all SS units, the modulation should be chosen as QPSK-3/4, even though doing so sacrifices system efficiency.

When a Multicast Service modulation is set to Auto, the modulation self-adjusts to the highest data rate that still supports all member SS units. The modulation selection is based upon the CINR and RSSI values of all member SS units. No uplink Multicast services are possible.

B. Multi Sector and Multi Site Operation

The need to sectorize a base site occurs as network subscription outstrips the capacity of a single BSU (sector). In this case, additional BSU sectors can be added to a base site. For Solectek's SkyWay MAX system, this also requires the provisioning of an Indoor Controller.

The Indoor Controller is a configurable and scalable system providing a number of functions to a multi-sector base site:

- Power + Data transport
- GPS Synchronization
- Remote Management (optional)
- BSU Failover Switching (optional)

More information on the commissioning and operation of the Indoor Controller can be found in *the Indoor Base Station Controller Installation and Operation Guide,* Solectek document 1524603.

Issues that must be taken into consideration when setting up multiple sectoral bases fall into two general areas: Radio Frequency and Authentication.

Radio Frequency
The Indoor Controller makes use of a GPS based synchronization pulse to align the transmit and receive time slots on all BSUs and SS units in all sectors. With synchronization, the different BSUs will await bursts from their SS units at the same time: if this synchronization is not present, some BSUs may transmit during this interval and potentially interfere with the relatively weaker signal coming from the remote SS units. In order for synchronization to function properly, RF frame length must be set uniformly across all BSUs.
Finally, channel selection is key to minimize the potential for interference between sectors. Especially when four or six BSUs share the same tower, care should be exercised that there be as much channel spacing as possible between two adjacent sectors. If there is adequate spectrum available, channel centers may be chosen so that there is a guard band between channels, and custom channel plans loaded on each BSU and SS. Details on creating custom channel plans can be found in the Appendix.

Authentication
In situations where SS units are in the signal range of multiple BSUs, the security features on the SkyWay MAX system should be configured to ensure that a particular SS unit will connect only to a particular BSU, and no other. Depending on the specific needs and challenges of a given network, authentication may be enabled on the SS or on the BSU.

On the SS side, BSID Verification can be used so that the SS unit will not attempt connection with any BSU other than the one it is configured for. The BSU has an ACL mode that can be enabled so that only specified SS units will be allowed to connect. In networks where SS units are not individually configured for use in a specific sector, it may be necessary to use ACL mode exclusively to ensure that the SS unit connects to the correct BSU. When possible, however, it's advisable to enable BSID Verification on the SS unit. Further, use of a custom channel plan (see Appendix) will prevent the SS unit from scanning to other channels, and will allow for the connection to complete more quickly.

VI. Administration

A. Notifications

BSU Notifications use SNMP traps to actively alert an Operator's management system (Manager Application, EMS or SNMP Manager) of important changes in system status, including:

- BSU reboot/restart
- SS exit or entrance to network
- Service add / delete / modification

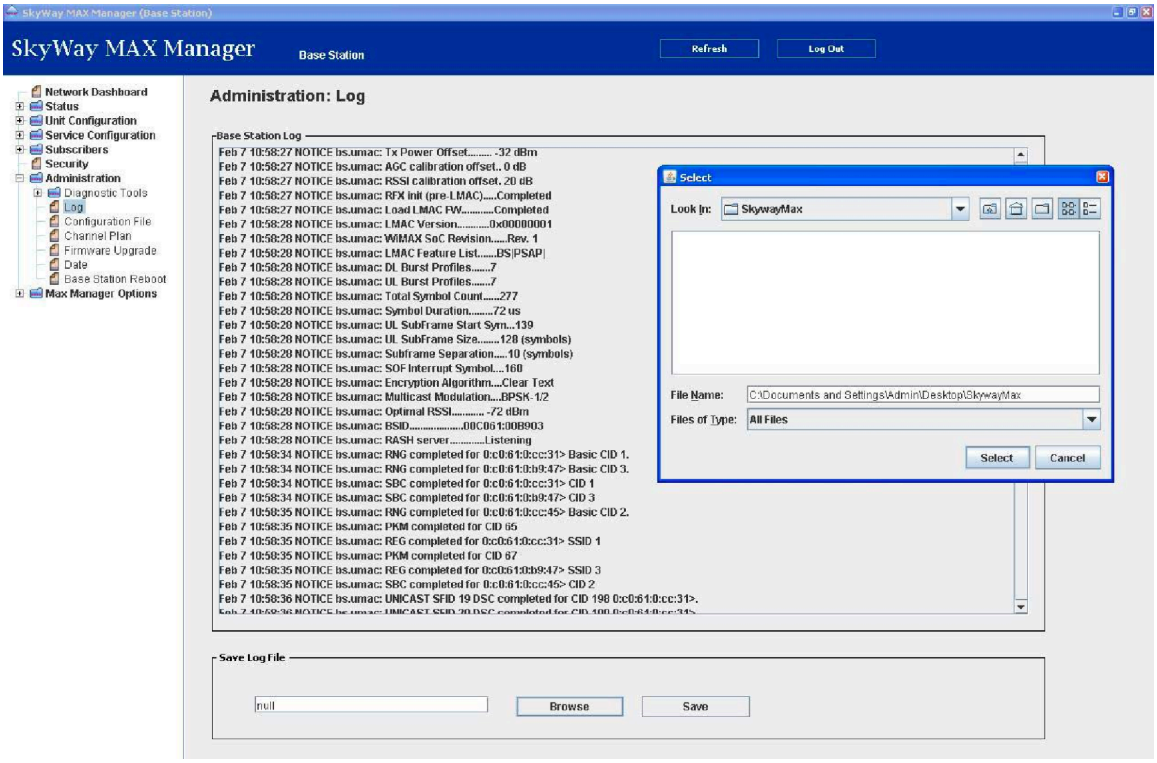
On the Manager Application, Notifications can be viewed under **Status : Notifications**, or by using the quick-link from the Dashboard.

Once viewed, Notifications can be erased or retained for future reference.

B. Event Logs

The SkyWay MAX BSU and SS devices automatically create and store a local event log file. This log is used to capture and timestamp detailed information regarding all system configuration and status events.

A device log file can be viewed using either the Manager Application, Telnet interface or EMS System, and/or exported to a local PC for further analysis via FTP. This export process is depicted in the following screen from the Manager Application:



Log info can also be viewed dynamically for both the BS and SS from the telnet interface using the show log command. Additional usage options are available by typing show log followed by a question mark (?).

C. Configuration Files

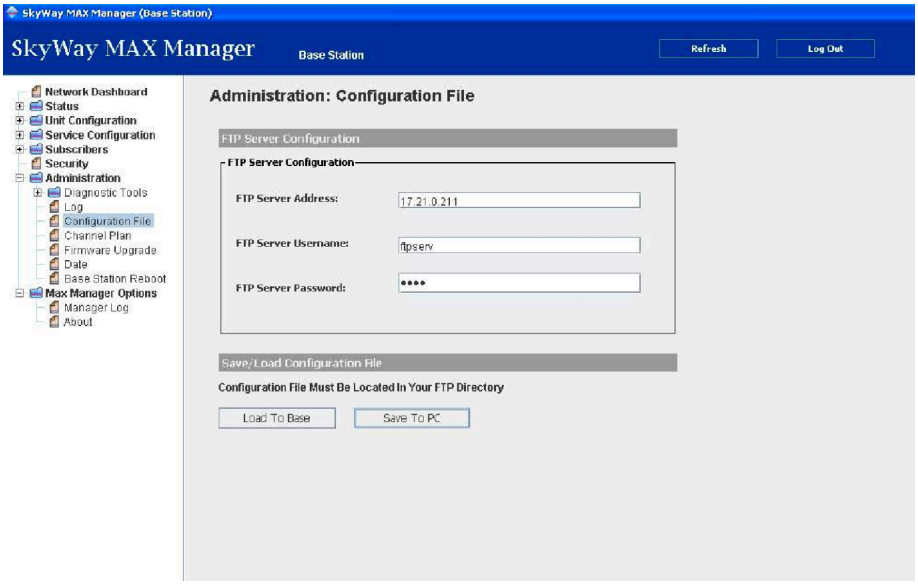
In addition to using one of the many management systems available (e.g. Manager Application, EMS, SNMP, Telnet), the device configuration can be managed through the import and export of an XML formatted configuration file.

Storing an operational BSU configuration off-line has several benefits:

- Reduces provisioning time and increases flexibility of sparing strategies with a BSU
- Provides a 'known-good' starting point when debugging system problems
- Becomes a template for adding new BSU sectors

For the SS, an off-line configuration file can act as a 'golden file' used to pre-configure each SS unit prior to deployment.

The import and export of a configuration file is accomplished using FTP. The applicable Manager Application screen is shown here:



Configuration files can be exported and archived using any descriptive filename with a .xml extension.
Restoring a configuration file from to the BS from backup requires using the specific file name of WimaxCfg.xml

D. Firmware upgrade

The firmware files for WiMAX Base Station Units and Subscriber Stations are released in a single distribution, which is available for registered system owners on Solectek support site at http://solectek.com/support. The distribution consists of the two packages for base and subscriber units, along with a utility program that can organize the files correctly on an FTP server.

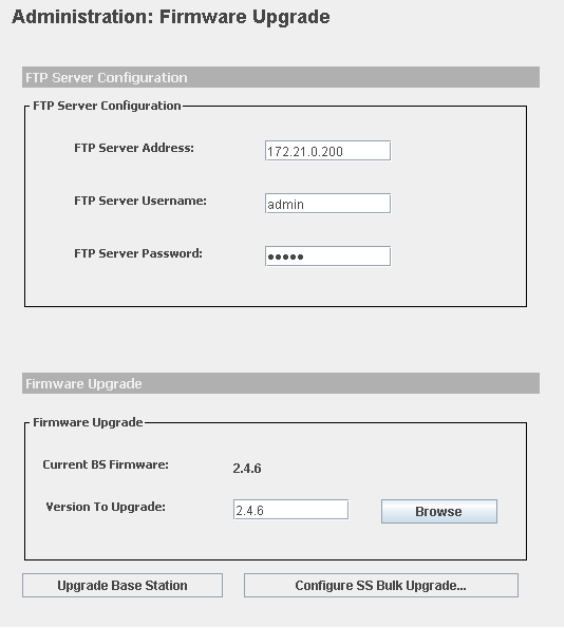
Note: make sure that the FTP server and the PC running SkyWay MAX Manager are on the same IP subnet as the BSU, and that the port for FTP (tcp/21) is not blocked between any of these systems.

The current version of firmware can be downloaded from the support site as a compressed zipfile. Decompress this file on the FTP server, and use the SetupFirmware.exe utility to specify the FTP root directory. If that directory does not contain a pub subdirectory, one will be created, and the firmware packages extracted to their proper subdirectories. The organization shown below is necessary for the upgrade process to operate correctly.

- <ftp root directory>
  - pub
    - bs
      - dists
        - <specific version>
          - images
    - ss
      - dists
        - <specific version>
          - images

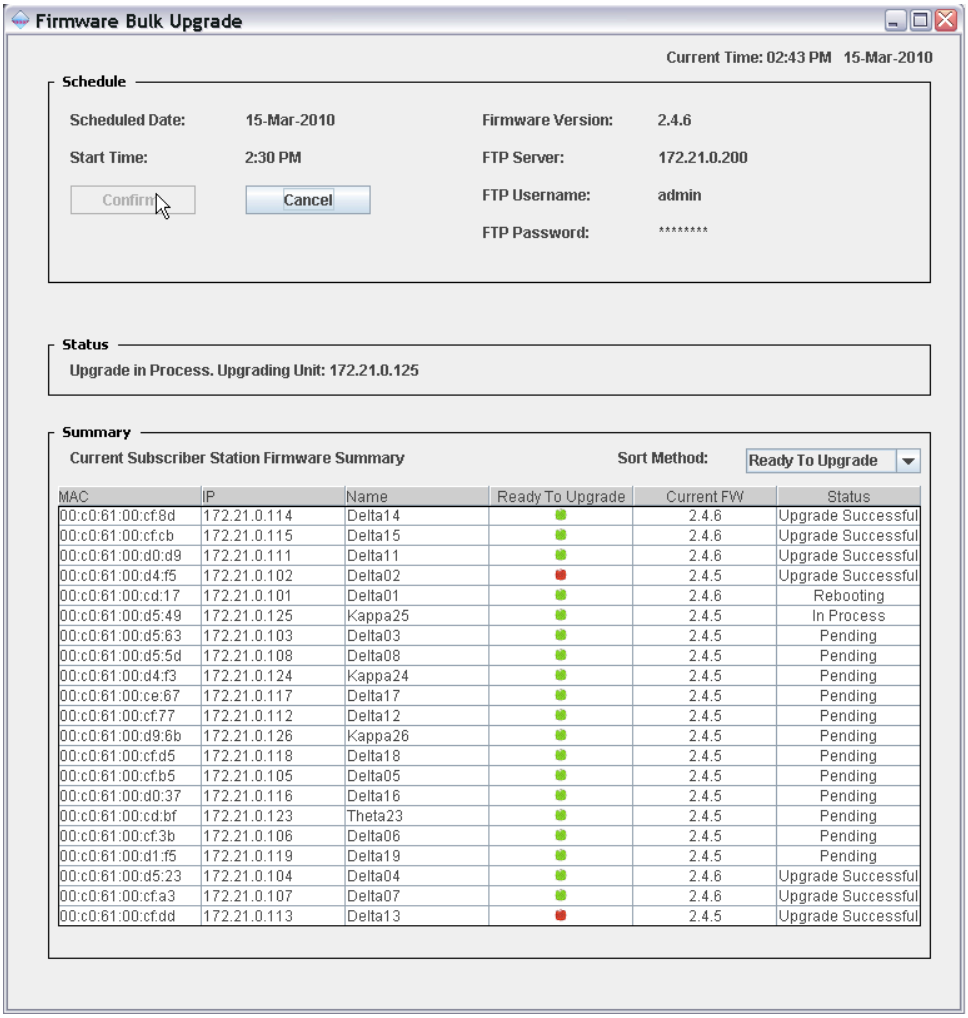
Using the Manager Application, devices may be upgraded individually, or all devices on a production network can be upgraded at once using the Bulk Upgrade function, provided that service flows are provisioned allowing IP traffic to flow **to and from the subscriber unit itself**.

To use the Manager Application to upgrade the BSU, navigate to **Administration: Firmware Upgrade** and confirm the FTP server address and login information. Then, click the Browse button to select the version of firmware you wish to upgrade to.



If the BSU alone is to be upgraded, click the *Upgrade Base Station* button and the process will begin. If all devices in the sector are to be upgraded, click the *Configure SS Bulk Upgrade* button and a new window will open.

In the Firmware Bulk Upgrade window, set the day and time that the upgrade process will begin. The configured BSU system time will be used for scheduling; current time appears in the upper-right corner of the window. To initiate the process, click the Confirm button.



The Manager Application will poll all of the SS units on the system and report their status under *Current Subscriber Station Firmware Summary*. SS units that are responding to the poll and have older versions of firmware will be shown as *Ready To Upgrade*. When the upgrade is scheduled, the status will change to *Pending*, and will show *In Process* when the upgrade begins. When the process completes, the individual subscribers will be shown with *Upgrade Successful* as their status, and a message will appear detailing which, in any, subscribers did not successfully update. The process can be restarted for those subscribers.

In the final step of the process, the BSU itself will be upgraded, and the communication between the Manager Application and the BSU will be interrupted when the BSU reboots. The Manager Application will temporarily indicate an error, which will clear when communications are restored. The system will display a log of the details of the upgrade process, which can be saved on the host PC.

Alone, a single SS can be upgraded by connecting it to a PC running an FTP server. Navigate to the Management: Firmware Upgrade section and input the desired firmware version number.

E. Date/Time

In each wireless sector, the BSU is responsible for maintaining the local time and date. Once configured, this information is stored in a battery-backed BSU real-time hardware clock.

During network entry, this date/time is passed to the SS. The SS has no internal clock, taking all time information from the BS directly. In all cases, the local time zone should also be configured in the BSU after time and date are set manually, to allow accurate conversions from UTC time.

F. Name/Location

To improve usability and record keeping an Operator can choose to assign names and locations to the BSU and SS units. This information can be assigned during initial provisioning, or anytime thereafter. Information for both the BSU *and* SS is stored on the BSU.

Location information is stored as GPS coordinates in the following format:

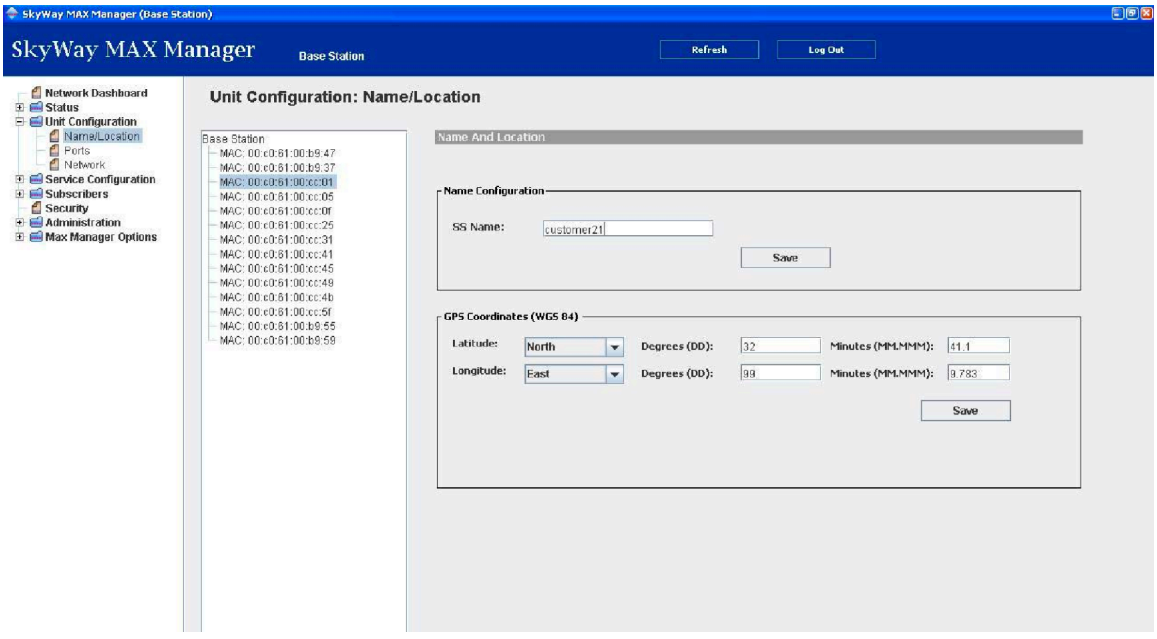
- Datum: WGS 84
- Lat/Long HDDD MM.MMM, where:
  H=Hemisphere (N or S for Lat, E or W for Long)
  DDD=Degrees, including leading zeros as necessary
  MM.MMM = Minutes in decimal format

In addition, information on the BSU antenna beamwidth and bearing can be captured.

In total, the following fields are available:

- BSU
- Name
- Location
- Antenna Bearing
- Antenna Beamwidth
- SS
- Name
- Location

Access to this information set on the Manager Application is via **Unit Configuration: Name/Location**



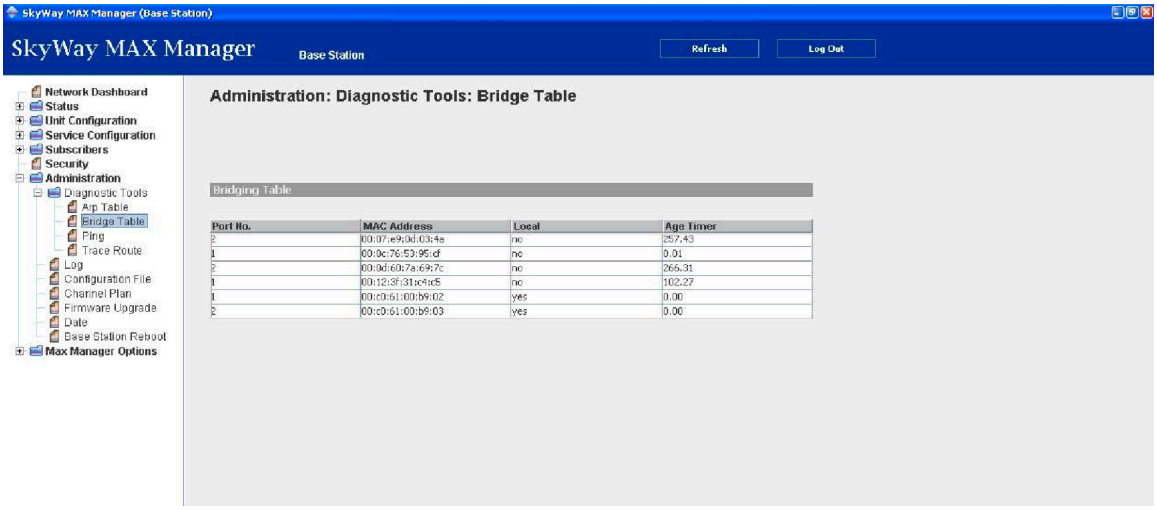
G. Diagnostic Tools

The BSU contains a number of embedded network tools to assist with the debug and verification of network operation.

These tools include:

- Ping
- Traceroute
- ARP Table
- Bridge Table

Usage and syntax of these tools is similar to those of standard networking appliances. Access to these tools on the Manager Application is via **Administration : Diagnostic Tools**.



Appendix A – System Defaults

A. Default Configuration

BSU	
Login	admin
Password	admin
IP Address	192.168.0.2
Netmask	255.255.255.0
Default Gateway	192.168.0.10
FTP Address	<blank>
FTP User	<blank>
FTP Password	<blank>
RF Channel Plan	default.cc
RF Power	33 dBm
Optimal RSSI	-70 dBm
Uplink Modulation	Auto
Downlink Modulation	Auto
BSID	00000B:xxxxxx (where x is last 3 octets of RF MAC)
Security	
X.509 Certificates	Disabled
Access Control List	Disabled
Administrative Services	None
User Services	None
Name	<blank>
Location	<blank>
GPS Coordinates	<blank>
Antenna Bearing	<blank>
Antenna Beamwidth	<blank>

SS	
Login	admin
Password	admin
IP Address	192.168.0.1
Netmask	255.255.255.0
Default Gateway	192.168.0.10
FTP Address	<blank>
FTP User	<blank>
FTP Password	<blank>
BSID Verification	Disabled
BSID table	<none>
RF Channel Plan	default.cc
SS Name	<blank>
SS Location	<blank>
GPS Coordinates	<blank>

B. Default Channel Plan File (3.4 – 3.7 GHz operation)

For coverage of the 3.4-3.7 GHz frequency range, the SkyWay MAX system uses a default channel plan which is a subset of the CEPT/ERC/REC 14-03E channel plan.

Operators may use the default channel plan file, as-is, or may use it as template to create custom .cc files. These files can be uploaded to the same directory in the BSU and SS and activated in the system through the management system.

Filename: default.cc
Path: /etc/umac/cc.d

```
#/etc/umac/cc.d/default.cc----------------------------------
#
# Contains default channel centers for 3.4-3.6 GHz operation
#
# Valid Entries are:
#
# name CHANNEL_PLAN_NAME
#   CHANNEL_PLAN_NAME is a string for name of the plan
#
# abbrev ABBREVIATION
#   ABREVIATION of plan up to 4 symbols
#
# channel FREQ  BW
#   FREQ - channel frequency in kHz
```

```
#   BW   - channel bandwidth in kHz
#
# Refr: SkyWay_MAX_Default_Channel_Plan_DOCS-1030_v1.4.xls
#-------------------------------------------------------
#
# This section is for common channel plan properties
#
name            Default
abbrev          DFLT
cyclic_prefix   32
#-------------------------------------------------------
# Channels are listed below this line.
#----------- Freq ----- BW --------------------------------
#
# For products ODB-3436 & ODS-3437
#
channel     3413500    7000
channel     3420500    7000
channel     3427500    7000
channel     3434500    7000
channel     3441500    7000
channel     3463500    7000
channel     3470500    7000
channel     3477500    7000
channel     3484500    7000
channel     3491500    7000
channel     3503500    7000
channel     3510500    7000
channel     3517500    7000
channel     3524500    7000
channel     3531500    7000
channel     3538500    7000
channel     3545500    7000
channel     3553500    7000
channel     3560500    7000
channel     3567500    7000
channel     3574500    7000
channel     3581500    7000
channel     3588500    7000
channel     3595500    7000
#
# For products ODB-3537 & ODS-3437
#
channel     3653750    7000
channel     3657250    7000
channel     3660750    7000
channel     3664250    7000
channel     3667750    7000
channel     3671250    7000
channel     3674750    7000
#end
```

Note that SS units are universal for domestic US operation at 3.65GHz and internationally at 3.4-3.6GHz. The default channel plan file will allow any SS to scan the full list above. Base Station units are factory configured as either ODB-3436 or ODB-3537, and can be configured to operate only in frequencies allowed for each type. Domestic operators can safely remove or comment out the frequencies listed in blue color above when creating a custom channel plan file. Channel bandwidth of 3.50MHz are supported, but not included in the default channel plan file.

C. Sample Custom Channel Plan File (3.650 – 3.675 GHz operation)

```
#/etc/umac/cc.d/New365.cc---------------------------------
#
# Contains default channel centers for 3.65 GHz operation
#
# Valid Entries are:
#
# name CHANNEL_PLAN_NAME
#   CHANNEL_PLAN_NAME is a string for name of the plan
#
# abbrev ABBREVIATION
#   ABREVIATION of plan up to 4 symbols
#
# channel FREQ  BW
#   FREQ - channel frequency in kHz
#   BW   - channel bandwidth in kHz
#
# Refr: SkyWay_MAX_Default_Channel_Plan_DOCS-1030_v1.4.xls
#-----------------------------------------------------------
#
# This section is for common channel plan properties
#
name            New365
abbrev          N365
cyclic_prefix   32
#-----------------------------------------------------------
# Channels are listed below this line.
#----------- Freq ----- BW --------------------------------
#
#
# For products ODB-3537 & ODS-3437
#
channel     3653750    7000
channel     3657250    7000
channel     3660750    7000
channel     3664250    7000
channel     3667750    7000
channel     3671250    7000
channel     3674750    7000
#
#
channel     3653750    3500
channel     3657250    3500
channel     3660750    3500
channel     3664250    3500
channel     3667750    3500
channel     3671250    3500
channel     3674750    3500
#end
```

The New365 channel plan file above shows the removal of International Frequencies and the addition of 3.50MHz wide channels using the same channel centers as the default 7.0MHz channels. Other channel centers may be used, as long as increments of 250KHz are retained; i.e. 3671400KHz is an invalid center.

Appendix B - SkyWay MAX Manager

- Network Dashboard
- Status
  - RF Port
  - Ethernet Port
  - Network
  - Services
  - Notifications
- Unit Configuration
  - Name/Location
  - Ports
  - Network
- Service Configuration
  - Service Classes
    - Add
    - Modify/Delete
- Services
  - Add
  - Delete
  - Modify
- Subscribers
  - Add
  - Delete
  - Modify
- Security
- Administration
  - Diagnostic Tools
    - ARP Table
    - Bridge Table
    - Ping
    - Trace Route
  - Log
  - Configuration File
  - Channel Plan
  - Firmware Upgrade
  - Date
  - Base Station Reboot
- Max Manager Options
  - Manager Log
  - About

Appendix C Services Reference

A. Available Classifiers

The following Classifier Types are supported on the SkyWay MAX system

802.3
Source MAC Address
Destination MAC Address
Ethertype

802.1p/q
VLAN ID
VLAN Priority Range - 802.1p (values 0-7)

IPv4
Protocol + Source/Destination Port Range
Source Address, with bit mask
Destination Address, with bit mask
ToS Value, with bit mask

B. QoS Scheduling Parameters

Available Parameters, by Scheduling Type

Scheduling Type	Supported Parameters
UGS	Maximum Sustained Traffic Rate Tolerated Jitter Maximum Latency
rtPS	Maximum Sustained Traffic Rate Minimum Reserved Traffic Rate Maximum Latency
nrtPS	Maximum Sustained Traffic Rate Minimum Reserved Traffic Rate Traffic Priority
BE	Maximum Sustained Traffic Rate Traffic Priority

Parameter Definitions

Parameter	Description	Default value
1. Grant Size:	The size of each UGS grant in bytes.	--
2. Grant Interval	The period between UGS grants, or rtPS polls, in mS	20
3. Max Sustained Traffic Rate	Upper limit, or ceiling, of traffic rate, in bits/second A setting of zero means unlimited.	0
4. Min Reserved Traffic Rate	Lower limit of traffic rate reserved per Service, in bits/sec	250
5. Max Latency	Upper latency limit per Service, in mS. Only applies when actual traffic rate is < Min Reserved Rate (ie - the Service is not overloading the reservation)	1200
6. Traffic Priority		
Defines priority when packet matches classification on multiple Services. Range is 0-16, 16 is the highest priority.		

0	Administrative and Open IP Services
7	User Services