WAVETEQ SHADOWMINI

User Manual

Revision 2.4
2008-07-17

222-3121 Hill Road, Lake Country, BC V4V1G1, Canada
US & Can: 1-888-928-3837 International +11-250-766-9229
Fax: 250-766-9221 www.waveteq.com

FCC Compliance

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

The user should not modify or change this device without written approval from Waveteq Communications Inc. Modification will void the warranty and authority to use the device. For safety reasons, people should not work in a situation where RF exposure limits could be exceeded. To prevent this situation, the user should avoid installing or using the antenna closer than 100 cm (39 in) from people.

Industry Canada Compliance

This Class B digital device complies with Canadian ICES-003. Operation of this device is subject to the following two conditions:

1. This device may not cause interference

2. This device must accept any interference, including interference that may cause undesired operation of the device.

The frequency band 5150-5250 MHz (channels 34-40) is only for indoor usage to reduce potential for harmful interference to co-channel mobile satellite systems. Users should also take note that high-power radars are allocated as primary users, which means that they have priority in the bands 5250-5350 MHz (channels 52-64) and 5650-5850 MHz (channels 132-165). These radars could cause interference to the Waveteq ShadowMini.

Copyright

Notice

Waveteq Communications Inc. reserves the right to change specifications without prior notice.

While the information in this guide has been compiled with great care, it may not be deemed as an assurance of product characteristics. Waveteq Communications Inc shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Waveteq Communications Inc.

Trademarks

The Waveteq logo, ShadowMini and ShadowMaster are trademarks of Waveteq Communications Inc.

All other registered and unregistered trademarks in this document are the sole property of their respective owners.

National Radio Regulations

The usage of wireless network components is subject to national and or regional regulations and laws. Administrator must ensure that they select the correct radio settings according to their regulatory domain. Please check the regulations valid for your country and set the parameters concerning frequency, channel, and output power to the permitted values!

Table of Contents

List of Tables

List of Figures

Purpose

The Waveteq ShadowMini Customer Premise Equipment (CPE) is a standards based customer device constructed specifically for rugged outdoor use and allows for the most flexible installations in the marketplace. This document provides information and procedures on setup, configuration, and management of the Waveteq ShadowMini outdoor client station. The focus of the following text is to describe how to install and use the Waveteq ShadowMini device.

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

ℹ	Additional information that may be helpful but which is not required.
❗	Important information that should be observed.
bold	Menu commands, buttons, input fields, links, and configuration keys are displayed in bold
italic	References to sections inside the document are displayed in italic.
code	File names, directory names, form names, system-generated output, and user typed entries are displayed in constant-width type
<value>	Placeholder for certain values, e.g. user inputs that must be replaced with real values.
[value]	Input field format, limitations, and/or restrictions.

Help Us to Improve this Document!

If you should encounter mistakes in this document or want to provide comments to improve the user's guide please send e-mail directly to support@Waveteq.com.

Waveteq Technical Support

If you encounter problems when installing or using this product, please contact support@Waveteq.com or by telephone at 1-888- 928-3837.

1.0 Introduction

Your Waveteq ShadowMini CPE has been designed to be the most flexible outdoor client station in the market. The unique flange and groove system allows easy mounting in a variety of situations. An integrated high gain antenna decreases installation costs and increases performance.

1.1. Inventory

The following items have been included with your Waveteq ShadowMini.

- ShadowMini CPE Package
- Passive Power Over Ethernet injector
- Wall mount adapter
- Field attachable IP67 Ethernet plug
- 2 U-bolts
- 4 nuts
- 4 washers
- 4 lock washers
- Waveteq ShadowMini Quick Start Guide
- Installation Worksheet
- CD

1.2. Feature List

Table 1 – Feature List

Wireless	Network
Access Point and Client Mode	Transparent Bridging
Client Mode	DHCP Client
Extended Frequency Set	DHCP Server
Hide SSID	DNS Masquerading
Transmit Power Control	NAT Server
ACK Timing Adjustment	Static Routing
RTS Threshold Adjustment	Ethernet or Wireless as WAN
Fragmentation Threshold Adjustment	Upstream Bandwidth Throttling
Transmit Rate Control	Remote Status Logging
Country Code Selection	Firewall
Antenna Port Selection	Port Forwarding
802.11a/b/g Operation	Spanning Tree Protocol
Wireless Distribution System Support	
Security	**Operation**
TLS Certificates	Web Management – Local and Remote
802.1x Radius Client Support	Secure Shell Management
WPA(2)-PSK	Statistical Graphing
WPA(2)-Enterprise	Throughput Test Utility
WEP	Ping Utility
Access Control Lists	Packet Sniffing Utility
802.1e Prioritization	Field Upgradeable Firmware
Emergency IP Address	Antenna Alignment Utility

2.0 Installation

The Waveteq ShadowMini can be installed in a variety of configurations, to act as an Access Point (AP) or a client CPE.

2.1. Mounting

The ShadowMini should be mounted in a manner so that its antenna has line of sight to its target. In the 2.4 GHz and 5.8 GHz ISM bands, very little penetration is possible through obstructions such as buildings or trees, but in some cases may be possible. The ShadowMini has been designed to allow simple pole mounting in two configurations. It can be mounted to any pipe or pole with diameters ranging from 1.0 to 3.0 inches. There are teeth built into the enclosure to allow low slippage mounting in either the horizontal or vertical polarization configurations.

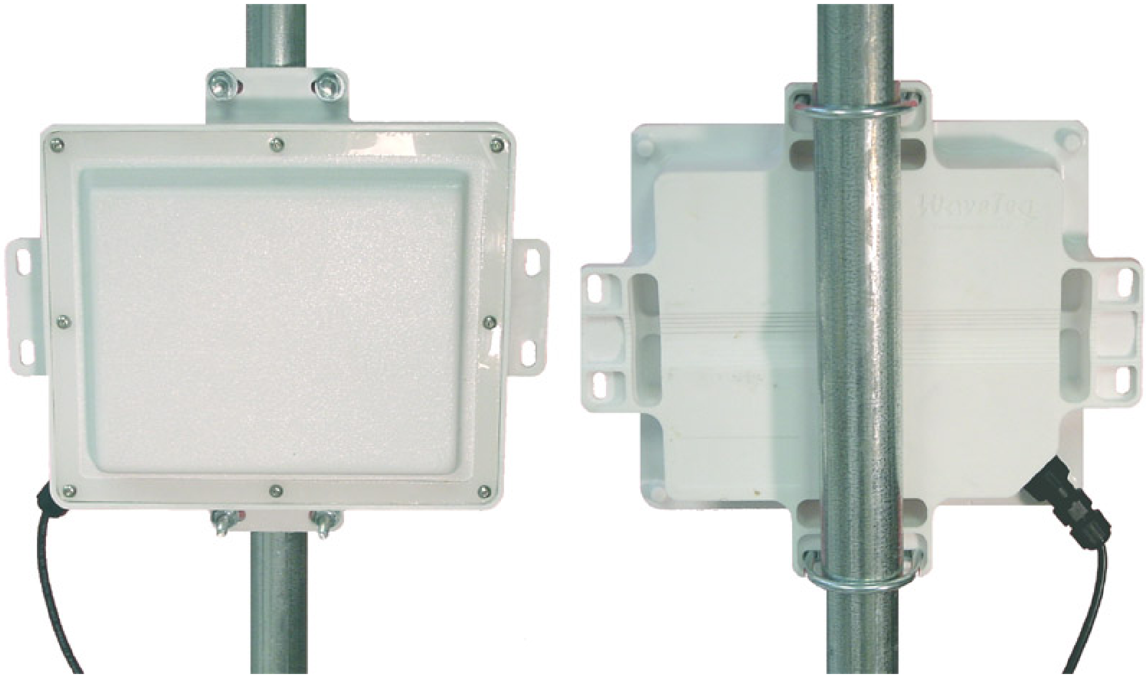


Figure 1 – Vertical Polarized Mounting

For vertical polarization (Figure 1), the Ethernet port should be on the bottom left side of the ShadowMini when viewing from the front (looking at radome). For horizontal polarization (Figure 2), the Ethernet will appear on the bottom right side. A DBS satellite mount is an ideal pole mount structure and can mount to sloped and flat surfaces. The u-bolts should be inserted from the back of the unit, and then the washer, lock washer and nut should be tightened onto the flat flange surface until the unit is secure.

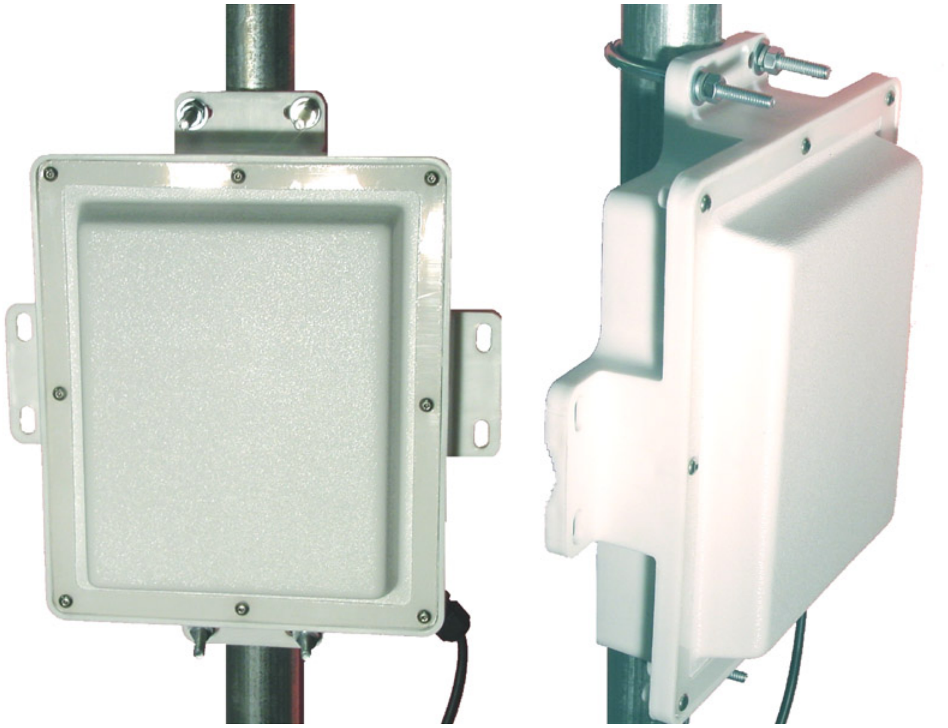


Figure 2 – Horizontal Polarized Mounting

In addition to pole mounting, the flanges can also be used to mount directly to a wall or other flat surface.

2.2. Ethernet Cable and Connector Assembly

The field attachable connecters are IP–67 Rated for ingress of water and dust when properly mated with an Ethernet cable. The steps below show how to create a custom length cable with the field attachable connector. Once this cable is complete, it can be connected to the Waveteq ShadowMini. Please follow the steps below to install the connector to your cable.

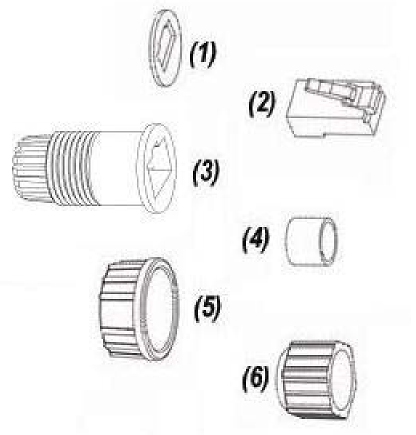


Figure 3 – Connector Parts

Step 1) Start with an outdoor rated Ethernet cable that is of sufficient length to reach the installation of the Waveteq ShadowMini. Allow several extra feet in case of future movement. The cable should not exceed 100m (328ft).

Step 2) Carefully strip off approximately 1.5” of the cable shielding using a small knife or crimping tool.

Step 3) Fan the wires of the cable, untwisting them until they are at the shielding that has been removed.

Step 4) Starting with (6) in, slide each of (6), (5), (4), (3), and (1) over the cable sheath from the end with the exposed wire, as in Figure 4.

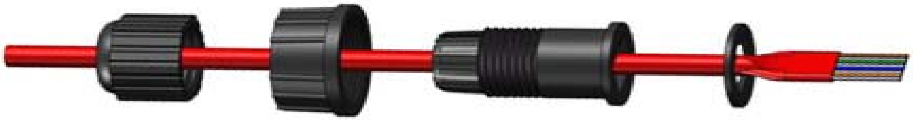


Figure 4 – Connector Parts Exploded View

Step 5) Slide the wires in the proper order into RJ-45 terminator (2) that was included with the connector. Take care to maintain the proper colour code. If the other end of your cable has already been terminated, ensure that you are using the same wire sequence. The two most popular Ethernet wiring standards are shown in Figure 5.

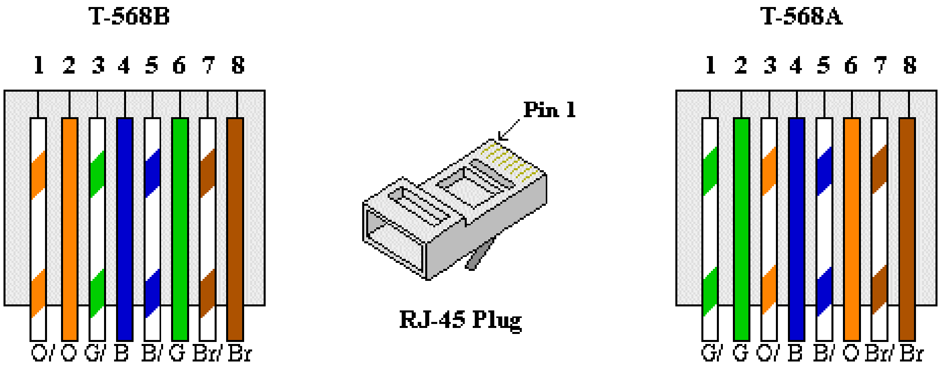


Figure 5 – Ethernet Wiring Colour Standards

Step 6) Ensure that the order of the wires is correct with respect to the wire code you are using.

Step 7) Push the wire bundle into the back of the RJ-45 terminator (2). Pay particular attention to the orientation of the RJ-45 housing to ensure that the wires are not going in backwards. Continue pushing until the wire bundle bottoms out on the housing and visually inspect to ensure all wires are seated onto the back wall of the housing.

Step 8) Using a RJ-45 hand crimper, crimp the assembly together.

Step 9) Move the coupler (5) over the plug holder (3) until it bottoms out.

Step 10) Seat the thick ring (4) inside the cable clinch (3)

Step 11) Slide the RJ-45 terminator plug back into the plug holder (3) until it can go no farther. Take care to push the RJ-45 clip down and seat it into the notch on the plug holder.

Step 12) While pulling the Ethernet cable slightly away from the plug assembly, mate the end cap (6) with the cable clinch (3) by threading in a clockwise direction until tight, as in Figure 6. This will cause the cable clinch to tighten around the cable, providing a waterproof seal. A small wrench may be used to further tighten.

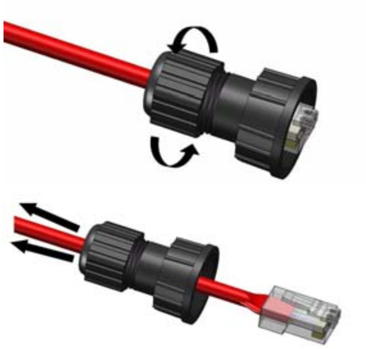


Figure 6 – Tightening the End Cap

2.3. Connecting the Waveteq ShadowMini

To power the Waveteq ShadowMini, you will require a PoE injector, an AC adapter, and the Ethernet cable created according to the procedure in Section 2.2 “Ethernet Cable and Connector Assembly”. Note that none of these devices are waterproof and it is STRONLY RECOMMENDED that they be installed in a watertight, enclosed space. To power the ShadowMini it is necessary to connect your Ethernet cable directly from the power port of the PoE Injector to the RJ-45 port of the ShadowMini. **DO NOT** instead plug the cable from the “PoE” port into your computer or routing device; it will short circuit the components! Next plug the AC adapter into the wall and the DC jack into the PoE Injector.

Connect the ShadowMini to a computer using a cross over cable connecting it to the LAN port of the POE and to the Ethernet port of a computer. If connecting to a switch, hub or router the crossover cable will need to be replaced by a regular, straight-thru Ethernet cable. Power to the ShadowMini unit is indicated by a link light on the Ethernet port of the computer, hub or modem that it is connected to.

2.4. Logging in to your Waveteq ShadowMini

Before logging in, the computer must be on the same subnet as the ShadowMini. By default, the ShadowMini's IP address is 192.168.10.1 with a netmask of 255.255.255.0. You may either manually set the computer IP to another address on this subnet (ie 192.168.10.x), or setup DHCP and let the ShadowMini dynamically assign the computer a valid IP. The DHCP server is on by default.

There are two methods provided to log into the Waveteq ShadowMini and both use the provided Ethernet connection. First, you can log in using a standard WEB browser and interact with your ShadowMini CPE device using a browser WEB GUI. The second method provides access through a secure shell (SSH) client, for example PuTTY, which is included on the CD.

2.5. Logging in via SSH

Several options are available when logged in via a secure shell, and this is the only place where passwords for the users can be changed.

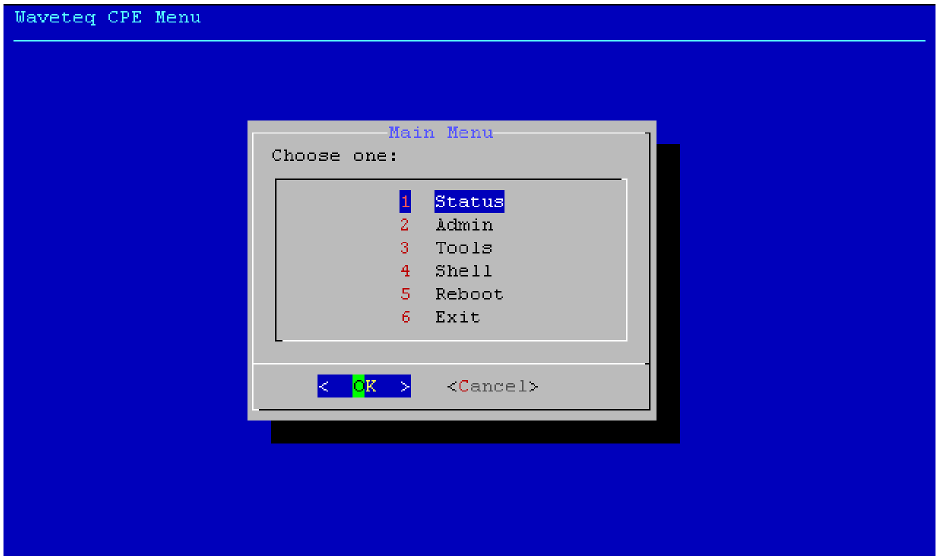


Figure 7 – SSH Menu

2.5.1. Status

Displays output ShadowMini status including network info, firewall info and CPU statistics

2.5.2. Admin

Allows the changing of passwords for the admin and user accounts. To change passwords the user must be logged in as admin. This is also where the ShadowMini can be restored to default settings.

2.5.3. Tools

Several troubleshooting options include TCPDump window for packet sniffing, a ping test and the ability to view all configuration files.

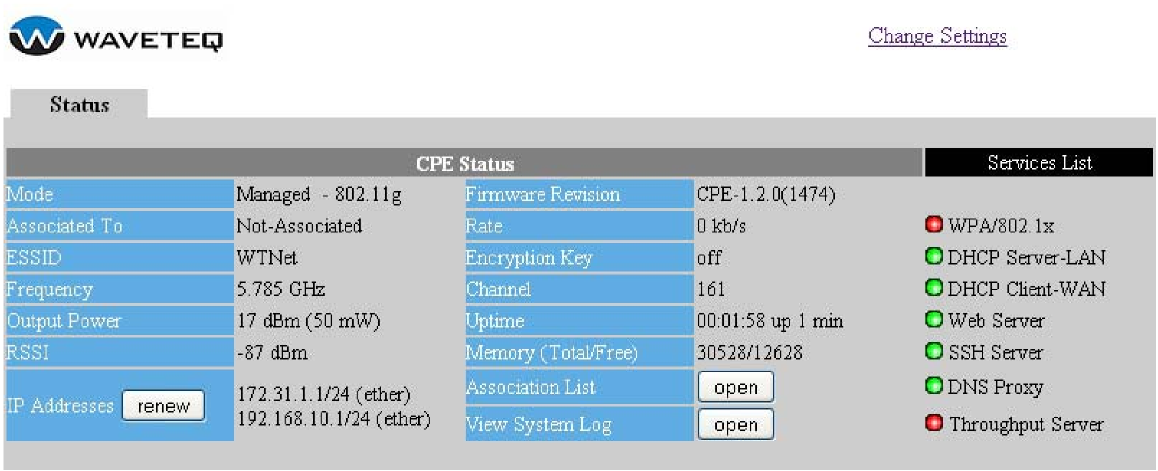
2.5.4. Shell

Accesses a Linux shell for advanced troubleshooting.

2.6. Logging in through the Web Interface

As mentioned above, in order to use the WEB Browser interface you must have a computer IP address on the same subnet (i.e. 192.168.10.x) but not the same address as your Waveteq ShadowMini. You can verify your computer address by opening a Command Prompt and typing "ipconfig" from the command line. Your "IP address" should look something like "192.168.10.100" with a "Subnet Mask" of "255.255.255.0".

Once you have verified this information you may point your browser to http://192.168.10.1.
By default, before you have logged in and become authenticated; you will be greeted by a status screen displaying most of the information available to logged-in users, but not allowing access to functions which can change the operation. This allows non authenticated users to check the status of the ShadowMini and renew IP addresses.



Change Settings

Status

CPE Status				Services List
Mode	Managed - 802.11g	Firmware Revision	CPE-1.2.0(1474)	
Associated To	Not-Associated	Rate	0 kb/s	🔴 WPA/802.1x
ESSID	WTNet	Encryption Key	off	🟢 DHCP Server-LAN
Frequency	5.785 GHz	Channel	161	🟢 DHCP Client-WAN
Output Power	17 dBm (50 mW)	Uptime	00:01:58 up 1 min	🟢 Web Server
RSSI	-87 dBm	Memory (Total/Free)	30528/12628	🟢 SSH Server
IP Addresses renew	172.31.1.1/24 (ether) 192.168.10.1/24 (ether)	Association List	open	🟢 DNS Proxy
		View System Log	open	🔴 Throughput Server

Figure 8 - Non-Authenticated Status Page

To login, click the **Change Settings** link on the top right of this page. You will be prompted for a username and a password.

2.6.1. Default Passwords

The Waveteq ShadowMini has been designed for 2 users, with different levels of access. The admin user has full access to all advanced and basic settings, while the user account is limited only to the basic settings.

Table 2 – Default Passwords

Username	Default Password	Web Access	SSH Access
admin	NOroot4u	Full	Full
user	waveCPE	Simplified	None

2.6.2. Saving and Activating Changes

After any settings are changed, the save button must be pressed before a reboot or navigation to another page. If the save button is not pressed, the settings will not be saved to permanent memory.

After settings have been changed and verified, it is important to click on the “Save” button. Only changes that have been **saved** will be permanently stored in memory.

When saving settings, the ShadowMini will test the user inputted values for validity, and will not allow saving if invalid choices have been made. In this case, any invalid values will be highlighted in red, and a range of valid values will be displayed. To re-enter, press the back browser button and change the highlighted values before resaving. The ShadowMini will require a reboot for the settings to take effect.

2.6.3. Emergency IP

In case of a configuration error or forgetfulness, it is quite common for the IP address to become un-usable. In most cases this is due to the user believing that the IP address is different than what has been configured. Most manufacturers require the unit to be sent back in this case, or a risky hardware reset functionality. We have provided a permanent IP address on the Ethernet interface that can never be deleted or changed; to solve this problem. One caveat is that the subnet used for the emergency IP can never be used in the same collision domain (LAN) with the ShadowMini.

The emergency IP is 172.31.1.1. The computer IP address must be set manually to the 172.31.1.x (255.255.255.0) subnet before attempting a connection.

3.0 Wireless Settings

This section explains the options in the **Wireless** configuration menu.

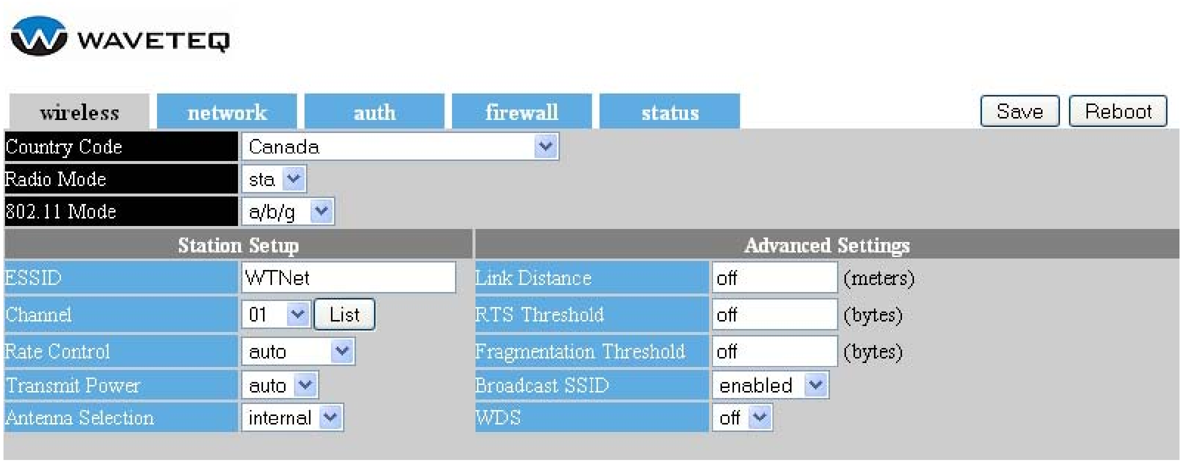
3.1. Wireless - Main

3.1.1. Country Code

This field constrains the frequency and transmit power lists to accepted values in the chosen country. Operation on frequencies, or with power levels, outside these values is illegal in most countries. This should be set to the country of operation. Please note that the channels and transmit power levels for a changed country code will not be correct until after a reboot.

3.1.2. Radio Mode

The Waveteq ShadowMini can operate in 2 radio infrastructure modes, either as a basic access point, or as an enterprise level client station. From the dropdown list, choose **ap** to setup as an access point or **sta** to operate as a client station. As an access point, the Waveteq ShadowMini will be the 'master' of the wireless network, and as a client station, it will participate as a 'managed' client.



Country Code	Canada
Radio Mode	sta
802.11 Mode	a/b/g

Station Setup		Advanced Settings	
ESSID	WTNet	Link Distance	off (meters)
Channel	01	RTS Threshold	off (bytes)
Rate Control	auto	Fragmentation Threshold	off (bytes)
Transmit Power	auto	Broadcast SSID	enabled
Antenna Selection	internal	WDS	off

Figure 9 – Wireless Menu

3.1.3. 802.11 Mode

If needed, the Waveteq ShadowMini can be locked into either an a, b, or g 802.11 mode. This will not only change the available frequencies, but will also not allow association to an access point operating in modes other than the one selected. In most cases, this should be left as default a/b/g allowing operation in all 3 modes.

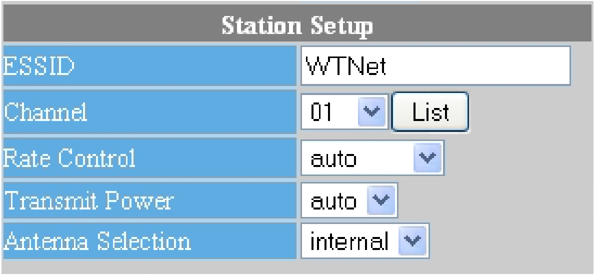
- 802.11b-rates from 1 to 11 Mbps using Direct Sequence Spread Spectrum (DSSS). This is the original 802.11 modulation scheme and is best used when older clients exist in the networks that are unable to use 802.11g.
- 802.11g-rates from 11 Mbps to 54 Mbps using Orthogonal Frequency Domain Multiplexing (OFDM). This is a more robust modulation scheme, decreasing the probability of interference and having more superior propagation characteristics. 802.11g is backwards compatible with 802.11b clients, but associations from these clients will slow down transmissions to 802.11b rates.
- 802.11a-rates from 11 to 54 Mbps using OFDM. This band is less congested with higher propagation, and therefore the probability of interference is reduced. The higher frequency translates into reduced propagation distance, but performance is generally better due to less interference. 802.11a is generally recommended for use as a backhaul link.

3.2. Station Setup

3.2.1. ESSID

Network Name (ESSID) - **Extended Service Set IDentifier (ESSID):** A type of unique identifier applied to both the AP and the wireless PC Card that is attached to each packet. This allows the AP to recognize each wireless client and its traffic. ESSIDs on the AP and on the Clients that connect to it must be the same.

The ESSID is case sensitive and can be no more than 20 characters.



Station Setup

ESSID	WTNet
Channel	01 List
Rate Control	auto
Transmit Power	auto
Antenna Selection	internal

Figure 10 – Station Setup

3.2.2. Channel

This is the 802.11 channel for communication to occur on. The channel defines both the operating frequency, and the modulation scheme to use. Available channels for license exempt operation are dependent on your country. To view a list for the currently active country, press the **“list”** button. Refer to *Appendix A* for a list of channels supported by the world’s regulatory domains.

3.2.3. Rate Control

This is the speed (in Mbps) the card should operate on, and is dependent on the mode and the quality of the channel. To have the rate automatically selected based on the connection, select “auto”

3.2.4. Transmit Power

The maximum transmit power is dependent on the country of operation, but in many cases the link will not need the full power to be effective, and performance can actually be degraded with a signal level too high. In addition, using more power than needed is a poor use of crowded license exempt spectrum and should be discouraged. The minimum value is 0 dBm, and the Waveteq ShadowMini can be set to values of 1 through 5 (max) of the maximum value the selected country will allow.

3.2.5. Antenna Selection

The Waveteq ShadowMini comes with an integrated panel antenna built into the chassis. In addition, some models are available with an external antenna connector as an option.

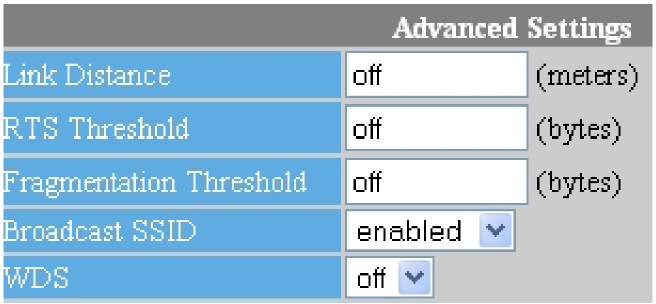
This field allows the user to choose whether the internal antenna, or an antenna coupled to the external connector should be used. If an external connector is not present, this should always be left set to internal.

3.3. Advanced Settings

3.3.1. Link Distance

This field sets the maximum time the radio will wait for an acknowledgement from the reciprocal station, in which data has been received properly. If an acknowledgement is not received, the radio will retransmit the data. If the link distance is set too low, and does not allow sufficient time for the remote radio to receive the transmission and send an acknowledgment, then valuable bandwidth will be wasted in retransmission.

This value should be set slightly higher than the distance to the furthest station. Values too high will have a small performance hit on the network due to some extra time waiting for acknowledgements, but values set too low will have serious negative consequences because of unnecessary retransmissions.



Advanced Settings

Link Distance	off	(meters)
RTS Threshold	off	(bytes)
Fragmentation Threshold	off	(bytes)
Broadcast SSID	enabled	
WDS	off	

Figure 11 – Wireless Advanced Settings

Link Distance values should be specified in metres, which is automatically converted to a time value. Valid values are between 0 and 120 000, or "off" to leave as default value of 300 metres.

3.3.2. RTS Threshold

The Waveteq ShadowMini can use the Request to Send (RTS) and Clear to Send (CTS) mechanisms to help improve network performance in situations where the hidden node problem is a concern. When a value exists for RTS, the ShadowMini will let the receiving station know that it has data to send (RTS), and wait for a corresponding signal telling it that it is OK to begin transmitting (CTS). This is most useful when many stations are communicating to a base station, but are unable to detect the traffic from other clients due to distance, obstructions, or antenna alignment. In these cases, the regular "transmit as soon as the channel is free" (CSMA) algorithm is ineffective because a station doesn't know when other stations are transmitting, possibly resulting in packet collision.

If RTS is to be used, an integer greater than 0 refers to the number of bytes to use as a threshold to force the station to request time to send its data. Any packet larger than this threshold will trigger the RTS, but those smaller will continue using the CSMA method.

Valid values are between 0 and 2347. The default is to leave RTS disabled, by entering "off".

3.3.3. Fragmentation Threshold

When network collisions are a problem, due to interference or network congestion, a large packet size increases the probability of a collision in addition to increasing the amount of data that needs to be retransmitted. Decreasing the fragmentation threshold allows larger packets to be fragmented and sent as several smaller packets; thereby decreasing the chances of collisions occurring for each packet. The Waveteq ShadowMini allows the threshold to be set for when this fragmentation occurs.

Valid values are between 256 – 2048 bytes, or "off" to turn off fragmentation, which is the default.

3.3.4. Broadcast SSID

The broadcast SSID setting is only valid in the Access Point mode. Disabling Broadcast SSID hides the SSID name from stations doing a site survey. To associate with the access point, users must know the SSID. This will add limited security to the access point, as casual users will have to determine the SSID before being able to associate with the access point. By default, this is enabled, and all users will know the SSID.

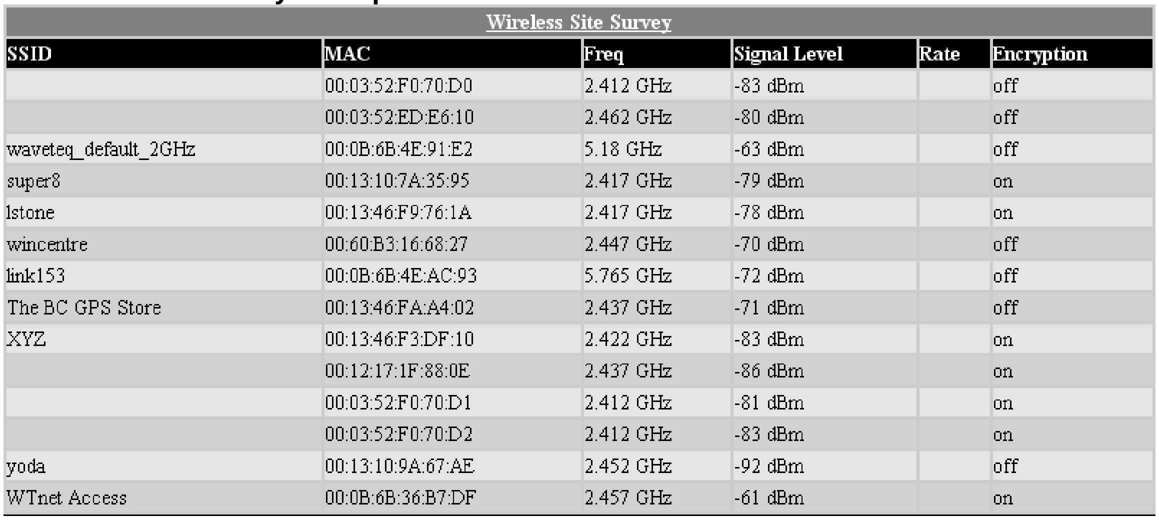
3.3.5. WDS – Wireless Distribution System

WDS allows for linking two Access Points together, or can be used when two ShadowMinis are used together as bridges; to create a transparent link. Setting this to yes permits 4 address headers to be used in the 802.11 transmission instead of 3.

3.4. Site Survey

When in client mode, the Web GUI will display a site survey whenever the Wireless page is loaded. This corresponds to all real or virtual access points whose beacons can be received during the scanning window (approximately 1 second).

Table 3 – Site Survey Example

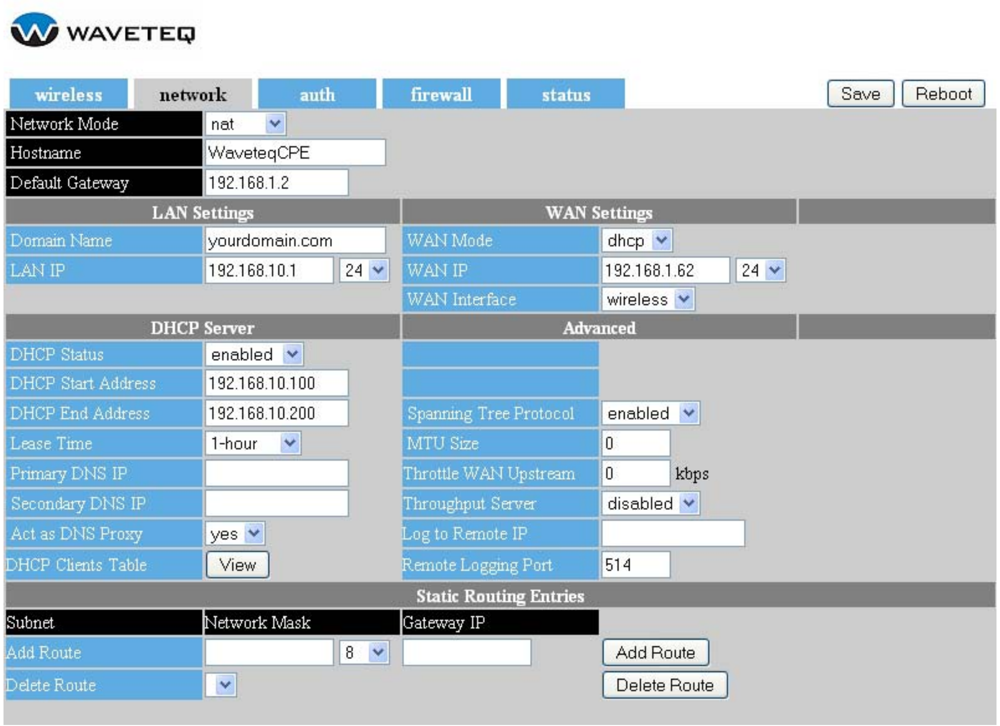


Wireless Site Survey

SSID	MAC	Freq	Signal Level	Rate	Encryption
	00:03:52:F0:70:D0	2.412 GHz	-83 dBm		off
	00:03:52:ED:E6:10	2.462 GHz	-80 dBm		off
waveteq_default_2GHz	00:0B:6B:4E:91:E2	5.18 GHz	-63 dBm		off
super8	00:13:10:7A:35:95	2.417 GHz	-79 dBm		on
lstone	00:13:46:F9:76:1A	2.417 GHz	-78 dBm		on
wincentre	00:60:B3:16:68:27	2.447 GHz	-70 dBm		off
link153	00:0B:6B:4E:AC:93	5.765 GHz	-72 dBm		off
The BC GPS Store	00:13:46:FA:A4:02	2.437 GHz	-71 dBm		off
XYZ	00:13:46:F3:DF:10	2.422 GHz	-83 dBm		on
	00:12:17:1F:88:0E	2.437 GHz	-86 dBm		on
	00:03:52:F0:70:D1	2.412 GHz	-81 dBm		on
	00:03:52:F0:70:D2	2.412 GHz	-83 dBm		on
yoda	00:13:10:9A:67:AE	2.452 GHz	-92 dBm		off
WTnet Access	00:0B:6B:36:B7:DF	2.457 GHz	-61 dBm		on

4.0 Network Settings

This section explains the options in the **Network** configuration menu.



Network Mode	nat
Hostname	WaveteqCPE
Default Gateway	192.168.1.2

LAN Settings		WAN Settings	
Domain Name	yourdomain.com	WAN Mode	dhcp
LAN IP	192.168.10.1 24	WAN IP	192.168.1.62 24
		WAN Interface	wireless
DHCP Server		**Advanced**	
DHCP Status	enabled		
DHCP Start Address	192.168.10.100		
DHCP End Address	192.168.10.200	Spanning Tree Protocol	enabled
Lease Time	1-hour	MTU Size	0
Primary DNS IP		Throttle WAN Upstream	0 kbps
Secondary DNS IP		Throughput Server	disabled
Act as DNS Proxy	yes	Log to Remote IP	
DHCP Clients Table	View	Remote Logging Port	514

Static Routing Entries

Subnet	Network Mask	Gateway IP	
Add Route	8		Add Route
Delete Route			Delete Route

Figure 12 – Network Settings Menu

4.1. Network - Main

4.1.1. Network Mode

The Waveteq ShadowMini can function in 3 different network modes:

- NAT Mode – Network Address Translation. When in this mode, there is a LAN (Local Area Network) and a WAN (Wide Area Network) interface. The LAN interface is connected to a customer's home or internal network, whereas the WAN interface connects to the internet or service provider. Multiple customers can connect to the LAN side, but all traffic destined for outside the network appears to come from the same machine, which is the ShadowMini. This is also referred to as masquerading and creates a logical demarcation point between a provider and customer.
- Router Mode – Both the wireless and Ethernet interfaces are members of different networks, and data passing through them is routed based on entries in a routing table. This allows different physical networks to be connected together based on the IP protocol. Static routes can be added to allow different paths for different networks.
- Bridge Mode – When in bridge mode, the ShadowMini simply forwards whatever appears at one interface, to the other. The IP assigned to the Ethernet port will now be assigned to the bridge, but its function is only to allow communications with the ShadowMini itself as a true bridge has no IP. As bridges function at layer 2, and as they are inherently inefficient and you are urged to learn about how a bridge works to determine the optimal solution for your application. By default, the bridge functions as a proxy ARP bridge (station bridge), but functions as a true wireless bridge when WDS is used.

4.1.2. Hostname

The hostname is a unique name given to a machine on a network. The hostname must be a string between 0 and 23 characters.

4.1.3. Default Gateway

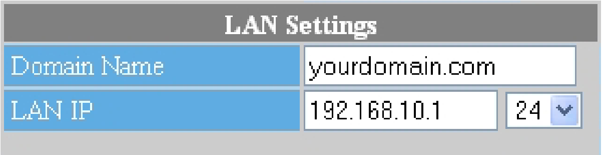
Any routed machine should have a default gateway. When no other routing rules exist for a particular subnet, it is this IP address that data is sent to. Usually this is the next router in line to the internet.

This field is mandatory if a static IP is to be configured on the WAN.

4.2. LAN Settings

4.2.1. Domain Name

Some computers are members of a domain, which can be entered here. This field must be 23 or less characters.



LAN Settings		
Domain Name	yourdomain.com	
LAN IP	192.168.10.1	24

Figure 13 – Lan Settings

4.2.2. LAN IP

The IP address to assign to the LAN interface. This is a mandatory setting and will also be used as a gateway for computers connecting to the LAN, and possible as a DNS proxy server and DHCP server. A valid IP address must be entered in addition to a valid netmask.

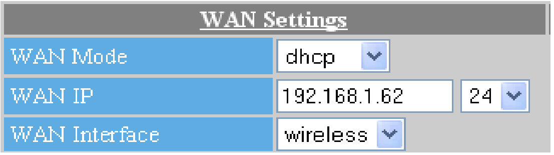
4.3. WAN Settings

4.3.1. WAN Mode

The WAN side can either be assigned a static IP, or can request one from a DHCP server. If DHCP is chosen, neither the WAN IP or Default Gateway fields need to be populated.

4.3.2. WAN IP

When the WAN is in static mode, a valid IP and netmask are required in this field.



WAN Settings		
WAN Mode	dhcp	
WAN IP	192.168.1.62	24
WAN Interface	wireless	

Figure 14 – WAN Settings

4.3.3. WAN Interface

A unique feature of the Waveteq ShadowMini is its ability to act as a basic access point in addition to its primary function as a client station. Furthermore, the side acting as the WAN interface (connecting to the provider or internet) can be switched between the Ethernet and wireless interfaces. Usually, when acting as a wireless client, the wireless interface will be the WAN, but when acting as an access point it might be useful to setup the Ethernet port as the WAN interface and masquerade all the wireless clients through it using NAT mode.

4.4. DHCP Server

4.4.1. DHCP Status

This setting turns the DHCP server on or off. If set to enabled, all the other DHCP settings will be validated on a save, and on the next boot the DHCP server will begin listening on the LAN and responding to DHCP requests. By default, this is enabled, and other devices will be able to connect to the Waveteq ShadowMini as DHCP clients.

4.4.2. DHCP Start Address

The lower address of the range to give out as addresses to DHCP clients. This must be part of the same subnet as the LAN IP, and a valid IP.

4.4.3. DHCP End Address

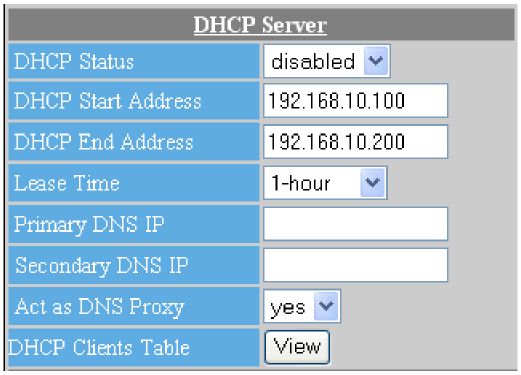
The upper address of the range to give out as addresses to DHCP clients. This must be part of the same subnet as the LAN IP, and be a valid IP address.

4.4.4. Lease Time

This specifies the absolute time that a DHCP lease is valid for. After this time is up, the client will request to renew its dynamically assigned IP address.

4.4.5. Primary DNS

If the WAN is set to a static IP and the DHCP server is used, a DNS server IP address is required in this field. This will be given to the clients requesting an address through DHCP. DNS will not function when the ShadowMini is in bridge mode.



DHCP Server	
DHCP Status	disabled
DHCP Start Address	192.168.10.100
DHCP End Address	192.168.10.200
Lease Time	1-hour
Primary DNS IP	
Secondary DNS IP	
Act as DNS Proxy	yes
DHCP Clients Table	View

Figure 15 – DHCP Server Settings

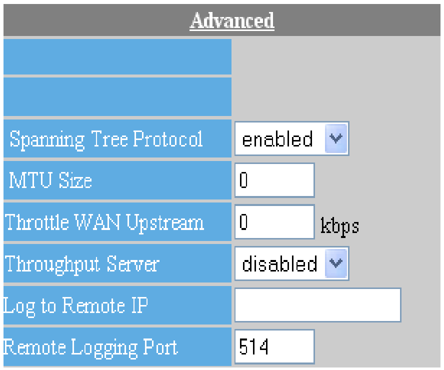
4.4.6. Secondary DNS

A backup to the primary DNS server when the ShadowMini is not acting as a proxy. Generally, most ISP's have a backup DNS server to respond to requests if the primary is down or overloaded.

4.4.7. Act as DNS Proxy

The ShadowMini can act as a DNS server proxy to the clients on the LAN. When enabled, clients receiving DHCP addresses will use the LAN IP of the ShadowMini as their DNS server. This makes the outside DNS servers transparent to the LAN clients, and also allows immediate timeouts when the WAN is offline.

4.5. Advanced



Advanced

Spanning Tree Protocol	enabled
MTU Size	0
Throttle WAN Upstream	0 kbps
Throughput Server	disabled
Log to Remote IP	
Remote Logging Port	514

Figure 16 – Advanced Network Settings

4.5.1. Spanning Tree Protocol

Spanning Tree Protocol is used when the ShadowMini is in bridged mode, and there are other redundant bridges on the network, to help eliminate bridge loops.

4.5.2. MTU Size

MTU, or maximum transmission unit defines the maximum packet or frame size, in bytes that can be passed through a network. If the packet is larger than the MTU, it must be broken down into smaller pieces (fragmented), which may cause increased packet loss, delay or jitter.

When set to 0, this defaults to 1500 for Ethernet, otherwise it must be an integer number between 1 and 10000.

4.5.3. Throttle WAN Upstream Bandwidth

Most modern networks use TCP/IP as their transport protocol. With TCP/IP, each end of a data stream tries to determine if packet loss is occurring, and if so tells the sending station to decrease its sending rate. Sometimes this is so slow to respond that the station continues to send more data than the network can send through, and therefore must continually resend packets that haven’t made it to the other end. This is particularly a problem with wireless, as stations will try to send as much data as possible, plugging up the channel for other users.

Throttling the upstream bandwidth is a method of traffic shaping, where computer network traffic is controlled in order to optimize or guarantee performance. Enabling this feature minimizes the number of retransmissions and wasted bandwidth. It can also allow an ISP to offer a maximum upstream bandwidth to their customers.

We recommend throttling to also take place on the access point so both data directions can be optimized. It is not a good solution to try to throttle incoming bandwidth as it is not efficient. When set to 0, no throttling will take place. Otherwise, the Waveteq ShadowMini will limit the outgoing WAN bandwidth to the value entered in kilobits per second.

Valid entries are from 0 to 20000.

4.5.4. Throughput Server

Selecting **enabled** here will activate a throughput server that can be used with another ShadowMini to initiate a data rate test between two units. This will measure the total Ethernet throughput that is being attained.

4.5.5. Log to Remote IP

The Waveteq ShadowMini can be setup to log its status to a remote syslog server. Free syslog servers are available for most operating systems, and are fairly easy to setup. If left blank, the ShadowMini does not attempt to log its status to a remote machine. Otherwise, this field must contain a valid IP address. In either case, the ShadowMini will continue to log locally, the results of which can be viewed from the status page.

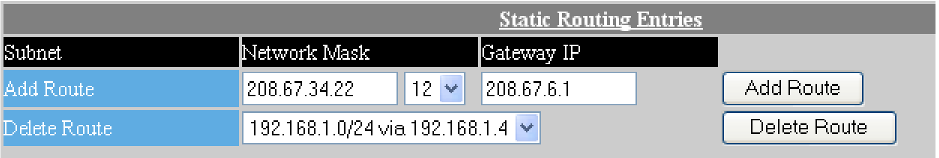
4.5.6. Remote Logging Port

When logging to a remote syslog server, an entry in this field will determine the port that the syslog service is listening on. By default, this should be set to 514 for UDP and 1468 for TCP, but can be changed if needed.

4.6. Static Route Entry

When used in router mode, there may be a need to define static routes, where packets should be routed when intended for a certain destination network. Proper entry will require a subnet and network mask corresponding to the destination network, and a gateway server IP to route these packets to. The Waveteq ShadowMini will only allow a maximum of 10 static routes to be entered, and will reject any combination of subnet, network mask and gateway that is invalid.

A valid route includes the Network Mask and its length in bits, which together specify the subnet mask. For example, if all IP addresses in the 192.168.10.x subnet are to be included in the route, the Network Mask will be 192.168.10.0, with a length of 24 bits. Also, the Gateway IP address must correspond to a device connected to the Waveteq ShadowMini which can help find the desired subnet. A default route is specified with a Network Mask of 0.0.0.0 and 0 bit length.



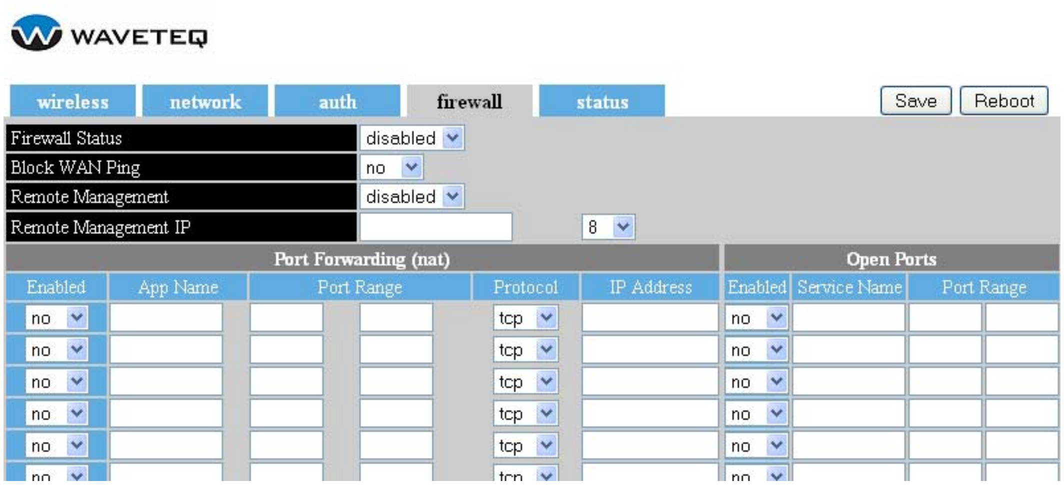
Static Routing Entries

Subnet	Network Mask		Gateway IP	
Add Route	208.67.34.22	12	208.67.6.1	Add Route
Delete Route	192.168.1.0/24 via 192.168.1.4			Delete Route

Figure 17 – Static Route Entry Box

5.0 Firewall Settings

This section explains the options in the **Firewall** configuration menu.



Firewall Status	disabled	
Block WAN Ping	no	
Remote Management	disabled	
Remote Management IP		8

Port Forwarding (nat)						Open Ports			
Enabled	App Name	Port Range		Protocol	IP Address	Enabled	Service Name	Port Range	
no				tcp		no			
no				tcp		no			
no				tcp		no			
no				tcp		no			
no				tcp		no			
no				tcp		no			

Figure 18 – Firewall Settings Menu

5.1. Firewall - Main

The Waveteq ShadowMini comes with a basic integrated firewall that has the ability to block ports and also to forward ports to machines behind a private gateway to allow public server access to machines behind the NAT firewall.

The firewall works at the Layer 3 packet layer, therefore can only be used when the ShadowMini is in either NAT or router network mode.

The firewall only functions when it has been set to Enabled from the Firewall Status dropdown box.

5.1.1. Firewall Status

When set to enabled, port forwarding is active when in the NAT network mode and the blocking firewall is enabled when in router mode. Set to disabled to turn off the firewall service.

5.1.2. Block WAN Ping

When Block WAN Ping is set to yes, the WAN side of the ShadowMini will not respond to ping requests.

5.1.3. Remote Management

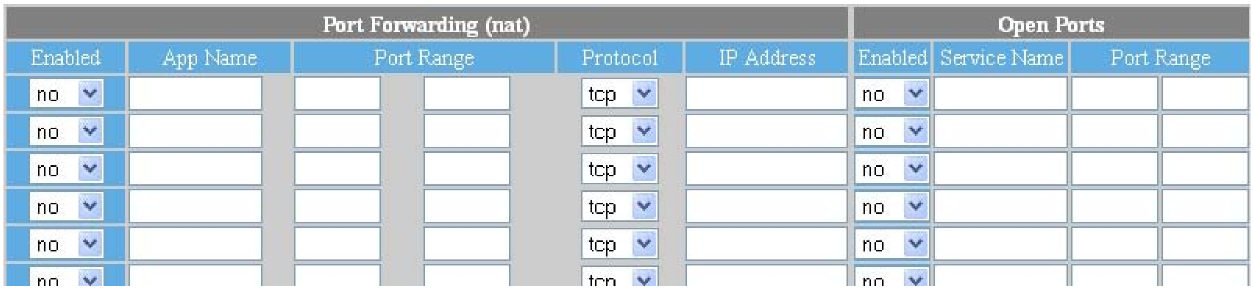
Allows remote management, which is the ability to access the web GUI and secure shell from the WAN interface, from a certain group of computers. When the firewall is off, access is allowed from anywhere when remote management is turned to off. When the firewall is off and remote management is on, only specified IPs can access the GUI/shell. When the firewall is on and remote management is off, no computer on the WAN side can access the GUI/shell. When the firewall is on, and remote management is enabled, only specified devices can access the management utilities.

5.1.4. Remote Management IP

Allows range of IP's to set as allowed when remote management is enabled.

5.2. NAT Firewall

When the ShadowMini network mode is set as NAT, the firewall becomes a port forwarder, which allows incoming WAN ports to be forwarded to LAN ports on specific machines. This allows a machine with a private IP address to have specific ports be "seen" from the public WAN (usually the internet). Port forwarding is particularly useful when a machine behind a NAT firewall wants to act as a web or ftp server. Users on the internet cannot directly access this computer because its private IP address isn't addressable from outside the network. Port forwarding allows the internet users to point at the public IP on the Waveteq ShadowMini, which will then transparently forward the requests to the private machine.



Port Forwarding (nat)						Open Ports			
Enabled	App Name	Port Range		Protocol	IP Address	Enabled	Service Name	Port Range	
no				tcp		no			
no				tcp		no			
no				tcp		no			
no				tcp		no			
no				tcp		no			
no				tcp		no			

Figure 19 – Port Forwarding

The ShadowMini will allow up to 10 port forwarding rules that can be turned on and off independently. Each rule takes 5 parameters as follows.

5.2.1. Enabled

If set to enabled, this rule is active the next time the settings are saved and activated (reboot). Otherwise, the rule is ignored but the settings are retained in memory.

5.2.2. App Name

The App Name field can be left blank, but is there to help the user remember what the rule is used for. For instance if you wanted to run an ftp server behind the NAT firewall, you may type "ftp" in this box to remind yourself of the rules purpose.

5.2.3. Port Range

For each rule, a port range must be entered. The port range lists the consecutive port numbers that will forwarded to the IP entered in the IP address box. The port numbers must be entered with the lower number in the left box, and higher number in the right. To specify a single port, enter the same port number in both boxes.

The numbers must be between 0 and 65535.

5.2.4. Protocol

Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are two methods of sending packet data between two points. UDP is connectionless, meaning there is no end to end checking while TCP is connection oriented and will have knowledge when errors occur. In the Waveteq

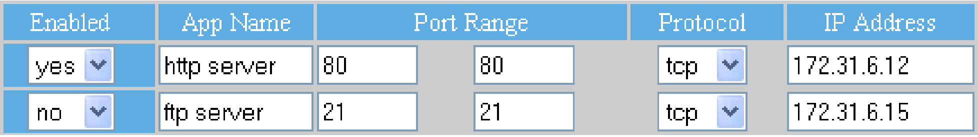
ShadowMini, a user can choose to forward only UDP packets or only TCP packets by selecting from the protocol drop-down menu.

5.2.5. IP Address

This is the internal private IP address to forward services on the specified port to. Obviously it must be a valid and existing IP address.

5.2.6. Port Forward Example

Assume that a user would like to set up both an FTP and a web server on different private machines behind the ShadowMini, when it's in NAT network mode. They would like to run the web server immediately on 172.31.6.12, but disable the ftp server on 172.31.6.15 until they can set it up properly. The following figure shows what they would enter if they planned on using the default ports.



Enabled	App Name	Port Range		Protocol	IP Address
yes	http server	80	80	tcp	172.31.6.12
no	ftp server	21	21	tcp	172.31.6.15

Figure 20 – Port Forwarding Example

If the Waveteq ShadowMini had a public IP on the WAN side of 23.34.34.6 then a user on the internet could now access the http server at 23.34.34.6:80, and when enabled could access the ftp server at 23.34.34.6:21, even though both of these servers have non-public IP addresses.

5.3. Router Firewall

When the Waveteq ShadowMini is operating in router mode, the firewall mode becomes a true firewall. It functions by blocking all layer 3 packets except the most commonly used protocols. In addition, the user also has the ability to add up to 10 additional services that will also be permitted, by opening specific port ranges. The following table lists the default ports that are open when the firewall is enabled.

Table 4 – Firewall Default Allowed Ports List

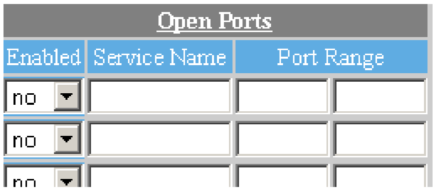
Port			
Low	High	Protocol	Abbr.
20	22	File Transfer Protocol	ftp
25	25	Simple Mail Transfer Protocol	smtp
52	52	XNS Time Protocol	xns-time
80	80	World Wide Web (http)	www
110	110	POP3 Mail	pop3
143	143	Internet Message Access Protocol	imap2
443	443	Secure http	https
465	465	Secure Simple Mail Transfer Protocol	smtps
554	554	Real Time Stream Protocol	Rtsp
563	563	Network News Transfer Protocol	nntps
989	990	Secure File Transfer Protocol	ftps
993	995	Secure IMAP4	imaps
1723	1723	Point to Point Tunnelling Protocol	pptp
1863	1863	MSN Messenger Protocol	msnp
3689	3689	Digital Audio Access Protocol	daap
5050	5050	Multimedia Conference Control	mmcc
5190	5190	America Online	aol

5.3.1. Enabled

If set to enabled, this firewall rule is active and the specified port range will be let through the firewall after the next reboot. Otherwise, the rule is ignored but the settings are retained in memory.

5.3.2. Service Name

The Service Name field can be left blank, but is there to help the user remember what the rule is used for. A useful description of what services the port range refers to should be entered.



Open Ports			
Enabled	Service Name	Port Range	
no			
no			
no			

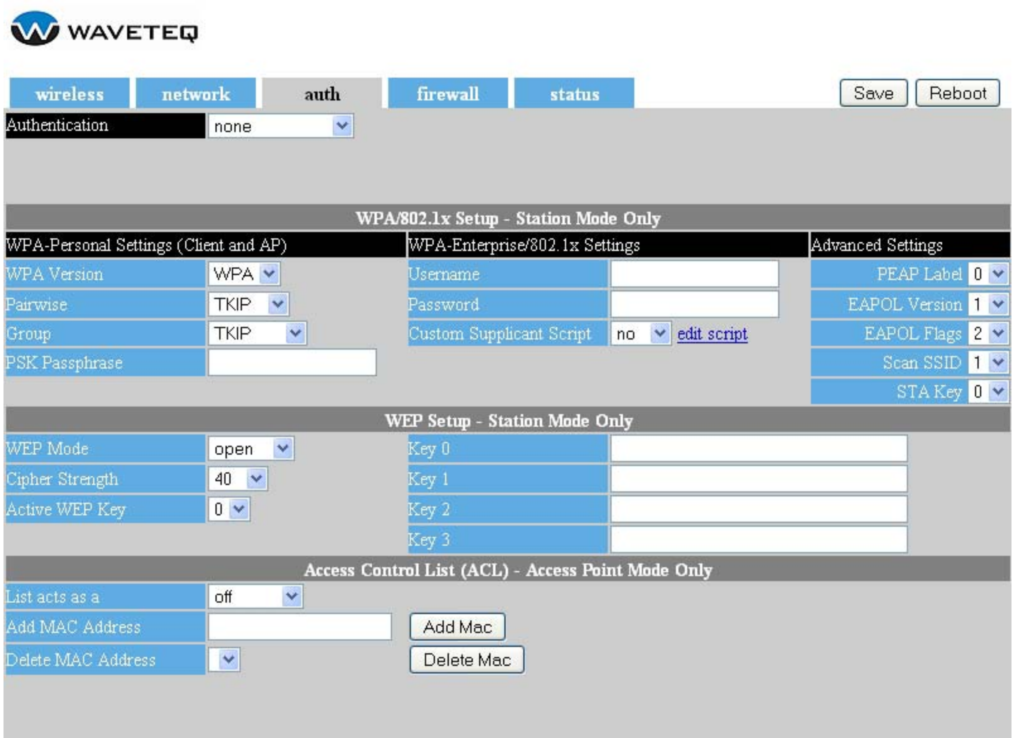
Figure 21 – Open Ports

5.3.3. Port Range

For each rule, a port range must be entered. The port range lists the consecutive port numbers that will allowed through the firewall when the rule is enabled. The port numbers must be entered with the lower number in the left box, and higher number in the right. To specify a single port, enter the same port number in both boxes.

The port numbers must be between 0 and 65535.

6.0 Authentication / Authorization Settings



Authentication: none

WPA/802.1x Setup - Station Mode Only

WPA-Personal Settings (Client and AP)
WPA Version: WPA
Pairwise: TKIP
Group: TKIP
PSK Passphrase:

WPA-Enterprise/802.1x Settings
Username:
Password:
Custom Supplicant Script: no

Advanced Settings
PEAP Label: 0
EAPOL Version: 1
EAPOL Flags: 2
Scan SSID: 1
STA Key: 0

WEP Setup - Station Mode Only
WEP Mode: open
Cipher Strength: 40
Active WEP Key: 0
Key 0:
Key 1:
Key 2:
Key 3:

Access Control List (ACL) - Access Point Mode Only
List acts as a: off
Add MAC Address:
Delete MAC Address:

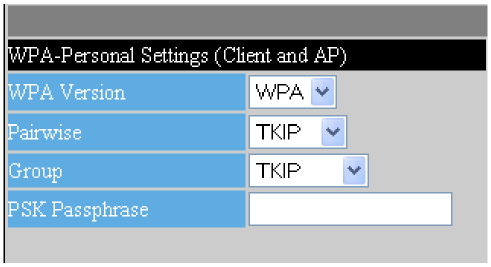
Figure 22 – Authentication and Authorization Settings Menu

The Waveteq ShadowMini has the ability to be used in numerous personal and enterprise authentication and encryption schemes when used as a client. These include:

- 64, 128-bit WEP
- WPA-PSK
- WPA and WPA2 with TKIP and CCMP ciphers
- WPA EAP/TLS, EAP/TTLS and EAP/PEAP
- 802.1x Radius

Additionally, when used as an access point, security can be attained by using an Access Control List to constrain allowed stations.

When using Authentication or Authorization schemes, select the corresponding type from the Authentication drop down box, or set it to none to not use any scheme.



WPA-Personal Settings (Client and AP)
WPA Version: WPA
Pairwise: TKIP
Group: TKIP
PSK Passphrase:

Figure 23 – WPA-PSK

6.1. WPA Personal (WPA-PSK)

This method uses a pre-shared key that must be known to both the access point and the clients for authorization. Data is encrypted using either TKIP or AES/CCMP algorithms.

6.1.1. WPA Version

Allows choice between WPA, and WPA2 (RSN). This should be set to the same value as that on the access point. RSN is more secure, but less access points support it, as it is a newer implementation of the 802.11i standard.

6.1.2. Pairwise

Unicast ciphers used by WPA and WPA2. Choose either TKIP or CCMP depending on the access point settings.

6.1.3. Group

Multicast and Broadcast ciphers used by WPA and WPA2. Choose TKIP, CCMP, WEP 40 or WEP 104 depending on the access point settings.

6.1.4. PSK Passphrase

This is the secret pass phrase that is shared between the access point and the clients. This pass phrase should never be shared with anyone.

6.2. WPA Enterprise and 802.1x Authentication

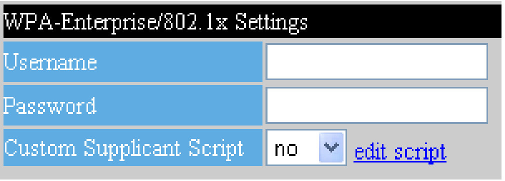
The access point communicates with a backend radius server to determine whether authentication is acceptable based on username, passwords and in some cases encrypted certificates. By default, the Waveteq ShadowMini is setup to be compatible with the most common forms of WPA-EAP and 802.1x authentication schemes, and only requires a username and password from a client. This is not true when authentication requires certificates, and a custom script will have to be created in those and other non standard cases.

6.2.1. Username

Enter the username to be verified against the radius server.

6.2.2. Password

Enter the password for the above username.



WPA-Enterprise/802.1x Settings

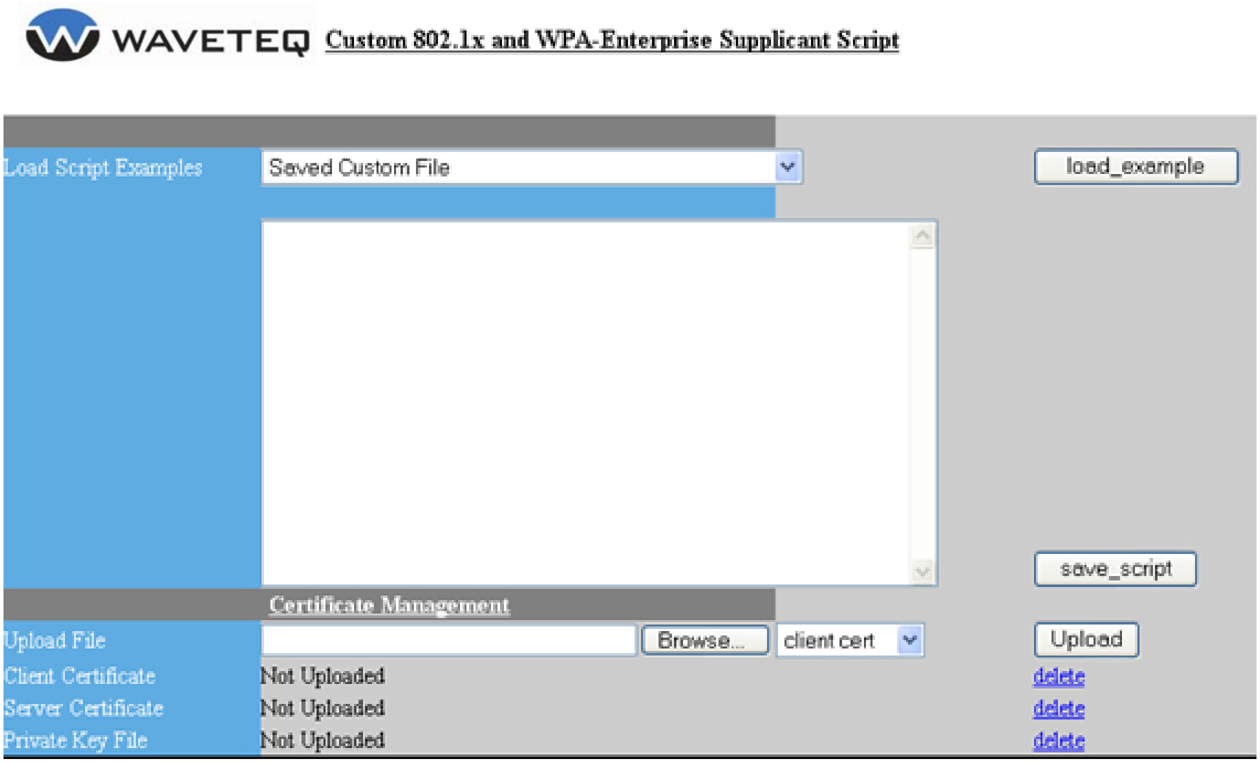
Username	
Password	
Custom Supplicant Script	no edit script

Figure 24 – WPA Enterprise

6.2.3. Custom Supplicant Script

For any authentication schemes that require certificates or other advanced options, a custom script can be created by clicking on “edit script”. After completion of the script, enable the Custom Supplicant Script and it will be used instead of the default.

6.3. Custom 802.1x and WPA-Enterprise Script



Custom 802.1x and WPA-Enterprise Supplicant Script

Load Script Examples: Saved Custom File

Certificate Management

Upload File	Browse... client cert	Upload
Client Certificate	Not Uploaded	delete
Server Certificate	Not Uploaded	delete
Private Key File	Not Uploaded	delete

Figure 25 – Custom Supplicant Script Menu

6.3.1. Load Script Examples

Several different scripts have been included as examples in the web GUI. In most cases, changing the SSID, username and passwords will be sufficient to make the script work. Choose a script from the dropdown box and press “load_example” button. When a certificate is required by a script, it must be uploaded to the ShadowMini following the directions below. After making the necessary changes, save the script by pressing the “save_script” button. This script can be brought back up by selecting “Saved Custom File” from the dropdown list.

6.3.2. Script Text Box

Enter the custom supplicant script here. The Waveteq ShadowMini uses the popular wpa_supplicant package to provide authentication, so there are numerous resources available on the internet to help make these scripts. When saved, the script is saved on the flash memory and can be loaded and changed from the Load Script Examples box.

6.3.3. Certificates

For very secure communications, a certificate authority may be used to verify digitally signed certificates on the server and client. The Waveteq ShadowMini has the ability to verify one client certificate and one server certificate, in addition to using a private key file. To upload a certificate or key, choose the certificate type (server, client or private key), browse to the file and press the “upload” button”. The filename will then show up beside its type and will list the size of the file. It can be deleted by pressing the "delete" link beside each certificate type. It is not possible to change the location or names of the uploaded files.

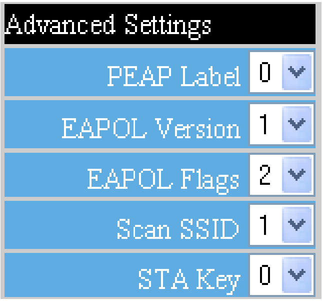
6.4. Advanced Settings

6.4.1. PEAP Label

When using PEAP, most access points and radius servers use the original peap label. If your equipment requires the new peap label then you can change this from the default of 0 to 1.

6.4.2. EAPOL Version

Some AP's do not support the new eapol version defined in IEEE 802.1X-2004, so the Waveteq ShadowMini defaults to the old version 1 for interoperability. If needed, this can be changed to support version 2.



Advanced Settings

PEAP Label	0
EAPOL Version	1
EAPOL Flags	2
Scan SSID	1
STA Key	0

Figure 26 – Auth Advanced Settings

6.4.3. EAPOL Flags

The IEEE 802.1X EAPOL option to specify whether unicast, broadcast or both unicast and broadcast wep keys are required for non WPA dynamic WEP. The default is to use both (3) but unicast only (1) and broadcast only (2) can also be selected if the access point requires it.

6.4.4. Scan SSID

By default, the Waveteq ShadowMini will find all Virtual Access points using multiple SSID's when scanning. This process is slow however, and if you don't want to find VAP's then this can changed to 0.

6.4.5. STA Key

This is set if the Key is to be used to secure STA to STA communication. Default is 0.

6.5. WEP Setup

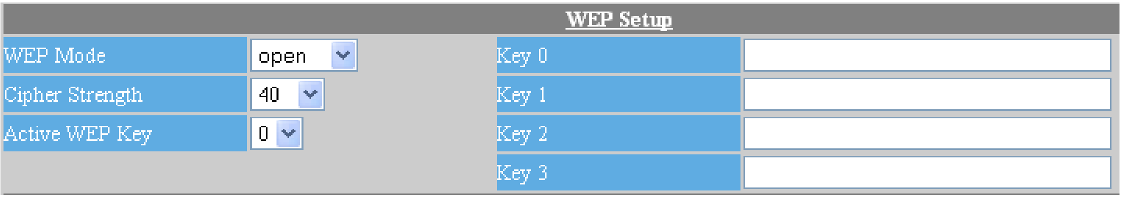
WEP is an older encryption method with serious encryption flaws that have been well documented. It does not provide for enterprise level of security, but in instances where highly secure networks are not needed, it is still used. Most importantly, even though WEP is not secure, it is still better than an open network. WEP is only available when in STA mode.

6.5.1. WEP Mode

802.11 Wired Equivalency Protocol supports both open system and shared key authentication, and both types are supported. Open authentication allows any wireless station requesting access onto the network, as long as the SSID is known. Shared key requires that each station (AP and client) have the same shared key before authentication can proceed. A challenge is then passed from the AP to the client before association takes place. This should be set to the same as the Access point.

6.5.2. Cipher Strength

Either 64 bit or 128 bit encryption strength is available. This consists of either a 40 or 104 bit secret key (in hex format). There is no error checking to ensure that this key is valid, so be sure to double check the entered value.



WEP Setup

WEP Mode	open	Key 0	
Cipher Strength	40	Key 1	
Active WEP Key	0	Key 2	
		Key 3	

Figure 27 – WEP Setup

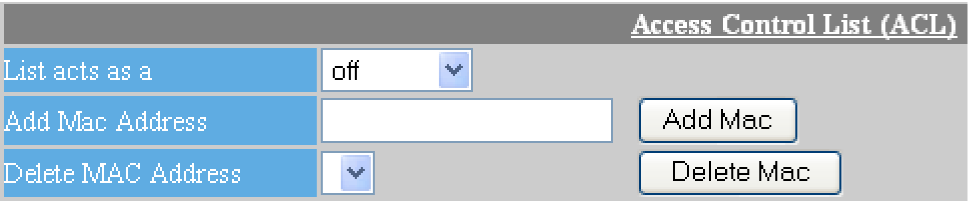
6.5.3. Active WEP Key

The Waveteq ShadowMini allows for up to 4 WEP keys to be entered and stored. This will allow users to change keys periodically (rotate through 4 known keys) without having to re-enter them. To set the active key, enter the number 0-3 corresponding to the key to be used.

6.5.4. WEP Keys 0-3

These fields allow entry of up to 4 WEP keys. Each one can be either a 40 or 104 bit hexadecimal number, corresponding to the secret key used on the access point that the ShadowMini will be connecting to. Only one key can be made active at a time.

6.6. Access Control List



Access Control List (ACL)

List acts as a	off	
Add Mac Address		
Delete MAC Address		

Figure 28 – Access Control List Entry

An access control list is used when the Waveteq ShadowMini is being used as an Access Point. It is the only method of limiting the stations that may associate to it. The list is always a list of valid MAC Addresses that are either the only stations that are allowed to access the network, or are stations banned from accessing the network

6.6.1. List Acts as a

When using ACL, the list can act as a whitelist or a blacklist. As a whitelist, all stations with MAC addresses matching the list are allowed network access, while all other stations are denied. As a blacklist, the access point is totally open to any station whose MAC address is not in the list. To turn off ACL and allow all stations to connect, the drop down box should be set to **"off"**.

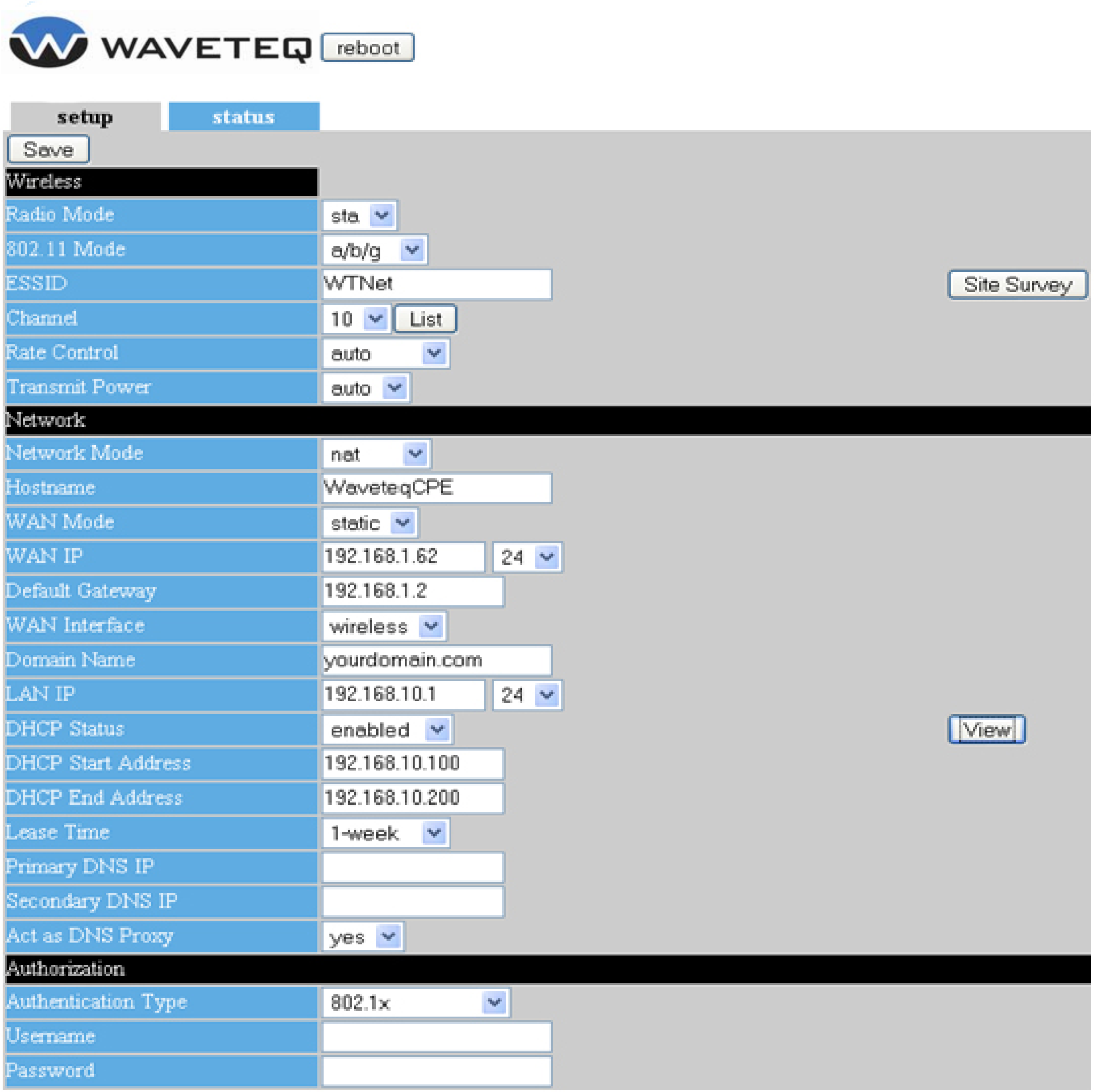
6.6.2. Add and Delete MAC Address

MAC addresses can be added to the list by entering the MAC address into the Add MAC Address text box and pressing the Add MAC Address button. If valid, this address will now appear in the dropdown box immediately below.

MAC addresses can be deleted from the list by selecting the corresponding MAC address in the Delete MAC Address drop down list and then pressing the delete MAC button.

7.0 Simplified Setup Menu

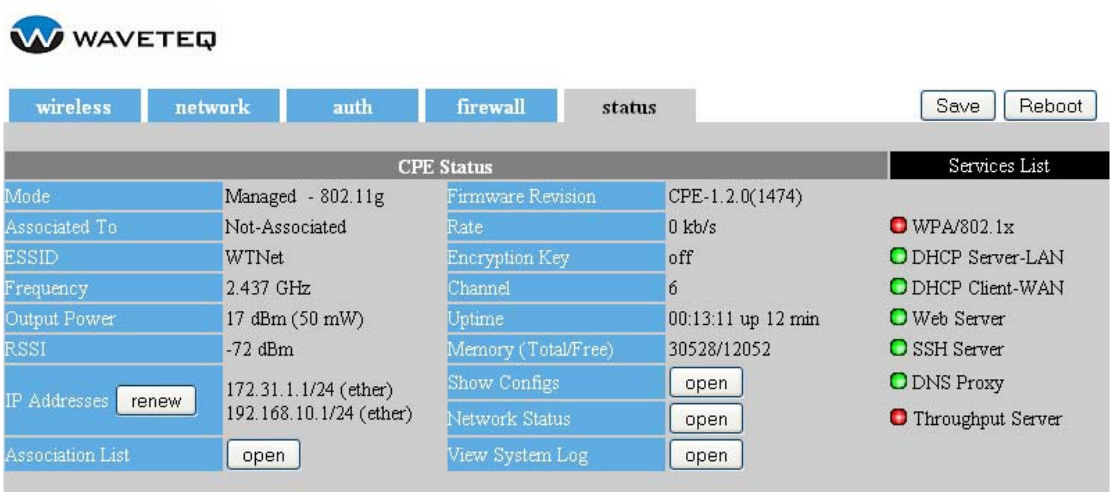
The Waveteq ShadowMini includes a simple mode to make administration easier for the average user. It has been designed to allow access to the most commonly changed wireless, network and authentication settings when logged in as **user** (see section *2.6 Logging* in through the WEB Interface), instead of admin. Settings that do not exist in simple mode can still be changed in the regular settings pages, and their values will remain. Please see the main wireless, network and authentication settings pages for descriptions of the fields.



Wireless	
Radio Mode	sta
802.11 Mode	a/b/g
ESSID	WTNet
Channel	10
Rate Control	auto
Transmit Power	auto
Network	
Network Mode	nat
Hostname	WaveteqCPE
WAN Mode	static
WAN IP	192.168.1.62 / 24
Default Gateway	192.168.1.2
WAN Interface	wireless
Domain Name	yourdomain.com
LAN IP	192.168.10.1 / 24
DHCP Status	enabled
DHCP Start Address	192.168.10.100
DHCP End Address	192.168.10.200
Lease Time	1-week
Primary DNS IP	
Secondary DNS IP	
Act as DNS Proxy	yes
Authorization	
Authentication Type	802.1x
Username	
Password	

Figure 29 – Simplified Setup Menu

8.0 Status Reporting



CPE Status				Services List
Mode	Managed - 802.11g	Firmware Revision	CPE-1.2.0(1474)	
Associated To	Not-Associated	Rate	0 kb/s	🟥 WPA/802.1x
ESSID	WTNet	Encryption Key	off	🟩 DHCP Server-LAN
Frequency	2.437 GHz	Channel	6	🟩 DHCP Client-WAN
Output Power	17 dBm (50 mW)	Uptime	00:13:11 up 12 min	🟩 Web Server
RSSI	-72 dBm	Memory (Total/Free)	30528/12052	🟩 SSH Server
IP Addresses renew	172.31.1.1/24 (ether) 192.168.10.1/24 (ether)	Show Configs	open	🟩 DNS Proxy
		Network Status	open	🟥 Throughput Server
Association List	open	View System Log	open	

Figure 30 – Status Reporting Page

8.1. ShadowMini Status Information

8.1.1. Mode

Displays the function (Access Point-Master or Client Station-Managed) and the 802.11 frequency mode (a,b,g) that the radio is currently operating in.

8.1.2. Associated to

When in client mode, displays the MAC address of the station that the ShadowMini CPE is connected to. When in Access Point mode, just displays the ShadowMini's own MAC address.

8.1.3. Output Power

Displays the output power the radio is using for transmission. This is constrained by the allowed maximum power determined by the country code setting.

8.1.4. RSSI

Received Signal Strength Indicator records the signal level in dBm of the station the ShadowMini is connected to. The RSSI is a function of the power, transmission losses, antenna gains and path profile between the two stations.

8.1.5. IP Addresses

Displays the current IP and netmask assigned to the ShadowMini interface, either ether(Ethernet), wireless or bridge. These IP is either assigned by DHCP, or statically as chosen in the Network Settings window. In addition, an emergency IP is also displayed for instances where the IP address has been forgotten or DHCP is not functioning correctly. There is also a button to renew the WAN IP if DHCP is being used. Pressing this button will release the current IP, and request a new one using the DHCP protocol.

8.1.6. Association List

When functioning as an Access Point, this button will open a window displaying statistics of all stations presently associated to the Access Point.

8.1.7. Firmware Revision

Displays the active firmware revision of the ShadowMini.

8.1.8. Rate

Displays the current 802.11 rate.

8.1.9. Uptime

Displays the time since the last bootup occurred.

8.1.10. Memory

Displays the total available memory (RAM) of the ShadowMini and how much is free. Performance will be degraded if the free memory gets too low, and if this happens, the ShadowMini should be rebooted.

8.1.11. Show Configs

When pressed, this will bring up a window displaying various user settings files. This can be useful in troubleshooting problems.

8.1.12. Network Status

Opens a window that displays the status of several networking subsystems including IP addresses, MAC addresses, ARP tables, Firewall rules, Routing tables and Access Control Lists.

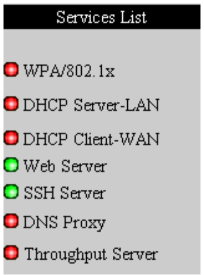
8.1.13. View System Log

Displays a detailed system log, to help aid in troubleshooting problems.

8.2. Services List

Displays the status of the following services by showing a green light for on and a red light for off.

- WPA/802.1x Authentication
- DHCP Server active on LAN
- DHCP Client active on WAN
- Web Server
- SSH Server
- ShadowMini Acting as a DNS Proxy



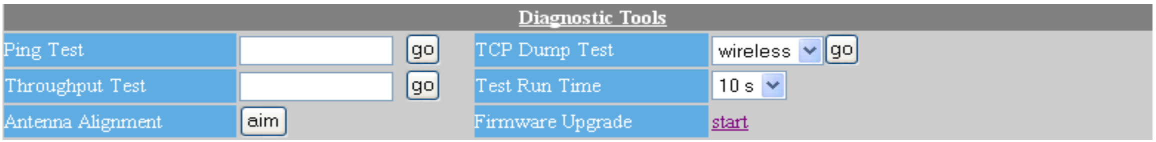
Services List

🔴 WPA/802.1x
🔴 DHCP Server-LAN
🔴 DHCP Client-WAN
🟢 Web Server
🟢 SSH Server
🔴 DNS Proxy
🔴 Throughput Server

Figure 31 – Services List

8.3. Diagnostic Tools

The Waveteq ShadowMini contains several tools that can be used to increase or measure performance.



Diagnostic Tools

Ping Test	[ ] go	TCP Dump Test	wireless ▾ go
Throughput Test	[ ] go	Test Run Time	10 s ▾
Antenna Alignment	aim	Firmware Upgrade	start

Figure 32 – Diagnostic Tools Entry Menu

8.3.1. Ping Test

The ping test requires a valid IP address entered into the text box. When "go" is pressed it will attempt 10 network pings, and record the response times.

8.3.2. Throughput Test

When a gauge of throughput is desired, the ShadowMini Throughput Test can be used. This test requires a Windows or *NIX machine that is running a nuttcp server; a freely available TCP test utility. When the server IP address is entered in the box and the "go" button is pressed, the ShadowMini will perform a transmit and a receive test for 10 seconds each. When completed, the throughput will be reported at 1 second intervals.

8.3.3. Antenna Alignment

This button will open up a window that will graph in real time the signal strength received at the ShadowMini. This function can be very useful when aligning the antenna for best performance.

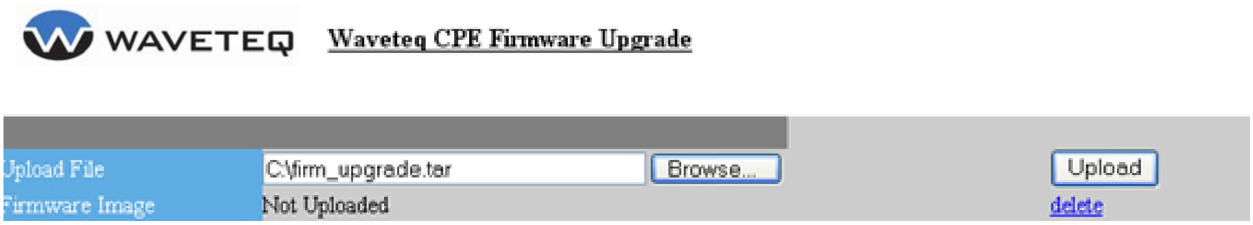
8.3.4. TCP Dump Test

The TCP Dump test will output a listing of all packets passing through either the wireless or Ethernet interface, for the time period chosen in the Test Run Time box. The output is equivalent to a packet sniffer, and can be useful in troubleshooting network problems.

8.4. Firmware Upgrade

The Waveteq ShadowMini has the ability to apply upgrades to the firmware when in the field. Periodically, Waveteq will release new firmware containing bug fixes and new features. To access the firmware upgrade section, press the start link beside the firmware upgrade section of the Diagnostic Tools.

To perform a firmware update, download a valid new firmware image from the Waveteq website (http://www.Waveteq.com) and from the Firmware Upgrade page browse to the file and click the upload button.



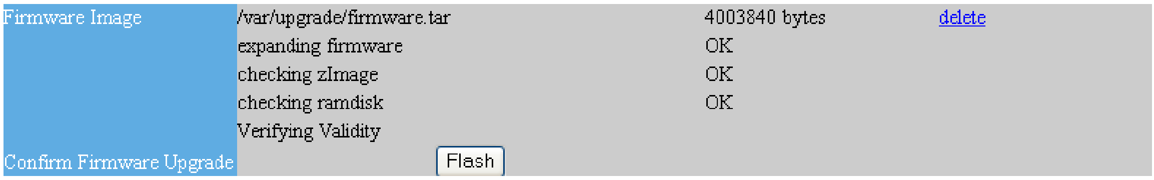
Waveteq CPE Firmware Upgrade

Upload File C:\firm_upgrade.tar

Firmware Image Not Uploaded

Figure 33 – Firmware Upload Page

After pressing the button, the update script will validate the uploaded firmware and if both the zImage and ramdisk portions of the firmware are uncorrupted, will present a flash button that will allow completion of the firmware upgrade.



Firmware Image /var/upgrade/firmware.tar 4003840 bytes

expanding firmware OK

checking zImage OK

checking ramdisk OK

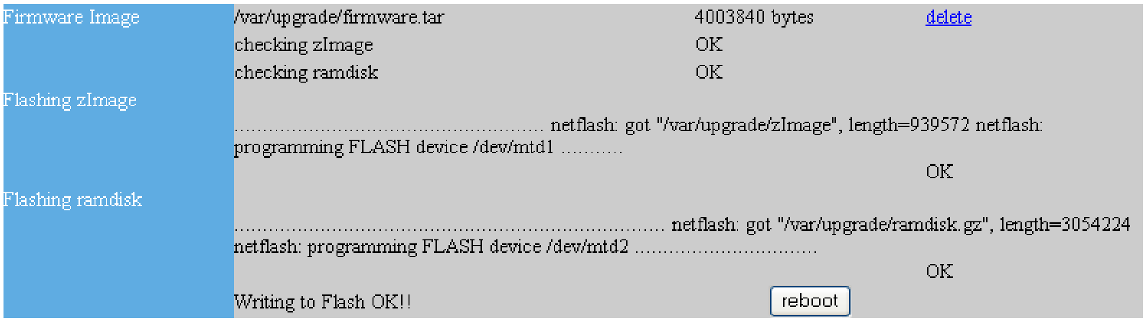
Verifying Validity

Confirm Firmware Upgrade

Figure 34 – Firmware Flash Page

It is important that after pressing the flash button the procedure runs through to completion without interrupting the power.

During the flash process the script will again check the validity of the zImage and ramdisk portions of the update and flash them to permanent storage separately. After each section is written a status message of OK or FAIL will be displayed on the screen. If either the zImage or ramdisk portion fails, or power is interrupted, the firmware image on the ShadowMini will permanently destroyed and the unit will have to be returned to the factory for reprogramming.



Firmware Image	/var/upgrade/firmware.tar	4003840 bytes	delete
	checking zImage	OK	
	checking ramdisk	OK	
Flashing zImage	.... netflash: got "/var/upgrade/zImage", length=939572 netflash: programming FLASH device /dev/mtd1		OK
Flashing ramdisk	.... netflash: got "/var/upgrade/ramdisk.gz", length=3054224 netflash: programming FLASH device /dev/mtd2		OK
	Writing to Flash OK!!	reboot	

Figure 35 – Firmware Completed

If successful, a button to reboot the unit will be displayed and should be pressed to complete the process.

Interrupting power or any other failure during the flash process will render the unit inoperable and will require a return to factory for reprogramming. Please ensure you follow these instructions carefully and double check you have downloaded a valid firmware image from a reputable source.

8.5. Status Graphs

The Waveteq ShadowMini CPE includes a graphing utility that can help you troubleshoot network problems, or get an idea of when different problems are occurring. Each minute, several important statistics are measured and stored by the ShadowMini. Data from the last seven days will be kept and graphed. All data will be reset after a reboot. The time specified on the X-Axis corresponds to the time the unit has been up since the last boot. There are links available to change the time scale of the graph. Available scales are 1 hour, 6 hours, 1 day, 3 days or 7 days.

8.5.1. Wi-fi Stats Graph

The Wi-Fi Statistics graph will keep track of the Signal Quality in dBm (RSSI-Noise), the associated 802.11 bit rate and also the ping time to the gateway server if defined.

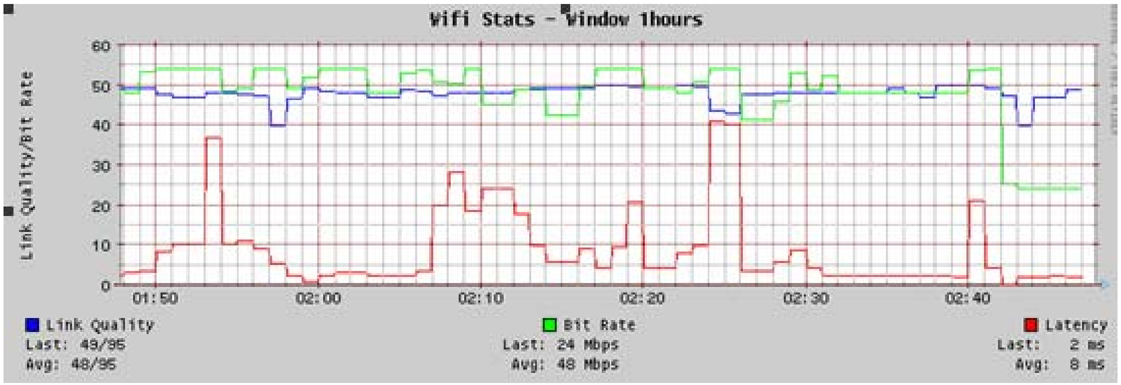


Figure 36 – Wireless Statistics Graph

8.5.2. Network Throughput Graphs

The network throughput graphs will plot the network throughput that has passed through either the wireless or Ethernet interfaces in both the upload and the download direction. The graphs are scaled in bits per second.

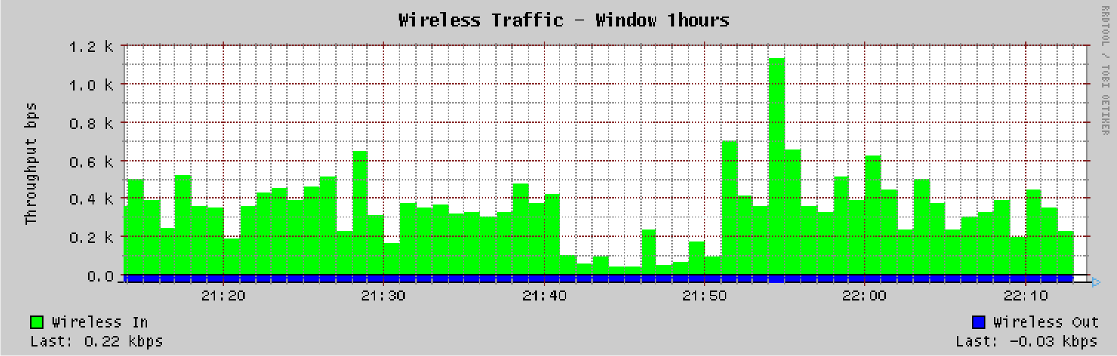


Figure 37 – Wireless Throughput Graph

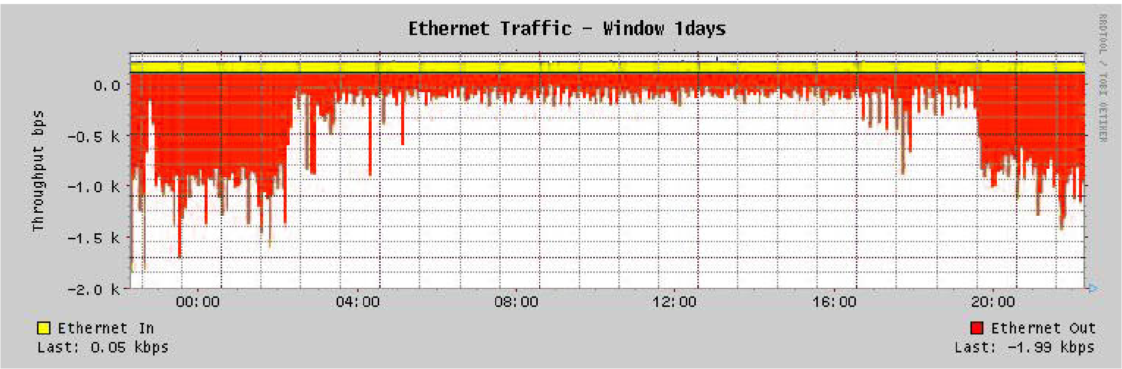


Figure 38 – Network Throughput Graph

9.0 Appendix A: Regulatory Domain/Channels

This appendix lists the IEEE 802.11a and IEEE 802.11b channels supported by the world's regulatory domains. The Waveteq ShadowMini supports all channels, but it has only been tested and certified to Industry Canada (IC) and Federal Communications Commission (FCC) standards for Canada and the USA.

Channels for IEEE 802.11b/g

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	Israel	France	China	Japan
1	2412	•	•	—	—	•	•
2	2417	•	•	—	—	•	•
3	2422	•	•	•	—	•	•
4	2427	•	•	•	—	•	•
5	2432	•	•	•	—	•	•
6	2437	•	•	•	—	•	•
7	2442	•	•	•	—	•	•
8	2447	•	•	•	—	•	•
9	2452	•	•	•	—	•	•
10	2457	•	•	—	•	•	•
11	2462	•	•	—	•	•	•
12	2467	—	•	—	•	•	•
13	2472	—	•	—	•	•	•
14	2484	—	—	—	—	—	•

Mexico is included in the Americas' regulatory domain; however, channels 1 through 8 are for indoor use only while channels 9 through 11 can be used indoors and outdoors. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of Mexico.

Channels for IEEE 802.11a

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	Singapore	China	Japan
34	5170	—	—	—	—	•
36	5180	•	•	•	—	—
38	5190	—	—	—	—	•
40	5200	•	•	•	—	—
42	5210	—	—	—	—	•
44	5220	•	•	•	—	—
46	5230	—	—	—	—	•
48	5240	•	•	•	—	—
52	5260	•	•	—	—	—
56	5280	•	•	—	—	—
60	5300	•	•	—	—	—
64	5320	•	•	—	—	—
100	5500	—	•	—	—	—
104	5520	—	•	—	—	—
108	5540	—	•	—	—	—
112	5560	—	•	—	—	—
116	5580	—	•	—	—	—
120	5600	—	•	—	—	—
124	5620	—	•	—	—	—
128	5640	—	•	—	—	—
132	5660	—	•	—	—	—
136	5680	—	•	—	—	—
140	5700	—	•	—	—	—
149	5745	•	—	—	•	—
153	5765	•	—	—	•	—
157	5785	•	—	—	•	—
161	5805	•	—	—	•	—

Mexico is included in the Americas regulatory domain; All channels are restricted to indoor use except in North America which allows for indoor and outdoor use of channels 52 – 64. Users are responsible for ensuring that the channel set configuration complies with the regulatory standards of Mexico.

10.0 Troubleshooting

- **I have connected my ShadowMini but there is no light illuminated on my Ethernet switch?**

  Make sure you have connected **tested** Ethernet cables and those cables are connected to the proper ports on the PoE device. Check to make sure directions provided in section 2.2 Ethernet Cable and Connector Assembly.

  Further, if problems remain, make sure you have applied proper power using the Waveteq supplied Wall Adapter.

- **OK, I have my Ethernet port LED illuminated but I cannot contact the ShadowMini through a browser interface?**

  First, make sure your computer or laptop is on the same subnet as your ShadowMini and that the submask matches. If the ShadowMini IP address has been changed for any reason, your computer IP must also change to be on the same subnet.

  If all else fails, change your computer or Laptop IP to an address on the same subnet as the emergency IP address (see 2.6.3 Emergency IP). You should now be able to connect to the Waveteq ShadowMini. If this still does not work, please contact our technical support team.

- **So I need to change my laptop IP address to be on the same subnet – what does that mean?**

  Your computer and the ShadowMini use a combination of an IP Address and subnet mask to determine how devices should respond to each other on the same physical (i.e. wire) interface. In reality it's a bit more complicated than that and a good reference can be found at;

  http://compnetworking.about.com/od/workingwithipaddresses/a/subnetmask.htm

  Suffice to say that if your Waveteq ShadowMini uses the default values your computer should have an Ethernet IP something like; 192.168.10.100 with a subnet mask that looks like 255.255.255.0

- **Thanks for the info on subnets, I'm using Windows XP and am wondering how do I know if I'm on the same subnet?**

  Since your new ShadowMini's default is to enable DHCP (Dynamic Host Configuration Protocol) your connection should already be set. Check it out by opening a "Command Prompt" through choosing "Start", "All Programs", "Accessories" and finally choosing the "Command Prompt".

  Now, type "ipconfig" at the prompt and your IP Address should look like the numbers shown in the previous question's paragraphs.

- **I checked out my IP address and it's not the same – what now?**

Two things; first, perhaps your ShadowMini's DHCP server has been turned off. In this case you need to know the IP address of the ShadowMini. This is because your ShadowMini is not providing your computer with information it needs to automatically set up your IP Address.

Second, your computer may have a static IP setup which is not on the same subnet. This can be changed by opening up your Network Connections dialogs and entering or adding a new IP with the appropriate subnets.

- **I suspect the DHCP has been turned off and/or I need to set up this new IP. How do I actually do that?**

If you are using a Windows based OS, and in particular Windows XP, you can follow these simple directions to add in a new IP.

1. Open up your network connections dialog by navigating to "Start" and clicking on "Control Panel".
2. Choose "Network Connections"
3. Select "Local Area Connections" by double clicking.
4. Choose "Properties".
5. Under "General", look for the dialog in the middle called "This connection uses the following items" and scroll down until you can see "Internet Protocol (TCP/IP)".
6. Click on this selection and choose the "Properties" button.
7. Make your selection using the radio button called "Use the following IP Address".
8. If there is no other IP Address which has been entered or you have just changed the radio button's setting, you can enter your new IP address in the text boxes below.
9. If there already exists a static IP entered into these boxes, then choose "Advanced" to **add** a second IP address. This second IP address will not interfere with your current static IP.
10. Once finished, click OK until you return to the Local Area Connection status dialog where you can now click "Close".
11. Once this dialog is closed your new IP address should have taken effect.
12. To check, see the previous page on "… **how do I know if I'm on the same subnet?"**

- **Whew, I've just changed and checked my IP but am still having trouble. Yes, the LED is illuminated. What's next?**

Well, sometimes even through your best efforts it still doesn't communicate. Once you've verified your IP address and know the ShadowMini is within that subnet range there is one last thing you can try.

With your Network Connections dialog box open, right click on the "Local Area Connection" entry and choose "Repair". Wait until it's finished and try connecting to your Waveteq ShadowMini again.

- **Thanks for all that information and troubleshooting tips but I'm still not able to browse my Waveteq ShadowMini.**

Well, thank you for your perseverance. If you have followed the troubleshooting tips so far and have tried both the primary IP and our Emergency IP, then perhaps now is the time to contact our support team, either at support@Waveteq.com via email address, or by phone at: 1-888-Waveteq(928-3837)

11.0 Glossary

ACL
Access Control List, this can be used to limit user from accessing the network. See the section on *Advanced Security and Access Control* for more details.

AES
Advanced Encryption Standard is the new Encryption standard used by the United States Government.

ARP
Address Resolution Protocol, This protocol translates between the IP address of a system and the MAC address or physical address.

Association List
This is a list of all the connected to a particular Access Point.

BGP
Border Gateway Protocol, Utilizes TCP exclusively as is transport protocol and allows for inter-Autonomous System routing. It is the only protocol able to manage the size of the Internet and being able to have multiple connections to unrelated routing domains at once.

Bridging
Bridging is a means to connect multiple networks using similar protocols. Bridges automatically forward information sent to one side of the bridge out on the other side.

BSS Channel
Basic Service Set channels, this are defined frequencies that are set by IEEE.

HTB
Hierarchal Token Bucket, This is a system of controlling Network Traffic by classifying Packets into pipes and giving priority to certain pipes.

DHCP
Dynamic Host Configuration Protocol, DHCP is a communications protocol that allows for the automatic appointing of IP addresses.

ESSID
Same as a Network Name

Firewall
Firewall is a term used to describe a system used to block unwanted Traffic from entering or leaving the LAN.

Gateway
This is a term give to a device that connects a Local Area Network (LAN) to a Wide Area Network (WAN).

IP Masquerading
This does the same function as NAT but every message that passed through the Gateway is considered as originating at the Gateway.

Mac Address
This is the physical address of a device. All network devices have a unique Mac Address used in transferring of information.

NAT
Network Address Translation is used by Gateways to hide the IP addresses for Devices inside its LAN. For example if a computer requests data from the internet a return IP address is stored in the request so the Server knows where to send the data, if this passes through a Gateway with NAT enabled that return IP address is changed so the Server doesn't know the exact origin of the message.

OSI Communications Model

This is a model for networking that consists of 7 layers. The bottom layer 1 is the physical connections of wires or in this case Wireless technology. Layer 2 consists of basic communication protocols and so on. For more information see: http://en.wikipedia.org/wiki/OSI_model

OSPF

Open Shortest Path First Protocol, is a dynamic routing protocol that can route through an unlimited number of sub networks as compared to the 5-jump limit imposed on RIP.

Ping

This is a method for determining what parts of a network a device can see. A ping is a simple function that uses IP protocol to request that a quick signal be sent to a host and that host reply. By measuring the time this process takes it is possible to measure the performance of the network.

Power over Ethernet (PoE)

This is a protocol created by IEEE to allow for power to be transferred over a standard Ethernet cable.

PPTP

Point-to-Point Protocol Is designed to tunnel the PPP protocol through IP. It allows for already existing Network Access Server functionality to be separated into two different categories.

QoS

Quality of Service, this refers to the ability of a device to control the amount and priority of traffic. QoS is important to guarantee SLA's (Service Level Agreements).

Routing

Is a method for multiple networks to communicate by making use of different protocols such as RIP OSPF and BGP. Unlike Bridging it can work on many interfaces and isn't limited to a single message in and out kind of transmission.

TX Power

This is the Power that is given to signals being sent out but a given Wireless Card.

VLAN

Virtual Local Area Network, This is a protocol that allows for the feeling of a LAN, but is provided over a larger network like the Internet.

WEP

Wired Equivalency Protocol, This was the origanal 802.11 security Standard. It does have security holes, see IEEE site for details.

WPA

Wi-Fi Protected Access, This protocol was designed to fix the problems with WEP. It can either use AES or TKIP encryption techniques.