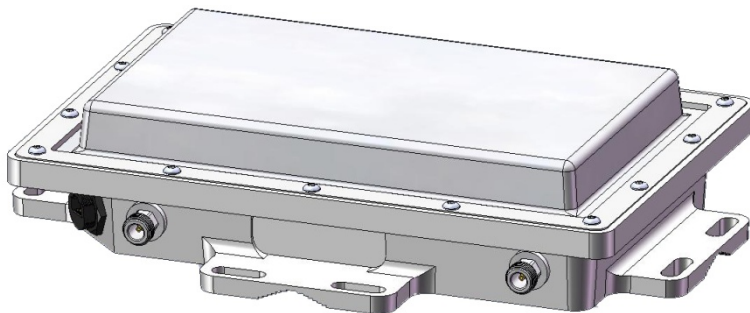


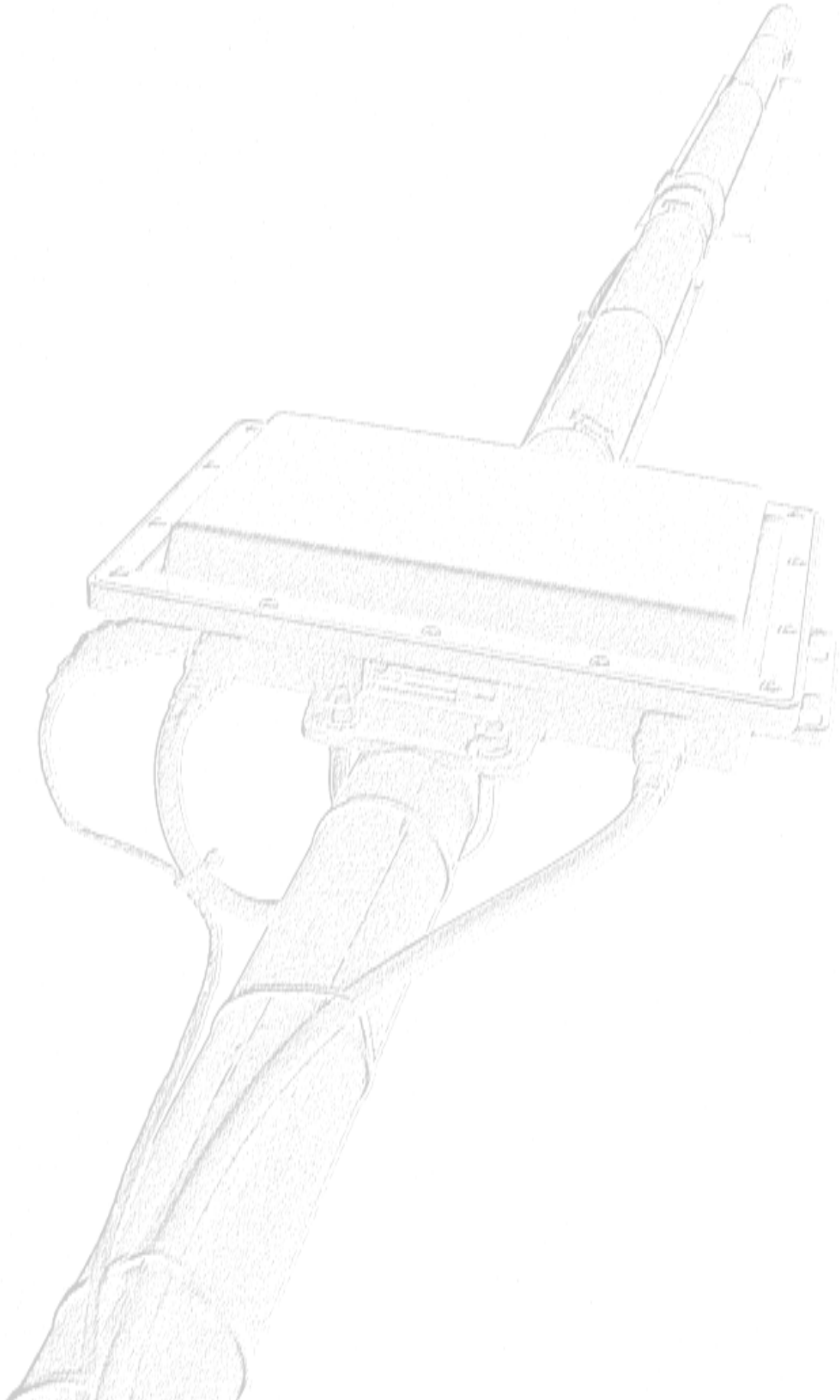


SHADOWMASTER User Manual



Revision 2.61

2008-08-14



Copyright

© 2006-2008 Waveteq Communications Inc

This user's guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Waveteq Communications Inc.

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 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. Administrators must ensure that they select the correct radio settings according to their regulatory domain. Refer to *Appendix B: Regulatory Domain/Channels* for more information on regulatory domains. Please check the regulations valid for your country and set the parameters concerning frequency, channel, and output power to the permitted values.

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 3 m (10') from people. Multiple antennas must also be mounted at least 20 cm (7.9") from each other.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p) is not more than that permitted for successful communication. The required antenna impedance is 50 ohms. Antenna types not included in this list, or antennas with gains greater than those listed below are strictly prohibited for use with this device. This device has been designed to operate with the antennas and power levels listed below:

- **SPDN6W**: 5100 – 5900 MHz 16.8 dBi panel antenna using transmit power levels of up to 7 dB (5180-5240 MHz), and 12 dB (5755-5795 MHz).
- **SPDJ6OP** – 5100 – 5900 MHz 9 dBi Omni antenna using transmit power levels of up to 14 dB (5180-5240 MHz), 15 dB (5755-5795 MHz).
- **SPAPG20** – 2300 - 2500 MHz 20.5 dBi panel antenna using transmit power levels up to 13 dB
- **SPDG80** – 2400 – 2483 MHz 9 dBi Omni antenna using transmit power levels up to 14 dB.

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 ShadowMaster.

Table of Contents

Table of Contents	v
Table of Figures	viii
1.0 Chapter 1 - Overview	1
1.1 ShadowMaster Features	2
1.2 Feature Locations	4
2.0 Chapter 2 - Installation	6
2.1 Mounting	6
2.2 Ethernet Cable and Connector Assembly	7
2.3 Factory Default Configuration	9
2.3.1 Emergency IP	9
2.4 Connecting to the ShadowMaster	10
2.4.1 Using Ethernet Connection	10
2.4.2 Using Wireless LAN Connection	12
2.5 Licensing	13
3.0 Chapter 3 – Command Line Interface Management	15
3.1 Introduction	15
3.2 CLI Access	15
3.3 Login	15
3.4 Authentication Check	16
3.5 Password	16
3.6 Shell	17
3.7 Show	17
3.8 Status	17
3.9 Reboot	18
3.10 Reset	18
3.11 Quit	18
4.0 Chapter 4 – Web Interface	19
4.1 Overview	19
4.2 Statistics	20
4.2.1 System Information	21
4.2.2 Network Details	22
4.2.3 Wireless Details	23
4.2.4 Routes	24
4.2.5 ARP Table	24
4.3 Configuration	25
4.3.1 Starting Point	25
4.3.2 Basic Network	27
4.3.3 Basic Wireless	28
4.3.4 Advanced Network	30
4.3.5 Advanced Wireless	31
4.3.6 Expert	32

4.4	System	33
4.4.1	Maintenance	33
4.4.2	Password	34
4.4.3	Remote Management	35
4.4.4	License	36
4.5	Tools	37
4.5.1	Site Survey	37
4.5.2	Antenna Alignment	38
4.5.3	Wireless Tests	39
4.6	Logout	41
5.0	Chapter 5 – SNMP Management	42
5.1	SNMP Versions	42
5.2	SNMP Agent	43
5.3	SNMP Community Strings	43
5.4	Use SNMP to Access MIB	43
6.0	Chapter 6 – Configuring the ShadowMaster	44
6.1	ShadowMaster Configuration File	44
6.2	Network Configuration	45
6.2.1	Interfaces	45
6.2.2	The Bridge	48
6.2.3	DHCP	50
6.2.4	DNS	52
6.2.5	DNS Forwarder	53
6.2.6	VLANs	54
6.2.7	IPsec	56
6.2.8	IPsec Racoon	58
6.2.9	GRE Tunnels	59
6.2.10	PPPoE Settings	60
6.3	Wireless Settings	61
6.3.1	Wireless Radio	61
6.3.2	Wireless Interface	65
6.3.3	AutoLock WLAN	68
6.3.4	Wireless Distribution System (WDS)	70
6.3.5	Wireless ACLs	71
6.3.6	Wireless Client Bridge	71
6.3.7	Static Supervision	72
6.3.8	Static Routing	73
6.3.9	Static Source Routing	74
6.3.10	Selective Source Routing	75
6.4	Network Access Configuration	77
6.4.1	Authentication, Authorization and Accounting	77
6.4.2	WPA/802.1x Supplicant	88
6.4.3	IP Firewall	96
6.4.4	Bridging Firewall	107
6.4.5	SMTP Redirection	116
6.4.6	White/Black List	117
6.4.7	Static Bandwidth Control	119
6.5	Management Access Configuration	121
6.5.1	SSH Server	121
6.5.2	HTTP(S) Server	121

6.5.3	SNMP Agent.....	122
6.5.4	Network Usage Statistics	124
6.6	System Services Configuration	124
6.6.1	Manual Clock Regulation	124
6.6.2	NTP Client	125
6.6.3	Trace System.....	126
6.6.4	Syslog.....	126
6.6.5	IP Logging	127
6.6.6	Sysctl Plugin	128
7.0	Appendix.....	129
7.1	Appendix A: ShadowMaster Specifications	129
7.2	Appendix B: Regulatory Domain/Channels	130
7.2.1	Channels for IEEE 802.11b/g.....	130
7.2.2	Channels for IEEE 802.11a.....	131
7.3	Appendix C: Standard RADIUS Attributes	132
7.3.1	Vendor Specific Attributes.....	134
7.4	Appendix D: /etc/protocols	136
7.5	Appendix E: ISO Country Codes	139
7.6	Appendix G: Weather-Proofing	141
7.7	Appendix H: Factory Default Configuration File.....	143
8.0	Glossary	152
9.0	Index	157
10.0	Customer Support.....	160

Table of Figures

Figure 1.2.1: ShadowMaster Features.....	5
Figure 2.1.1: Fresnel Zone Clearance	6
Figure 2.2.1: IP 67 Components	7
Figure 2.2.2: IP 67 Assembly	7
Figure 2.2.3: Common Ethernet Termination Standards	8
Figure 2.2.4: Tightening the End Cap	8
Figure 2.3.1: Factory Default Configuration	9
Figure 2.4.1: Network Connections Window.....	10
Figure 2.4.2: Network Connection TCP/IP Settings.....	11
Figure 2.4.3: Administrator Login Screen	12
Figure 2.4.4: Enabling the Wireless Network Connection	12
Figure 2.4.5: List of Wireless Connections	13
Figure 2.5.1: Device License Page	13
Figure 2.5.2: Successful Upload Screen.....	14
Figure 2.5.3: Maintenance Screen	14
Figure 2.5.4: System Information Screen	14
Figure 3.3.1: CLI Login.....	16
Figure 3.3.2: Main CLI Commands	16
Figure 3.4.1: The authcheck Command's Parameters	16
Figure 3.5.1: Change the Administrator's Password.....	17
Figure 3.6.1: Start System Shell	17
Figure 3.8.1: Device Statistics	18
Figure 4.1.1: Main ShadowMaster Management Menu	19
Figure 4.2.1: System Information	21
Figure 4.2.2: Wireless Details	23
Figure 4.2.3: Table of Routes	24
Figure 4.2.4: ARP Table.....	24
Figure 4.3.1: Configuration Starting Page.....	25
Figure 4.3.2: Starting Point Page	26
Figure 4.3.3: Basic Network Page	27
Figure 4.3.4: Basic Wireless Page.....	28
Figure 4.3.5: DHCP Server Subsection	30
Figure 4.3.6: Static Routing Subsection.....	30
Figure 4.3.7: Wireless Security Page.....	31
Figure 4.3.8: Edit Configuration File Manually	32
Figure 4.4.1: System Menu.....	33
Figure 4.4.2: Maintenance Page	33
Figure 4.4.3: Change the Administrator's Password.....	34
Figure 4.4.4: Remote Management Page.....	35
Figure 4.4.5: Device License Page	36
Figure 4.5.1: Tools Menu	37
Figure 4.5.2: Site Survey Table	38
Figure 4.5.3: Antenna Alignment Tool	38
Figure 4.5.4: Rates Test.....	39
Figure 4.5.5: ACK Timeout Test	39
Figure 4.5.6: Throughput Test subsection	40
Figure 4.5.7: Wireless Test Results	41
Figure 4.6.1: Logout from the Web Management	41
Figure 5.4.1: SNMP Network	43
Figure 6.4.1: Traffic Limitation.....	120

Figure 7.6.1: Properly taped Ethernet adapter.....	142
Figure 7.6.2: Properly taped external antenna port.	142

This Page is Left Intentionally Blank

Purpose

This document provides information and procedures on setup, configuration, and management of the ShadowMaster Multi-Radio AP/Repeater. The ShadowMaster is a basis for the implementation of a wide variety of secure wireless and wired networking devices: routers, bridges, Access Points (AP), and Access Controllers (AC) for public access areas. The ShadowMaster-based AC implementation should include all the functionality of the ShadowMaster software and is the focus of this book.

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:



Additional information that may be helpful though 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 guide please send e-mail directly to support@waveteq.com.

ShadowMaster/Waveteq Technical Support

If you encounter problems when installing or using this product, please contact support@waveteq.com

1.0 Chapter 1 - Overview

Introduction

Thank you for purchasing the Waveteq ShadowMaster. The dual radio design allows installation in a variety of configurations, including as a true repeater, an access point with integrated backhaul and as dual access points. Unique features such as an integrated backhaul antenna and enclosure with mounting brackets will allow the ShadowMaster to fit into your network at the lowest cost possible, without sacrificing performance or quality.

Authentication, Authorization & Accounting

The ShadowMaster supports multiple secure authentication methods, including MAC authentication to 802.1x/EAP authentication with passwords, certificates or SIM cards. The integrated real-time accounting system is based on industry standard RADIUS/EAP and supports various billing plans: prepaid, pay-per-time, per-volume, per-use or flat rate. Integration into existing Operation Support Systems (OSS) and Business Support Systems (BSS) can be done with ease.

Remote Control

The ShadowMaster based device is placed at the edge of a broadband access network and allows operators to provide cost-effective, public Wi-Fi® services by managing per-user access control, device configuration, and radio performance from the operations center. HTTPS, SSH and SNMP agents can be used for secure remote management.

Privacy

The ShadowMaster supports different levels of security and data encryption: WEP/WPA/WPA2, Dynamic Key, 802.1x Authenticator and Supplicant. Device security settings can be configured per BSSID basis. Client stations can be separated on the data link layer (Layer 2 User Isolation), preventing intruders from accessing the computers of the other users. User credentials (passwords) are protected by SSL or EAP-based authentication methods. User traffic can be encrypted either by VPNs (pass-through) or by Wi-Fi® Protected Access (WPA).

1.1 ShadowMaster Features

Supported Standards

- IEEE 802.11a/b/g
- IEEE 802.11i
- IEEE 802.11d – Country element support
- IEEE 802.11e – Enhancement: QoS, including packet bursting (WMM)
- IEEE 802.11h – 5 GHz spectrum, DCS/DFS, TPC
- IEEE 802.11j – Security and Public safety band support

Hardware Configuration

- 802.11a/b/g operation on 2 distinct radio channels
- Cast aluminum custom enclosure
- Integrated 5 GHz antenna
- Low loss N-Type connectors
- Ingress Protection (IP) rating 67 Field Attachable Ethernet Connectors

Wireless Functionality

- Virtual AP (MBSSID) with individual wireless security settings
- Multiple wireless interfaces
- Association limitation per Virtual AP (MBSSID)
- Automated channel selection
- Antenna diversity control
- Output power control
- Wireless distribution system (WDS)
- Open client mode
- Secure client mode with WEP, WPA, WPA2 PSK and enterprise (dynamic key) with 802.1x supplicant
- WPA2 pre-authentication support
- Half and quarter rate channel support
- FCC security band support

Wireless Security

- WPA/WPA2 personal and enterprise (with dynamic key from remote RADIUS server) TKIP, AES (CCMP)
- Secure WDS mode, WDS inter access point traffic is secured by WPA/WPA2 in personal or enterprise modes
- Static and dynamic WEP
- 802.1x with EAP-MD5, EAP-TLS, EAP-PEAP, EAP-TTLS, EAP-SIM, EAP-LEAP
- Layer 2 intra access point client isolation
- SSID broadcasting suppression
- Static wireless Access Control List, MAC address filtering

Networking

- Static and dynamic VLAN tagging, up to 4096 VLAN tags, VLAN pass-through
- Bridging, spanning tree protocol (STP)
- Static and dynamic IP routing with Quagga Routing Suite
- DHCP server, client, relay

- DNS relay/proxy
- NTP and internal clock support
- Per VLAN, Virtual AP (MBSSID), IP tunnel or physical interface networking settings
- 802.1x authenticator and supplicant
- IP and MAC filtering per interface
- IP filtering per interface
- Stateful inspection firewall with P2P traffic matching module
- IPSec with static keys and dynamic re-keying, hardware acceleration for IXP-42x platform
- Multiple GRE tunnels
- NAT/NAPT/ IP masquerading per interface and VLAN/Virtual AP (MBSSID)
- Diffserv with 802.1p mapping for WMM queues
- PPPoE client

Public Access

- WEB login redirection (captive portal) with HTTP proxy support and multiple/selective authentication methods PAP/CHAP/MSCHAP/MSCHAPv2)
- RADIUS and MAC authentication
- SMTP redirection
- Static and dynamic white and black lists
- RADIUS client has support for multiple authentication and accounting RADIUS servers
- RADIUS accounting client supports fail over and backup modes
- RADIUS authentication client supports fail over mode
- Per virtual AP (MBSSID) RADIUS, DHCP and NAT configuration
- WISPr RADIUS attributes support with per user dynamic bandwidth management
- Static bandwidth control (w/o RADIUS)

Management

- WEB management via HTTPS
- Command line management via SSH and serial console
- Configuration file upload via HTTPS and SFTP
- Firmware management and status reporting agent with NAT/firewall traversal functionality
- Subnet or VLAN for management traffic
- Management access control list
- Administrator authentication via RADIUS or TACACS
- SNMP V1/2/3
- SNMP Traps
- Supported MIB's: 802.11, 802.1x, MIBII, RADIUS authentication, RADIUS accounting
- SYSLOG support including remote servers and debug levels
- Dual firmware images and TFTP firmware recovery from boot loader if both firmware images were damaged

Management Options

The ShadowMaster can be monitored or managed through the following interfaces:

- Command Line Interface (CLI) (refer to Chapter 3 – Command Line Interface Management)
- Web browser interface (refer to Chapter 4 – Web Interface)
- Simple Network Management Protocol (SNMP v1, v2, v3) (refer to *Chapter 5 – SNMP Management*)
- Local SYSLOG facility with logging to remote server

Package Contents

Each ShadowMaster comes with the following:

- ShadowMaster Radio
- Wall Plug AC Adapter
- Passive Power Over Ethernet (PPoE) Injector
- 2 U-Bolts (plus 2 washers and 2 hex nuts)
- 2 Field Attachable IP67 Ethernet Connectors
- Self-Seal Tape
- 1 Ethernet Dust Cover
- ShadowMaster Quick Start Guide
- Documentation CD



If any of these items are missing or damaged, please contact Waveteq or a local Waveteq sales representative.

1.2 Feature Locations

Please see Figure 1.2.1 for a look at the location of the ShadowMaster's exterior features. Also, please note the following regarding these features:

- Features 1 and 2, which are Ethernet ports #1 and #2, will be referred to throughout the manual as `ixp0` and `ixp1`, respectively.
- Feature 3, which is the N connector port to Radio 1, will be referred to throughout the manual as `ath0`.
- Feature 4, which is the N connector port to Radio 2, will be referred to throughout the manual as `ath1`.

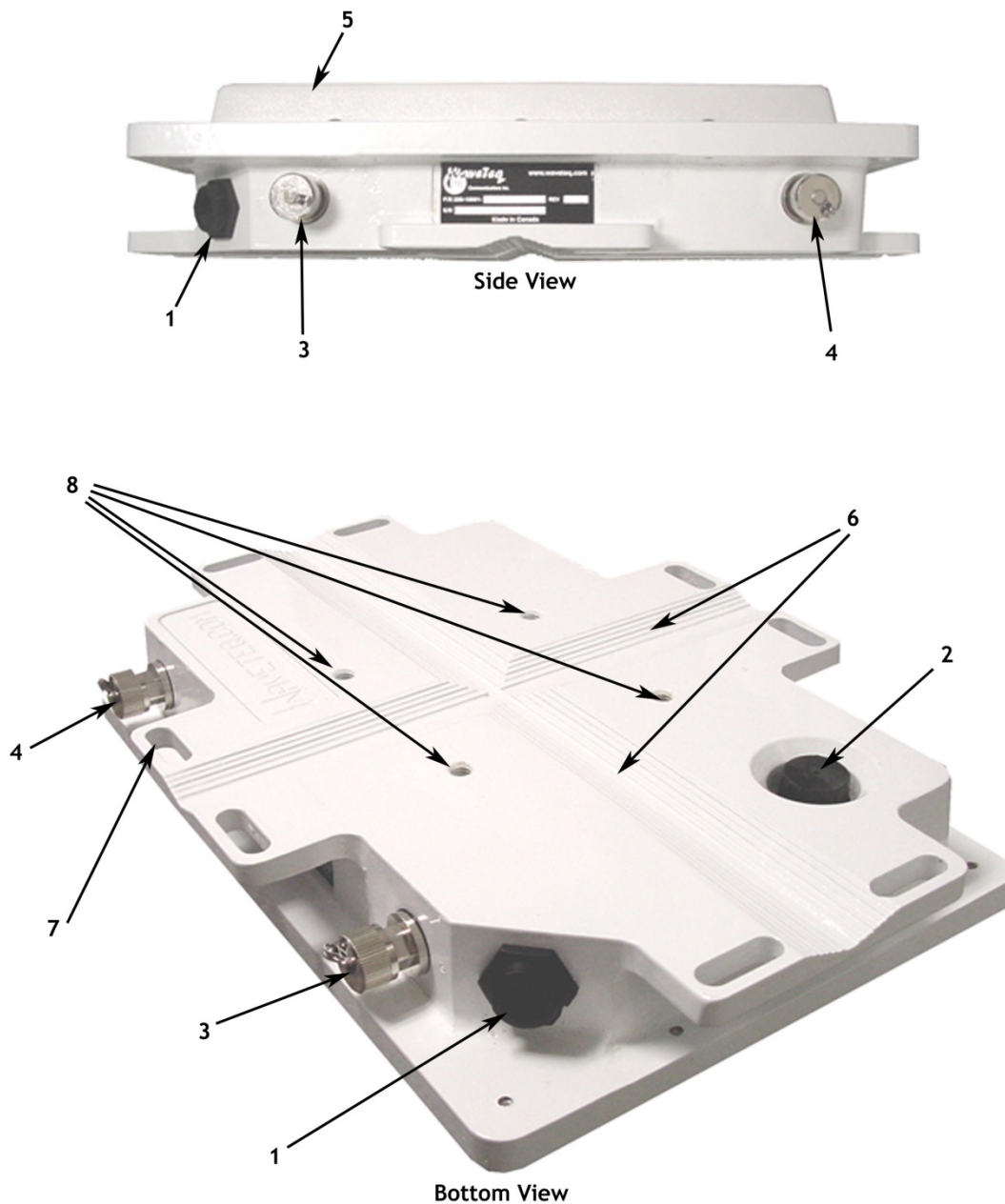


Figure 1.2.1: ShadowMaster Features

- | | |
|--|---|
| 1 – Ethernet Interface #1, IP 67 Rated (ipx0) | 5 – Radio 1's Integrated 5.8 GHz, 16.8 dBi Antenna |
| 2 – Ethernet Interface #2, IP 67 Rated (ipx1) | 6 – Pole Mounting Grip Groove for H&V Polarized Mounting |
| 3 – Radio 1, N RF Connector (ath0) | 7 – Mounting Flanges for Pole or Wall Mounting |
| 4 – Radio 2, N RF Connector (ath1) | 8 – Holes for Optional Mounting Kits |

2.0 Chapter 2 - Installation

The ShadowMaster can be installed in a variety of configurations: as an Access Point (AP) with an integrated backhaul radio, as two independent AP's, or as a true repeater with a separate radio device for each portion of the link. In a standard Waveteq ShadowMaster box there are the following: 1 ShadowMaster, 1 Passive Power over Ethernet Injector (PPoE), 1 wall plug AC adapter, 2 U-bolts (plus 2 washers and 2 hex nuts), 2 field attachable IP67 connectors, 1 Ethernet Dust Cover, self-seal tape, 1 ShadowMaster Quick-Start Guide and a documentation CD..

2.1 Mounting

The ShadowMaster should be mounted in a manner so that its antennas have a line of sight to their respective targets. This is less of a necessity when using an Omni-directional antenna. The ShadowMaster has been designed to allow for simple pole mounting; it can be mounted to any pipe or pole with diameters ranging from 1.5 to 3.5 inches (4 cm – 9 cm). There are teeth built into the enclosure to allow low slippage mounting in either the horizontal or vertical polarization configurations.

True Line of Sight (LoS) between two radios is not quite as straight-forward as typically thought. Line of sight requires at least two conditions:

1. The two antennas can be connected with an imaginary straight line with no objects obstructing this line.
2. There needs to be a clear, elliptical area surrounding the visual path known as the Fresnel zone. Without the Fresnel zone clearance, an object may cause diffraction effects that will degrade the signal. The required clearance can roughly be computed by:

$$r = C \sqrt{\frac{D}{4f}}$$

C = 8.66 in metric (or 36.025 for imperial)
D = total distance in kilometres (or miles)
f = frequency in gigahertz
r = radius in meters (or feet)

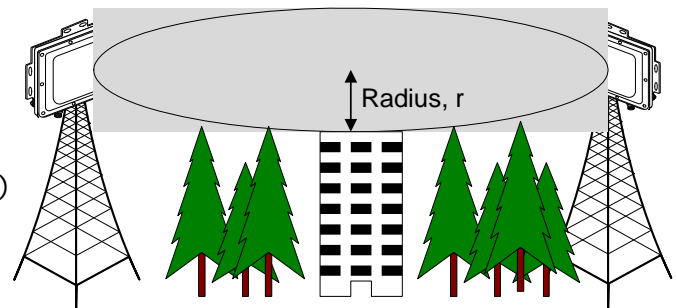


Figure 2.1.1: Fresnel Zone Clearance

While true line of sight is difficult to achieve, the requirements should be kept in mind so that the mounting point can best be determined in order to achieve at least 60% Fresnel Zone clearance. Reduced Fresnel Zone clearance will contribute to an increased noise floor, thereby decreasing the Signal-to-Noise ratio. Once the ShadowMaster has been mounted, a site scan should be performed to adjust the aim of the antenna to achieve the best possible alignment. For more details on antenna alignment, please see section 4.5.2.

The ShadowMaster is designed to be weatherproof, but under certain circumstances it can be recommended that additional weather-proofing be applied to the connectors once the ShadowMaster has been mounted and connections have been completed. For more details, please see section Appendix G: Weather-Proofing.

2.2 Ethernet Cable and Connector Assembly

The field attachable connectors are IP-67 rated to prevent 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 ShadowMaster. Referring to Figure 2.2.1 throughout, please follow the steps below to install the connector to your cable.

3. Start with an outdoor rated Ethernet cable that is of sufficient length to reach the installation of the Waveteq ShadowMaster. Allow several extra feet in case of future movement. The cable should not exceed 100m.
4. Carefully strip off approximately 1.5" of the cable shielding using a small knife or crimping tool.
5. Fan the wires of the cable, untwisting them until they are straight up to where the shielding was removed.
6. Starting with (6) in, slide each of (6), (5), (4), and (3) over the cable sheath from the end with the exposed wire, as in Figure 2.2.2.

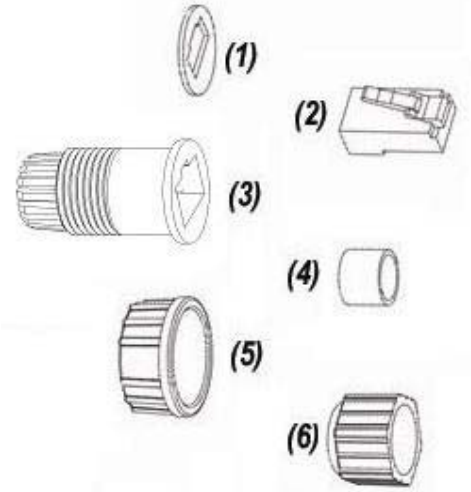


Figure 2.2.1: IP 67 Components

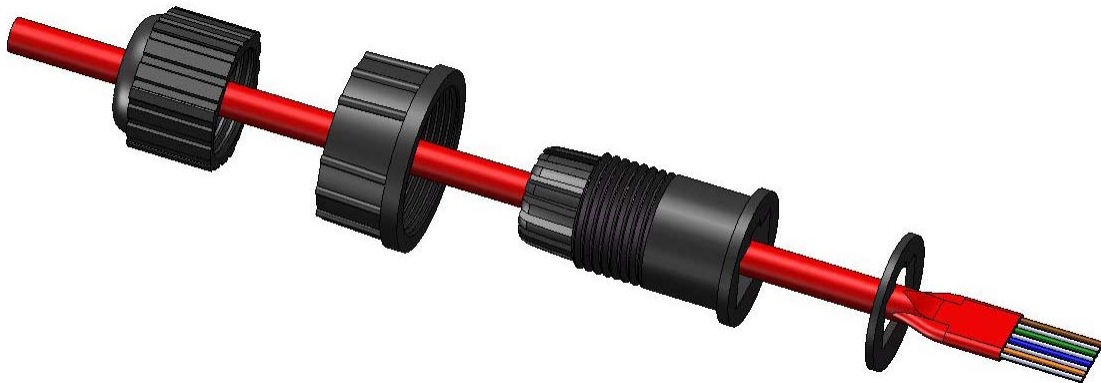


Figure 2.2.2: IP 67 Assembly

7. Slide the wires in the proper order into the RJ-45 terminator plug (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 2.2.3.



If proper wiring sequences are not used to terminate the cable, malfunction and - in this case, because of the Passive Power over Ethernet (PPoE) technology - damage to your equipment can result.

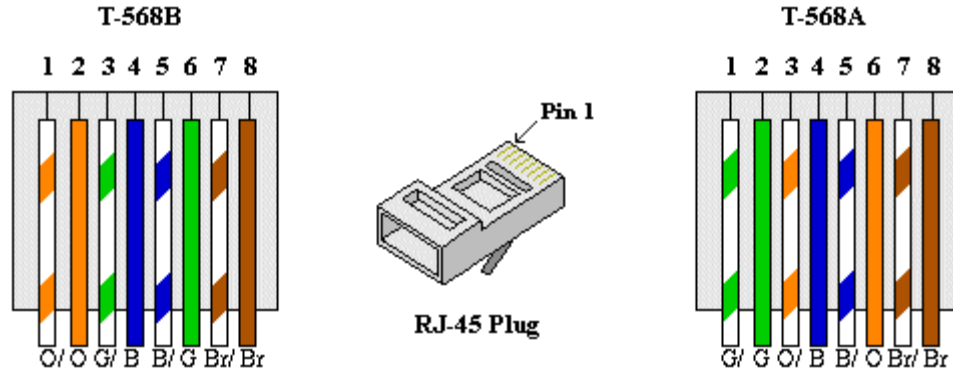


Figure 2.2.3: Common Ethernet Termination Standards

8. Push the wire bundle into the back of the RJ-45 terminator plug (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 wires are all flush with the back wall of the housing; the wires must go in past the pins in order to make a proper connection.
9. Using a RJ-45 hand crimper, crimp the assembly together.
10. Move the coupler (5) over the plug holder (3) until it bottoms out.
11. Seat the thick ring (4) inside the cable clinch (3)
12. 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.



13. 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
14. Figure 2.2.4. This will cause the cable clinch to tighten around the cable, providing a waterproof seal. A small wrench may be used to further tighten.
15. Carefully remove the backing from the plug gasket (1).
16. Stick the plug gasket (1) onto the face of the plug holder (3), ensuring proper orientation and that the sticky side is facing the plug.

Figure 2.2.4: Tightening the End Cap

To power the ShadowMaster, you will require the (included) Ppoe injector, an Ethernet cable and the AC adaptor. Note that none of these devices are waterproof and it is **STRONGLY RECOMMENDED** that they be installed in a watertight, enclosed space. To power on the ShadowMaster it is necessary to connect your Ethernet cable directly from the power port of the Ppoe Injector to the main RJ-45 port of the ShadowMaster. Note that the end attached to the ShadowMaster should have the field attachable connector on it. Next, plug the AC adaptor into the wall and the DC jack into the Ppoe injector.

To connect the ShadowMaster to a computer use a CROSS OVER CABLE from the LAN port of the Ppoe to the Ethernet port of the computer. To connect to a network device like a hub/router/switch use instead a STRAIGHT THROUGH cable.



When connecting a computer, router, hub or switch to the ShadowMaster through the PpOE, ensure you are doing so through the “LAN” RJ45 Port! The “PoE” port outputs passive DC power intended for the ShadowMaster, and will damage most other Ethernet ports.

Power to the ShadowMaster unit is indicated when the link light on the Ethernet port of the computer, hub or modem is enabled. Note that the default IP address of the Ethernet #1 (ixp0 for short) port is 192.168.3.1 and connecting it to a network with another device with the same IP address WILL CAUSE PROBLEMS. Once this cable is set up it is possible to configure the ShadowMaster; see other sections on details pertaining to software setup.

2.3 Factory Default Configuration

By default, the ShadowMaster is configured to operate as an access point by transparently bridging the Ethernet port (ixp0) to the internal 5 GHz antenna (ath0) as shown in the figure below:

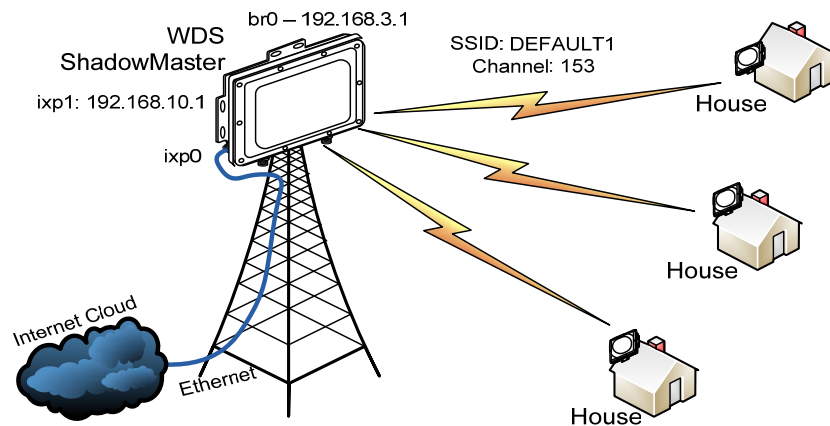


Figure 2.3.1: Factory Default Configuration

The bridge IP address (192.168.3.1) is only for administrative purposes so that the user can login and reconfigure the radio through either the ixp0 interface or the wireless (ath0) interface on the DEFAULT1 SSID. For more details regarding the default configuration on the ShadowMaster, please refer to Appendix H: Factory Default Configuration File.

2.3.1 Emergency IP

In case of a configuration error or forgetfulness, you may not be able to connect to the ShadowMaster as expected. 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 ShadowMaster.



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.

2.4 Connecting to the ShadowMaster

Connection to the ShadowMaster based device can be made using the wireless or Ethernet interfaces. The next sections outline the instructions on how to access the ShadowMaster based device management interfaces.

2.4.1 Using Ethernet Connection

Dynamic Host Configuration Protocol (DHCP) is not enabled on the Ethernet ports by default, so the ixp0 port on the ShadowMaster will initially only respond to the default static IP address 192.168.3.1. All installation steps refer to the users using the Windows XP operating system, although procedures for other operating systems may be similar. Use the following procedure to access the ShadowMaster Web management pages via the ixp0 interface, assuming it is using its default settings:

Step 1 Connect the Ethernet cable from the LAN port of the PPoE Injector to your computer.

Step 2 Setup the network adapter on your computer (Go to **Start>Settings>Network Connections>**Right click on **Local Area Connection** and select **Properties**):

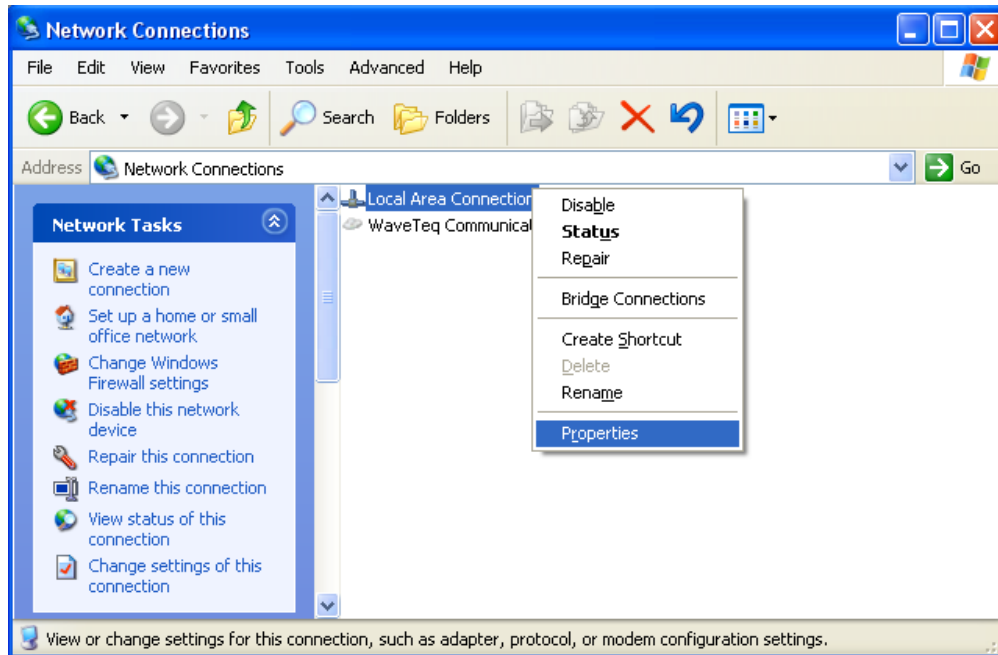


Figure 2.4.1: Network Connections Window

- Step 4** Access the network adapter's TCP/IP settings (choose **Internet Protocol (TCP/IP)** and click **Properties**).
- Step 5** Manually assign the host an IP address that ranges within the ShadowMaster's IP's subnet. The default subnet for the bridge interface on ath0 ranges from 192.168.3.1 to 192.168.3.254. Enter an IP address different from the ShadowMasters address (i.e. 192.168.3.100), and the subnet mask as 255.255.255.0:

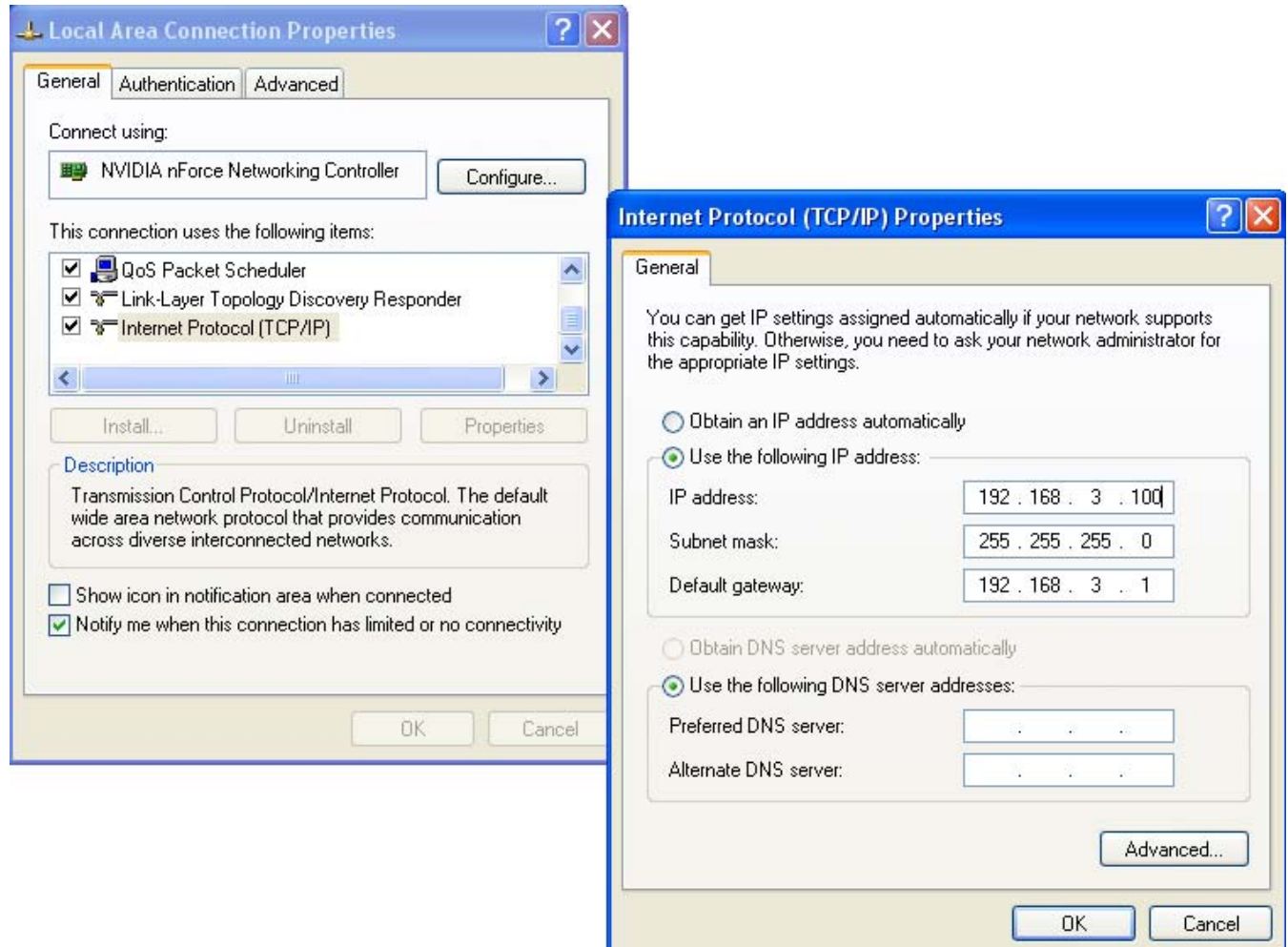


Figure 2.4.2: Network Connection TCP/IP Settings

- Step 5** Open a Web browser and type the default IP address of ixp0 on the ShadowMaster, <http://192.168.3.1/>. After the connection has established, you will see the Web User Interface.



Figure 2.4.3: Administrator Login Screen

Step 6 Enter the administrator login details to access the web interface, as in Figure 2.4.3:



The default administrator login settings for all ShadowMaster interfaces are:

User Name: **admin**

Password: **admin01**

Step 7 After successfully logging in as the administrator, you will see the main page of the ShadowMaster device Web management interface. The ShadowMaster device is now ready for configuration. For further instructions on Web management refer to *Chapter 4 – Web Interface*.

2.4.2 Using Wireless LAN Connection

By default the ShadowMaster based device does not run a DHCP server on any of its interfaces. ath0 is bridged to device ixp0 and therefore will respond to the static IP address 192.168.3.1.

Use the following procedure to access the ShadowMaster based device Web management pages via wireless interface. All installation steps refer to the users using Windows XP and other Windows versions accordingly, and assume that a wireless networking device is already installed on the computer.

Step 1 Follow steps 1-4 from 2.4.1 - Using Ethernet Connection, modifying your **Wireless Network Connection** instead of your **Local Area Network Connection**.

Step 2 If not already done, enable the wireless network connection:

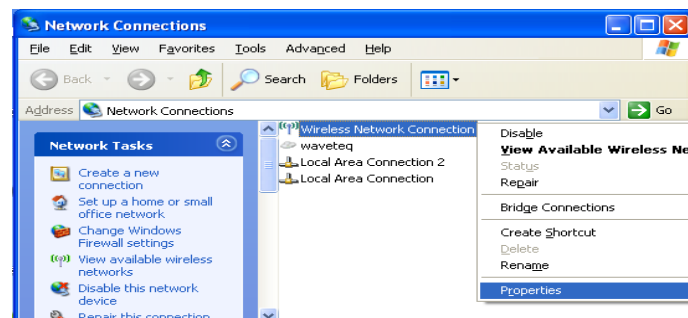


Figure 2.4.4: Enabling the Wireless Network Connection

- Step 7** Choose the ShadowMaster device's SSID from the list of available wireless networks. The default SSID is DEFAULT1 for the xip0/ath0 bridge, using channel 153 on the 802.11a (5.765 GHz) band.



Figure 2.4.5: List of Wireless Connections

- Step 8** Repeat steps 5-7 from section 2.4.1. For further instructions on Web management refer to Chapter 4 – Web Interface.

2.5 Licensing

The ShadowMaster firmware you have purchased includes a free 1 year upgrade licence. A valid license file should already be loaded on your ShadowMaster device when you received it. If for some reason it is not present, please contact Waveteq immediately.

A valid license file should be uploaded on the ShadowMaster based device to activate a full set of the device features. Use the following procedure to upload a new license file onto the ShadowMaster based device using web interface:

- Step 1** Connect to the ShadowMaster web interface and choose **System | License** menu:

Device License

License status	not valid
License period	N/A
Download current license file	<input type="button" value="Download"/>

Upload New License

License file upload	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>
----------------------------	----------------------	--	---------------------------------------

Figure 2.5.1: Device License Page

- Step 2** Use the **Browse...** button to choose the license file and click the **Upload** button under **Upload New License** section to load the file on the system. Be certain you are uploading a valid license file.

- Step 3** After the license file has been successfully uploaded to the device, the information message appears:

License uploaded and saved. License will be activated after reboot.

Device License

License status	not valid
License period	N/A
Download current license file	Download

Figure 2.5.2: Successful Upload Screen

- Step 4** Use the Reboot section under the **System | Maintenance** menu to **reboot** the device for all locked features to be activated.

Reboot

Reboot device [Reboot](#)

Figure 2.5.3: Maintenance Screen

- Step 5** After the license is uploaded and the device has rebooted, check the license validity on the Web management interface under **Statistics | System Information** menu:

System Information

Uptime	00:07:58
License status	valid
Firmware version	v5.21

Check the license validity

Figure 2.5.4: System Information Screen

3.0 Chapter 3 - Command Line Interface Management

3.1 Introduction

The CLI (Command Line Interface) software is a configuration shell for the ShadowMaster based device. CLI is an alternative way for configuring the device. It is not intended to be a main device managing method. Using the CLI, the operator can test authentication parameters, change the administrator's password, reboot the device, reset the device to defaults, show the device configuration or view the device status.

All available key combinations in CLI mode are listed in Table 3.1.1.

Table 3.1.1 - Key Combinations in the CLI:

Key and/or Combination	Function
"<text>"	Enter parameter's string with space
<TAB>	Complete current keyword or list all the options
<CTRL>+<D>	Break out of subshell
<CTRL>+<A>	Jump to the beginning of the line
<CTRL>+<E>	Jump to the end of the line
<CursUP>/<CursDOWN>	Scroll through the history of commands

3.2 CLI Access

Use a SSH client application (e.g., Tera Term <http://tssh2.sourceforge.jp/> or PuTTY <http://www.putty.nl>) to access the CLI of the ShadowMaster based device.



Make sure that the SSH server is configured properly (see chapter *SSH Server*)

Default ShadowMaster configuration has the DHCP client disabled on the WAN interface. The device IP address will be, by default, 192.168.3.1. When connected, the login prompt will be displayed.

3.3 Login

Enter the administrator login settings on the displayed command prompt.



Default administrator login settings are:

User Name: **admin**

Password: **admin01**



Change the default administrator password as soon as possible.

```
login as: admin
admin@192.168.2.235's password:
CLI version 1.0
```

Figure 3.3.1: CLI Login

After a successful login a list of available commands followed by CLI command prompt will be displayed.

```
Available commands:
authcheck  - Test authentication config
passwd     - Change any administrator password
reboot     - Reboot device
reset      - Reset device to defaults
shell      - Start system shell
show       - Show device configuration
status     - Show device status
quit       - Exit CLI
cli> █
```

Figure 3.3.2: Main CLI Commands

3.4 Authentication Check

With the **authcheck** command you can test configured authentication settings. To get a list of available command parameters type 'authcheck' and press enter:

```
cli> authcheck
Usage: authcheck <options>

options:
-i <interface name> - mandatory
-m <MAC address> - optional, taken from interface by default.
-u <username> - optional, default: test
-p <password> - optional, default: test
-t <timeout in milliseconds> - optional, default: 30000
```

Figure 3.4.1: The authcheck Command's Parameters

The **authcheck** command requires interface name parameter to be specified. Other parameters are optional.

Example:

```
authcheck -i ath0 -u testuser -p testpass
```

will try to authenticate with username *testuser* and password *testpass* on local interface called *ath0*.

Test result will be displayed immediately after command execution.

3.5 Password

With the **passwd** command you can change the administrator's password. To change password you will need to provide the old and the new passwords:

```
cli> passwd
Changing password for administrator: admin
Enter old password:
Enter new password:
Confirm new password:
Command executed successfully.
```

Figure 3.5.1: Change the Administrator's Password



Passwords will not appear on the screen for safety.



The only way to gain access to the management tool if you forget the administrator's password is to send your ShadowMaster back to Waveteq Communications.

3.6 Shell

shell starts UNIX Bourne like system shell for the administrator.

```
cli> shell
Launching system shell.
Enter 'exit' or Ctrl-D to return from shell.

BusyBox v1.5.0 (2007-08-02 10:43:25 EEST) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

# █
```

Figure 3.6.1: Start System Shell

Type exit or press Ctrl + D key combination to quit the shell and return to CLI interface.

3.7 Show

The **show** command displays the current system configuration file.

3.8 Status

The **status** command displays general device status (device type, firmware version, hardware revision, uptime, memory, average load) and receive/transmit statistics for all interfaces.

```
cli> status
Current system status:
Device name:      WILI-S
Firmware version: WILI-S.COYOTE.v3.50.xscale.ath.wilibox.7323.051011.1432
Hardware revision: XScale-IXP425 rev 1 (v5b)
Uptime:          00:17:48
System memory:    Total: 62712 kB, Free: 47260 kB
Average load:     1min: 1.99 5min: 1.93 15min: 1.35
Licensing:
License status:   valid
License period:   2005-01-01 to 2005-12-31
Network configuration:
Interface        | MAC address      | IP address      | Netmask
-----|-----|-----|-----
ixp0             | 00:90:4B:69:46:9E | 192.168.3.1    | 255.255.255.0
ixp1             | 00:90:4B:69:46:9F | 192.168.2.221  | 255.255.255.0
ath0             | 00:90:4B:CC:74:F9 | 192.168.4.1    | 255.255.255.0
Network statistics:
Interface|      bytes      | Receive statistics |      bytes      | Transmit statistics
-----|-----|-----|-----|-----|-----|-----|-----|-----|
Interface|      bytes      | packets errors drop |      bytes      | packets errors drop
-----|-----|-----|-----|-----|-----|-----|-----|
lo|          0          | 0 0 0 0 |          0          | 0 0 0 0
tunl0|          0          | 0 0 0 0 |          0          | 0 0 0 0
gre0|          0          | 0 0 0 0 |          0          | 0 0 0 0
ixp0|          0          | 0 0 0 0 |          0          | 0 0 0 0
ixp1|       162626       | 1977 0 0 0 |       73207        | 286 0 0 0
ath0|          0          | 0 338 0 0 |          0          | 0 0 0 0
uat0|          0          | 0 0 0 0 |          0          | 0 0 0 0
```

Figure 3.8.1: Device Statistics

3.9 Reboot

Type **reboot now** to immediately reboot the ShadowMaster.

3.10 Reset

To reset the ShadowMaster device to factory defaults, use the **reset** command. The device is restarted and default values are set.



Please note that the administrator password will be set to the factory default.

3.11 Quit

Type **quit** to leave the **CLI** mode.

4.0 Chapter 4 - Web Interface

The ShadowMaster's Graphical User Interface (GUI) is presented after connecting to the device through a web browser. From the web interface, all administrative details and configuration options may be accessed. For details on connecting to the ShadowMaster device, see section 2.4 *Connecting to the ShadowMaster*.

4.1 Overview

The main web management menu is displayed after successfully logging into the system (see Figure 4.1.1 below). From this menu all administrative pages are accessed.

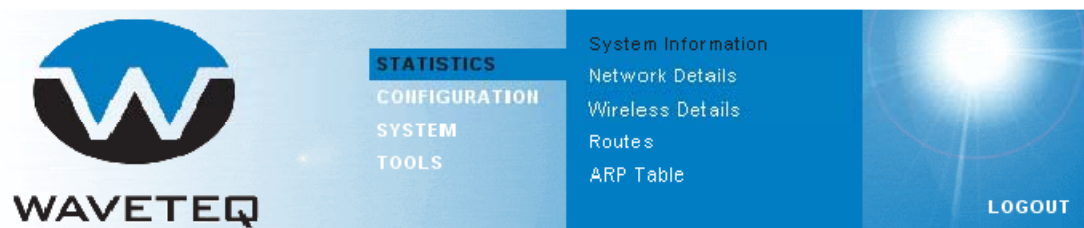


Figure 4.1.1: Main ShadowMaster Management Menu

By default the **Statistics | System Information** menu is activated and the main ShadowMaster device system information is displayed. The active menu is displayed in a different color.

The web management menu has the following structure:

Statistics

- System Information** – displays general information about the ShadowMaster device.
- Network Details** – displays main network statistics for the ShadowMaster device.
- Wireless Details** – displays wireless statistics for the ShadowMaster device.
- Routes** – displays route table for the ShadowMaster device.
- ARP Table** – displays ARP table for the ShadowMaster device.

Configuration

- Starting Point** – choose from a variety of commonly implemented configuration files.
- Basic Network** – set up network interfaces, static DNS servers, and bridging configuration.
- Basic Wireless** – define radio and wireless configuration.
- Advanced Network** – define DHCP and DNS server status, as well as static routing rules.
- Advanced Wireless** – setup wireless security (WEP, WPA, WPA2, access control lists).
- Expert** – manually edit the configuration file.

System

- Maintenance** – upgrade with a new firmware, reboot or reset to factory defaults.
- Password** – change administrator's password.
- Remote Management** – configure administrative access and monitoring of the ShadowMaster.

License – license file validity and upload on the ShadowMaster device.

Tools

Site Survey – perform a site evaluation to show overview information for other wireless networks in the local geography.

Antenna Alignment – measures signal quality between wireless devices.

Wireless Tests – perform a wireless throughput test between two ShadowMasters.

In the following sections, short references for all menu items are presented.

4.2 Statistics

Use the **Statistics** menu to check the current status of the ShadowMaster. There are five sections of the status information:

- **System Information** – displays system information including uptime, and version.
- **Network Details** – detailed receive/transmit statistics for all interfaces.
- **Wireless Details** – detailed radio and wireless network statistics.
- **Routes** – displays routing information.
- **ARP Table** – displays the ShadowMaster's ARP table (IP addresses associated with MAC addresses).

4.2.1 System Information

System Information menu displays general device status, as well as network and wireless information. This is the default page shown when accessing the ShadowMaster.

- **System Information** – displays system information including uptime, license status, and firmware version.
- **Network Information** – displays basic receive and transmit information. The table displays how many packets are sent and received, how many errors have occurred while communicating, and the IP address associated to each interface.
- **Wireless Information** – displays general wireless device information. The Status column shows if an interface is turned on, and the Link column shows the signal strength for the wireless link based on the current noise level.
- **Refresh** – click to renew the system information page.

System Information

Uptime	00:02:12
License status	valid
Firmware version	v5.22

Network Information

Interface	MAC Address	IP Address	RX Pkts	RX Errors	TX Pkts	TX Errors
Main Ethernet (ixp0)	00:D0:12:0D:A4:5C		223	0	277	0
Secondary Ethernet (ixp1)	00:D0:12:0E:A5:5D	172.31.1.1	0	0	6	0
Bridge (br0)	00:0B:6B:84:8B:1C	192.168.3.1	223	0	277	0

Wireless Information

Interface	SSID	IEEE Mode	Channel	Status	Link
Radio 1 (ath0)	DEFAULT1	A	153	up	0

[Refresh](#)

© 2008 WAVETEQ Communications Inc

Figure 4.2.1: System Information

4.2.2 Network Details

The Network Details page displays the main network configuration and receive/transmit statistics of all interfaces.

Network Statistics

Interface	Receive statistics				Transmit statistics			
	bytes	packets	errors	drops	bytes	packets	errors	drops
Main Ethernet	105928	757	0	0	105928	624	0	0
Back Ethernet	0	0	0	0	0	0	0	0
Radio 1	0	0	0	0	0	223	0	0
Radio 2	4540	33	0	0	4540	235	0	0
Bridge (br0)	94210	766	0	0	94210	590	0	0

Network Configuration

Interface	MAC address	IP address	Netmask	Broadcast
Back Ethernet	00:D0:12:13:46:73	172.31.1.1	255.255.255.0	172.31.1.255
Bridge (br0)	00:0B:6B:84:38:5E	192.168.3.1	255.255.255.0	192.168.3.255

[Refresh](#)

© 2008 WAVETEQ Communications Inc

Network Statistics – displays detailed receive and transmit statistics of each interface.

Network Configuration – displays the main parameters of the interfaces (MAC address, IP address, Netmask). The broadcast column

Refresh – click to renew network statistics information.

4.2.3 Wireless Details

The **Wireless Details** page displays the main statistics of wireless interfaces, including connectivity and associated devices (peers).

Wireless Statistics

Interface	Status	Link	Level	Noise	Invalid network ID	Decryption errors	Invalid fragments	Retry count	Miscellaneous errors	Missed beacons
Radio 1 (ath0)	up	0	160	160	45	0	0	0	0	0
Radio 2 (ath1)	up	30	190	160	2	0	0	0	0	0

Peers/Access-Points

Interface	Mode	HW address	Quality	Signal level	Noise level	Data rate
ath1	Master	00:0b:6b:36:b9:7e	30	-65 dBm	-96 dBm	36 Mbps

Radio Information

Country	CA				
Interface	MAC address	IEEE mode	Channel	ESSID	
Radio 1 (ath0)	00:0B:6B:84:38:5E	A	36	DEFAULT1	
Radio 2 (ath1)	00:0B:6B:84:39:51	G	1	DEFAULT2	

[Refresh](#)

© 2008 WAVETEQ Communications Inc

Figure 4.2.2: Wireless Details

Wireless Statistics – displays detailed statistics of each wireless interface.

Peers/Access-Points – displays detailed information about the associated stations (in master mode) or information about the device the ShadowMaster is associated with (managed mode).

Radio Information – displays the main information of the device radio.

Refresh – click to update wireless information.

4.2.4 Routes

The **Routes** page displays the routing table for each interface.

Routes

Interface	Destination	Gateway	Netmask	Flags
Bridge (br0)	192.168.3.0	0.0.0.0	255.255.255.0	U
Back Ethernet	172.31.1.0	0.0.0.0	255.255.255.0	U

Refresh

Figure 4.2.3: Table of Routes

Destination – The subnet that doesn't exist on the ShadowMaster but can be found through the associated gateway address.

Gateway – The IP address of the device connected to the ShadowMaster that can help find the desired destination IP address.

Netmask – Specifies which part of the IP addresses is the subnet, and which part is the destination machine.

Flags – Displays the status of the route. **U**: route is up, **H**: target is a host, **G**: use gateway, **R**: reinstate route for dynamic routing, **D**: dynamically installed by daemon or redirect, **M**: modified from routing daemon or redirect, **A**: installed by addrconf, **C**: cache entry, **!**: reject route

Refresh – click to renew information in table of routes.

4.2.5 ARP Table

The **ARP Table** page displays the table of ARP (Address Resolution Protocol) entries. ARP is primarily used to translate IP addresses to Ethernet MAC addresses.

ARP Table

Interface	IP address	HW type	Flags	HW address
Bridge (br0)	192.168.3.175	0x1	0x2	00:17:31:46:9B:BE

Refresh

Figure 4.2.4: ARP Table

IP address – The known IP address of the device hardware address.

Hardware Type – The hardware type distinguishes between Ethernet (1), IEEE 802 Networks (6), IPsec tunnels (31), etc.

Flags – ARP flags, most commonly 0x02 (ARP on Ethernet)

HW address – The hardware address of the device, most commonly a MAC address.

Refresh – click to update information in ARP table.

4.3 Configuration

Use the **Configuration** section to manage the device's configuration file. On each page, there are headings which offer helpful advice for adjusting different configuration options.



Figure 4.3.1: Configuration Starting Page

There are six sections of system configuration file management:

- **Starting Point** – choose from a variety of commonly implemented configuration files.
- **Basic Network** – set up network interfaces, static DNS servers, and bridging configuration.
- **Basic Wireless** – define radio and wireless configuration.
- **Advanced Network** – define DHCP and DNS server status, as well as static routing rules.
- **Advanced Wireless** – setup wireless security (WEP, WPA, WPA2, access control lists).
- **Expert** – manually edit the configuration file.

4.3.1 Starting Point

This section is for loading pre defined configuration files. These include the factory default, as well as other common basic configurations. Use the Network Diagram links to see a visual representation of each configuration. Figure 4.3.2 below shows the starting point page on the ShadowMaster web interface.

Factory Default

By default, the ShadowMaster is configured to operate as an access point by transparently bridging the Ethernet port (ixp0) to the internal 5 GHz antenna (ath0) while the second radio (ath1) is unused. [More Details](#)

[Network Diagram](#)
[Load 'Factory Default'](#)

Link & Cover

Link and Cover combines a point-to-point link (the 'link') with a point-to-multipoint link (the 'cover').

BRIDGED: ☐ Local ShadowMaster ☐ Remote ShadowMaster
ROUTED: ☐ Local ShadowMaster ☐ Remote ShadowMaster

[Network Diagram](#)
[Network Diagram](#)
[Load 'Link & Cover'](#)

Redundant Link

Redundancy in networks can be useful to help reduce downtime and improve the availability of communications networks. Creating two Wireless Distribution (WDS) links allows two separate paths in the event that one fails. [More Details](#)

☐ Local ShadowMaster ☐ Remote ShadowMaster

[Network Diagram](#)
[Load 'Redundant Link'](#)

Dual Access Point (AP)

Using both radios, the ShadowMaster can be configured to provide an Access Point for two different operational modes. By providing dual access, you can mix channels, authentication types and/or 802.11 modes. This example configures the ShadowMaster to deliver broadband access via both A and G 802.11 modes. [More Details](#)

[Network Diagram](#)
[Load 'Dual AP'](#)

Figure 4.3.2: Starting Point Page

Factory Default – click to load the Factory Default configuration file. By default, the ShadowMaster is configured as an access point by transparently bridging the Ethernet port to the internal 5GHz antenna.

Link & Cover – choose between bridged or routed Link and Cover setup. This combines a point-to-point link with a point-to-multipoint cover.

Redundant Link – Specify local or remote ShadowMaster for the Redundant Link configuration. A redundant link allows a double connection so that in the event that one fails, the other will take its place.

Dual Access Point – click to configure the ShadowMaster as a Dual Access Point. In this mode, the ShadowMaster can provide broadband access via both A and G 802.11 modes.

Expert Mode – click to upload a custom configuration file or to download the running configuration file. Multiple ShadowMasters can be quickly configured the same way by loading in the same configuration file into each device.

4.3.2 Basic Network

This section is for configuring the basic networking interfaces on the ShadowMaster. From this page, each interface can be set up as a DHCP client to obtain an IP address automatically, or it can be assigned a unique IP address. Static DNS servers and bridging devices may also be configured.

Basic Network

Save ?

IP Address Configuration

Main Ethernet (ixp0)

☐ Obtain an IP address automatically
 ☒ Use the following IP address

IP Address

0.0.0.0

IP Subnet Mask

255.255.255.0

☒ Enable Secondary Ethernet (ixp1)

☐ Obtain an IP address automatically
 ☒ Use the following IP address

IP Address

172.31.1.1

IP Subnet Mask

255.255.255.0

☒ Enable Radio #1 (ath0)

☐ Obtain an IP address automatically
 ☒ Use the following IP address

IP Address

0.0.0.0

IP Subnet Mask

255.255.255.0

☐ Enable Radio #2 (ath1)

☐ Obtain an IP address automatically
 ☒ Use the following IP address

IP Address

0.0.0.0

IP Subnet Mask

255.255.255.0

Default Gateway

DNS

☐ Enabled

DNS Server 1

DNS Server 2

Bridging

☒ Enabled

Bridge 0

Interfaces

☒ Main Ethernet (ixp0)
 ☐ Secondary Ethernet (ixp1)
 ☒ Radio #1 (ath0)
 ☐ Radio #2 (ath1)

IP Address

192.168.3.1

IP Subnet Mask

255.255.255.0

Bridge 1

Interfaces

☐ Main Ethernet (ixp0)
 ☐ Secondary Ethernet (ixp1)
 ☐ Radio #1 (ath0)
 ☐ Radio #2 (ath1)

IP Address

IP Subnet Mask

© 2008 WAVETEQ Communications Inc

Figure 4.3.3: Basic Network Page

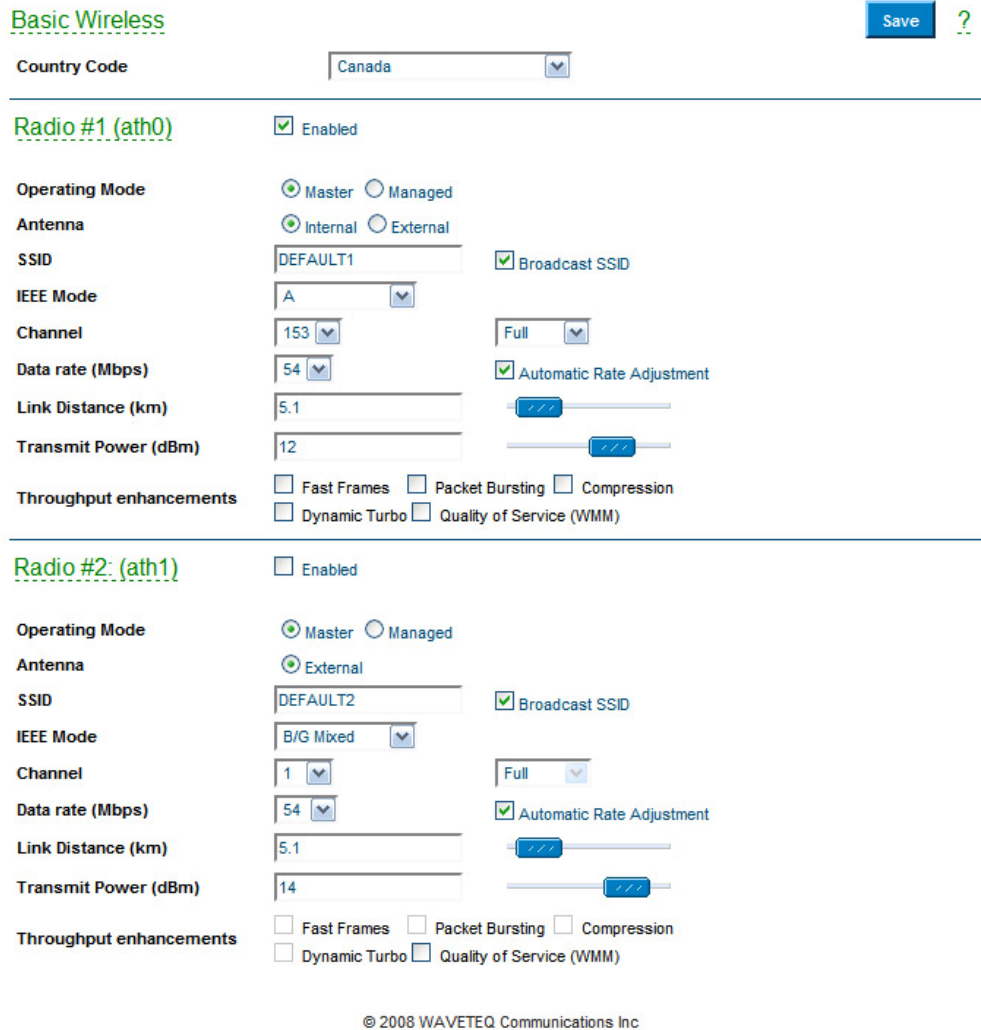
IP Address Configuration – For each of the interfaces, specify “Obtain an IP address automatically” to enable it as a DHCP client (see section 6.2.3.1 *DHCP Client* for details), or else specify a static IP address and subnet mask. Be sure to enable each device in use. You can also specify a default gateway IP address for the ShadowMaster.

DNS – Use this section to enable and configure the static Domain Name Service (DNS). For more details on DNS configuration, see section 6.2.4 *DNS*.

Bridging – Use this section to bridge a combination of interfaces on the ShadowMaster. Please see section 6.2.2 *The Bridge* for details and limitations on bridge configuration.

4.3.3 Basic Wireless

The Basic Wireless page allows configuration of both radios as well as wireless network setup. From this page, choose how the ShadowMaster transmits data wirelessly. These settings are covered in detail in section 6.3 *Wireless Settings*.



Basic Wireless [Save] [?]

Country Code: Canada

Radio #1 (ath0) ☒ Enabled

Operating Mode: ☒ Master ☐ Managed

Antenna: ☒ Internal ☐ External

SSID: DEFAULT1 ☒ Broadcast SSID

IEEE Mode: A

Channel: 153 Full

Data rate (Mbps): 54 ☒ Automatic Rate Adjustment

Link Distance (km): 5.1

Transmit Power (dBm): 12

Throughput enhancements: ☐ Fast Frames ☐ Packet Bursting ☐ Compression ☐ Dynamic Turbo ☐ Quality of Service (WMM)

Radio #2 (ath1) ☐ Enabled

Operating Mode: ☒ Master ☐ Managed

Antenna: ☒ External

SSID: DEFAULT2 ☒ Broadcast SSID

IEEE Mode: B/G Mixed

Channel: 1 Full

Data rate (Mbps): 54 ☒ Automatic Rate Adjustment

Link Distance (km): 5.1

Transmit Power (dBm): 14

Throughput enhancements: ☐ Fast Frames ☐ Packet Bursting ☐ Compression ☐ Dynamic Turbo ☐ Quality of Service (WMM)

© 2008 WAVETEQ Communications Inc

Figure 4.3.4: Basic Wireless Page

Country Code – Specify which country the device is operating in. This automatically limits the operating conditions on the rest of the page to ensure that it operates within a countries regulatory domain. See Appendix B: Regulatory Domain/Channels for details on regulatory domain restrictions.

Operating Mode – Specify the operating mode of the device (Managed/Master).

Antenna – You can use either the internal antenna, or any external antenna connected to external 'N' port. See section 1.2 *Feature Locations* for connection details. Ensure that any antenna you connect meets the regulatory requirements for your particular area and application.

SSID – The Service Set Identifier (SSID) is the name of the wireless network the radio is connected to (managed mode) or broadcasting (master mode).

IEEE Mode – Specify which IEEE 802.11 standard the radio will operate in.

Channel – Specify which channel the radio will operate on. Ensure that the chosen channel meets the regulatory requirements for your particular area and application. You may also choose to adjust the channel width to full, half, or quarter which will drop the transfer rate accordingly, but will increase the power density and may help to achieve greater operation distances.

Data rate (Mbps) – Specify the maximum transmission rate of the radio. The Automatic Rate Adjustment checkbox will allow the radio to decrease the data rate in poor wireless conditions.

Link Distance (km) – Setting this value too large may decrease performance, while setting it too small may prevent communication entirely.

Transmit Power (dBm) – The transmit power is limited by your country's regulatory domain. Ensure that your chosen antenna, channel and transmit power are all within the regulatory requirements for your particular area and application.

Throughput Enhancements – Choose from a variety of throughput enhancements. Note that all devices on the network will need to be compatible with each enhancement. Each feature must be enabled on both sides of the wireless connection in order to work properly. Most of these options are only available on A, G and auto IEEE modes.

- **Fast Frames** – packet aggregation and timing modifications.
- **Packet Bursting** – more data frames per given time period.
- **Dynamic Turbo** – maximizes throughput using multiple channels.
- **Compression** – utilizes compression techniques to reduce the amount of data to be transmitted.
- **Quality of service (WMM)** – enable to support quality of service for prioritizing traffic from the Ethernet to the access point.

4.3.4 Advanced Network

The Advanced Network page allows management of advanced networking features, including DHCP server and DNS services, as well as static routing.

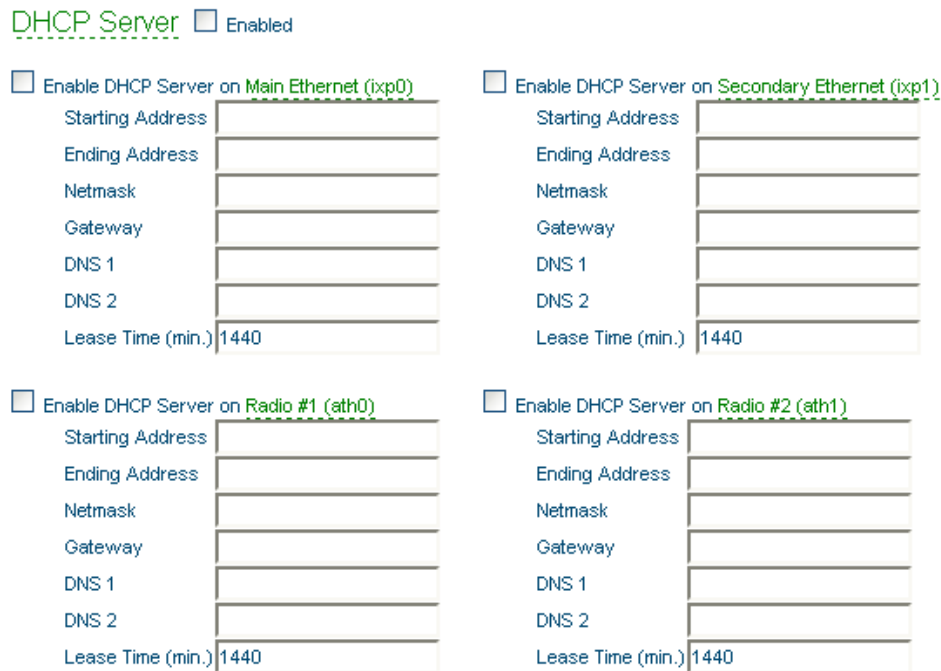
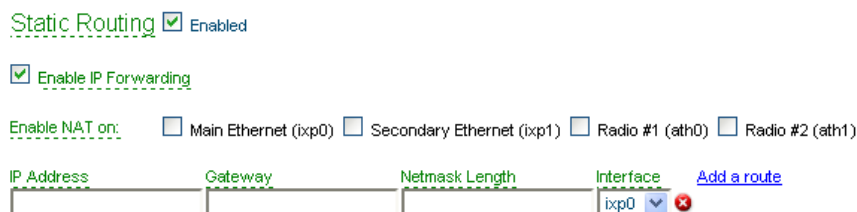


Figure 4.3.5: DHCP Server Subsection

DHCP Server – Use this section to configure an interface as a DHCP server. Be sure to click the enable checkboxes for the DHCP server status, as well as each interface it is to be enabled on.



© 2008 WAVETEQ Communications Inc.

Figure 4.3.6: Static Routing Subsection

Static Routing – Specify IP address, Gateway, Netmask Length, and which interface to enable a route on. Click **Add a route** to configure more than one routing rule.

IP Forwarding – allows your ShadowAP to act as a gateway or router. It is usually enabled.

NAT – Network Address Translation (NAT), also known as network masquerading, native address translation or IP masquerading, will rewrite the source and/or destination IP address as network traffic passes through the interface. This is commonly needed for routed network configurations.

4.3.5 Advanced Wireless

The Advanced Wireless page allows configuration of WEP, WPA, WPA2 security on each wireless device. Access Control Lists can also be specified. Be sure to click on each subheading to learn the required format for entering each WEP Key, Passphrase, and MAC Address.

Radio #1: (ath0)

Wired Equivalent Privacy (WEP)	<input type="text" value="Open system"/>	WEP Key	<input type="text"/>
Wi-Fi Protected Access (WPA)	<input type="text" value="Open system"/>	Passphrase	<input type="text"/>
Access Control List Mode	<input type="text" value="Open system"/>	MAC Address	<input type="text"/> Add ACL MAC Address

Radio #2: (ath1)

Wired Equivalent Privacy (WEP)	<input type="text" value="Open system"/>	WEP Key	<input type="text"/>
Wi-Fi Protected Access (WPA)	<input type="text" value="Open system"/>	Passphrase	<input type="text"/>
Access Control List Mode	<input type="text" value="Open system"/>	MAC Address	<input type="text"/> Add ACL MAC Address

© 2008 WAVETEQ Communications Inc

Figure 4.3.7: Wireless Security Page

Wired Equivalent Privacy (WEP) – Specify either 64-bit or 128-bit WEP security.

Wi-Fi Protected Access (WPA) – Specify either WPA or WPA2 mode with either TKIP or AES encryption.

Access Control List (ACL) Mode – Choose to Allow or Deny all except the MAC Addresses specified. Click **Add ACL MAC Address** to add multiple MAC addresses to the ACL.

4.3.6 Expert

This section is for editing the configuration file manually. The configuration file entry field is active and ready for editing.



Refer to section 6.1 *ShadowMaster Configuration File* for detailed information about the syntax of the configuration file.

Configuration File Management

Upload new configuration file:

Download running configuration file:

Edit Configuration

```

#####
# Configuration created by skin
# Skin: Waveteq, version: 080703.001
# Generated on 2008-07-04 12:40:16 GMT
#####
-Product=ShadowMaster
-notes.1=Link & Cover
-notes.2=Bridged 5.18 GHz (802.11a) Link and 2.412 GHz (802.11g) Access Point

# AUTHENTICATION, AUTHORIZATION AND ACCOUNTING:
#
aaa.1.devname=ath0
aaa.1.nas.1.profile=NAS-ath0
aaa.1.nas.1.status=disabled
aaa.1.status=disabled

```

Adjust edit area height:

© 2008 WAVETEQ Communications Inc

Figure 4.3.8: Edit Configuration File Manually

Save – click to save a modified configuration file to the device flash memory. Modified ShadowMaster system configuration will become active after device reboot. The system information message appears with direction to reboot the device. Use the **Reboot** button to reboot the device and apply device configuration changes.

Device needs to be rebooted for new configuration to take effect.



Incorrect configuration file modifications (keys and values) may cause the ShadowMaster to stop working. In this case try to upload a known good configuration file or perform a reset to factory defaults (See 4.4.1 for details). The emergency IP may also be used to communicate in such a situation (see 2.3.1 for details).

Reset – use this button to cancel recent changes of the configuration file text. This button is functional before using the Save button.

Read active – load the last saved configuration file from device flash memory.

Read backup – load the next-to-last saved configuration file from device flash memory.

Adjust edit area height – choose the height of the edit area.

4.4 System

Use the **System** menu to define access settings to the device, or to use system utilities:

- **Maintenance** – to upgrade firmware, reboot, or reset to factory default configuration.
- **Password** – to change the administrative access password.
- **Remote Management** – to configure administrative access.
- **License** – to manage license file status.



Figure 4.4.1: System Menu

4.4.1 Maintenance

Use the **Maintenance** menu to upgrade system firmware, reboot the device or set the device to factory default values.

Firmware Upgrade

Current Firmware Version: WMLI-S.AVILA.v5.22.xscale.Waveteq.19380.080705.031442

Firmware image:

Reboot

Reboot device

Factory Defaults

Reset device to factory defaults

© 2008 WAVETEQ Communications Inc

Figure 4.4.2: Maintenance Page

Current Firmware Version – Use the information displayed to determine if a firmware version upgrade is necessary.

Firmware Image – Click **browse** to find the new firmware image on your computer. Then click **Upload** to save it onto the device.



Upgrading your ShadowMaster's firmware will cause the current configuration to be reset to the factory defaults. Please back up your configuration before upgrading your ShadowMaster.

Reboot Device – Clicking reboot will save the current modified configuration file onto the device, and the device will then proceed to restart and refresh all of the most recent settings. This process may take up to one minute to complete.

Reset device to factory defaults – Click this button to reload the factory default configuration.



Do not switch off and do not disconnect the device from the power supply during the firmware update process as the device could be damaged.

4.4.2 Password

The Password page is for changing the existing administrators' password. The only way to gain access to the web management if you forget the administrator password is to return your ShadowMaster to Waveteq Communications.

Administrative Account

Username	admin
Old password	<input type="password"/>
New password	<input type="password"/>
Verify password	<input type="password"/>
	<input type="button" value="Change"/>

Figure 4.4.3: Change the Administrator's Password

Username – displays the username of the current connected administrator. This parameter is not changeable.

Old password – enter the old administrator password.

New password – enter the new administrator password for user authentication.

Verify password – re-enter the new password to verify its accuracy.

Change – click to save the new administrator password.



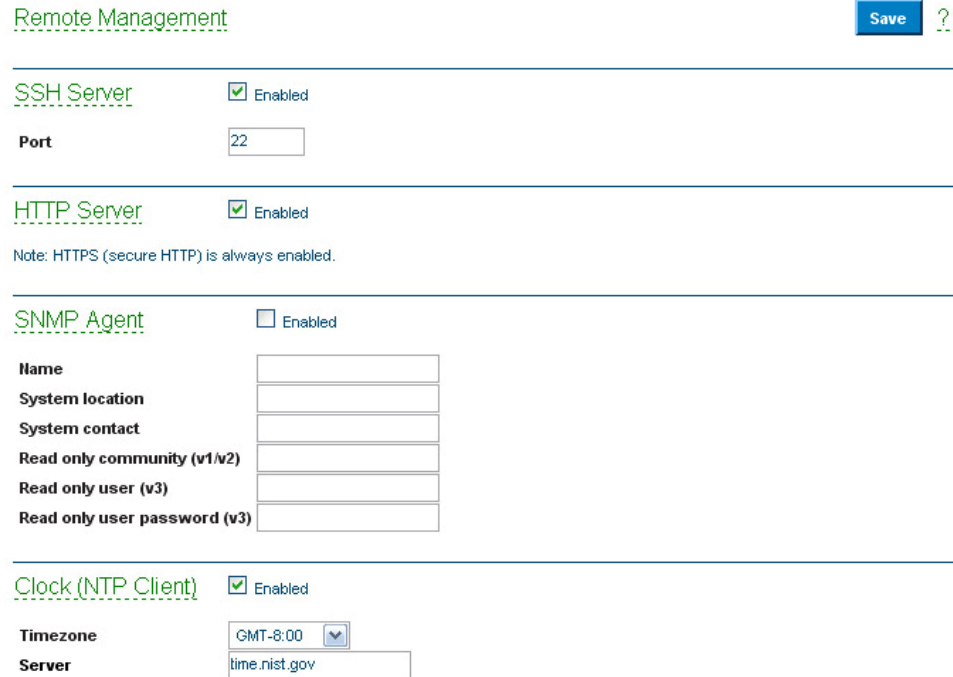
The only way to gain access to the web management if you forget the administrator password is to return your ShadowMaster to Waveteq Communications.



Default administrator login settings are:
User Name: admin
Password: admin01

4.4.3 Remote Management

The Remote Management page allows configuration of administrative access and monitoring of the ShadowMaster.



Remote Management Save ?

SSH Server ☒ Enabled

Port

HTTP Server ☒ Enabled

Note: HTTPS (secure HTTP) is always enabled.

SNMP Agent ☐ Enabled

Name

System location

System contact

Read only community (v1/v2)

Read only user (v3)

Read only user password (v3)

Clock (NTP Client) ☒ Enabled

Timezone

Server

© 2008 WAVETEQ Communications Inc

Figure 4.4.4: Remote Management Page

SSH Server – Secure Shell (SSH) is a network protocol that allows data to be exchanged using a secure channel between two computers. When enabled, the ShadowMaster Shell can be accessed with an SSH client like PuTTY.

HTTP Server – The HTTP server will process web browser requests to display this graphical user interface. Secure HTTP (HTTPS) is always enabled on port 443.

SNMP Agent – Standard Network Management Protocol (SNMP) is used in network management systems to monitor network-attached devices. The ShadowMaster supports all three SNMP protocol versions in read only mode.

Clock (NTP Client) – The ShadowMaster can be configured to periodically update its internal clock to an internet time server. Ensure that your ShadowMaster is properly configured to be able to access the specified server.

4.4.4 License

When the device is installed and ready for use, the valid license file should be uploaded on the device to activate a full set of the device features. Within the valid license period, the new released firmware images will be available to upgrade/downgrade on the ShadowMaster device.



After the expiration of license the device will keep functioning. However, new firmware revisions for the later period will not be available. Contact Waveteq if you require a new firmware version and your update period has expired.

Device License

License status valid

License period unlimited

Download current license file

Download

Upload New License

License file upload

Browse...

Upload

© 2008 WAVETEQ Communications Inc

Figure 4.4.5: Device License Page

License status – displays the license validity status:

- **valid** – this license status means that device has full functionality of the purchased ShadowMaster firmware release. Even after the **license period** expiration the device will keep functioning with the current firmware.
- **not valid** – this license status provides only a very limited functionality.
 - It runs only with a default configuration. Only a single BSSID is allowed; DHCP client runs on WAN interface, DHCP servers run on LAN and Wireless interfaces.
 - It is impossible to change the configuration. All features are locked down until a valid license is presented. Any changes made in configuration will be stored in the flash memory of the device. Thus only a default setting will be used after the reboot.

License period – specifies the time period wherein the new released firmware images can be upgraded on particular ShadowMaster device. Once a valid license file was uploaded it will be valid even after the license period expiration.



The device license will be still valid after resetting the device to defaults.

Download current license file – click to download current device license file to your local PC.

License File Upload – click for the license file upload on the device.

Browse... – click to specify the license file you want to upload on the device.

Upload – click to upload the chosen license file on the device.



Be certain you are uploading a valid license file.

After the new license file is uploaded, the device must be rebooted for changes to take effect. For instructions on how to reboot the device, refer to the Reboot section on the Maintenance page.



In case the fault license file has been uploaded, the device becomes inactive after reboot and the default configuration will be uploaded with the dynamic IP address given by the local DHCP server.

4.5 Tools

Use the **Tools** menu to align, and test the ShadowMaster:



Figure 4.5.1: Tools Menu

- **Site Survey** – to view the list of wireless networks in the local geographical area.
- **Antenna Alignment** – to align a ShadowMaster device antenna.
- **Wireless Tests** – to perform detailed wireless testing.

4.5.1 Site Survey

The **Site Survey** shows overview information for wireless networks in a local geographic area.

Using this test, an administrator can scan for working access points, check their operating channels, WEP encryption and see signal/noise levels. An administrator can use this feature to identify a clear channel to set the ShadowMaster to one that will not receive interference from other wireless devices.



Note that **Site Survey** function can take several minutes to perform.

A Site Survey test is performed every time on the start-up of the device, therefore the results of the last performed Site Survey test and its time can be found on the page. Thus, to obtain the results, the initiation of the scan is not necessary.

Choose wireless interface – choose the interface on which the Site Survey test will be performed from the drop-down list.



The **Site Survey** function is impossible if the selected wireless interface is disabled.

Scan – click to update the Site Survey.

Figure 4.5.2 below shows the Site Survey table found in the web interface.

Site Survey

Results from 1 min. 59 sec. ago

(Click the column header to sort the table by that column)

MAC address ▲	ESSID	Encryption	Signal strength	Noise floor	Frequency, GHz	Channel
00:0B:6B:4E:AD:D6	DEFAULT1	WPA	-58	-95	5.18	36
00:0B:6B:80:BD:77	WAVETEQ_2K_24	-	-68	-95	2.412	1
00:0B:6B:84:39:51	DEFAULT2	-	-61	-95	2.412	1

Note: initiating **Scan** will temporary disable radio link with selected interface.

Choose wireless interface:

Figure 4.5.2: Site Survey Table

4.5.2 Antenna Alignment

The antenna alignment test measures signal quality between the ShadowMaster and other wireless networking devices. For best results turn off all wireless networking devices within range of the device except the device(s) with which you are trying to align the antenna. Watch the constantly updated display in the Alignment Test window as you adjust the antenna.

Antenna Alignment

Choose wireless interface:

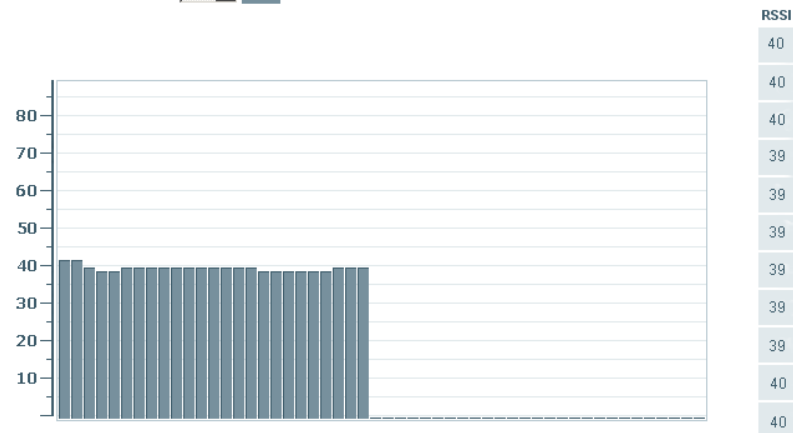


Figure 4.5.3: Antenna Alignment Tool

Choose wireless interface – select the wireless interface to align the antenna on.

The Antenna Alignment test results appear when you click the **Start** button, and finishes when you click **Stop**.

4.5.3 Wireless Tests

This test generates TCP/UDP traffic and measures throughput from client to server with current established point-to-point link conditions. Use the following procedure to configure and run a test between two ShadowMaster Devices.

Step 1: Configure the Rates Test subsection for each ShadowMaster device.

Rates Test

Choose wireless interface:	<input type="text" value="ath0"/>
Choose data rate, Mbps:	<input type="text" value="auto"/>
Current data rate, Mbps:	54
	<input type="button" value="Set"/>
Save values to configuration file:	<input type="button" value="Save"/>

Figure 4.5.4: Rates Test

Choose Wireless Interface – choose between radio 1 (ath0), or radio 2 (ath1) to perform the rates test.

Choose data rate – select the data rate at which to perform the wireless test.

Current data rate – displays the currently configured data rate. A value of zero means that the data rate is automatically set.

Set – click this button after setting the wireless interface and data rate to confirm the settings for the wireless test.

Save – click this button to load the tested data rate into the configuration file. The device will use this rate upon successful reboot.

Step 2: Configure the ACK Timeout Test subsection for each ShadowMaster device. The ACK Timeout value is directly related to the distance between two ShadowMaster devices. Setting this value too high will reduce performance, while setting it too low may inhibit a successful connection.

ACK Timeout Test

Choose wireless interface:	<input type="text" value="ath0"/>
ACK timeout:	<input type="text" value="55"/> <input type="range" value="55"/>
	<input type="button" value="Set"/>
Save values to configuration file:	<input type="button" value="Save"/>

Figure 4.5.5: ACK Timeout Test

Choose Wireless Interface – choose between radio 1 (ath0), or radio 2 (ath1) to perform the ACK timeout test.

ACK timeout – select the ACK timeout value used to perform the wireless test. The default value of 55 corresponds to a link distance of 5Km (3.1 miles). See section 6.3.1 *Wireless Radio* for more details on the relationship between ACK timeout value and link distance.

Set – click this button after setting the wireless interface and ACK timeout value to confirm the settings for the wireless test.

Save – click this button to load the tested value into the configuration file. The device will use this value upon successful reboot.

Step 3: Configure each ShadowMaster's operating mode and device-specific settings.

Throughput Test

Operating mode: Server ▼

Protocol: TCP ▼

Host:

Duplex traffic: ☐

Figure 4.5.6: Throughput Test subsection

Operating Mode – choose between server or client operation for both radios being tested. One should be a server, and the other a client.

Protocol – when operating as the client for the wireless test, the ShadowMaster can select either TCP or UDP networking protocols.

Host – when operating as the client for the wireless test, the IP address of the server ShadowMaster must be entered into this textbox.

Duplex Traffic – click this checkbox to test sending and receiving data traffic simultaneously. This will typically provide lower throughput results than a unidirectional test.

Step 4: Begin the test by clicking start on the ShadowMaster configured as the test server. Next, click start on the ShadowMaster configured as the test client. "TCP/UDP socket connected to xxx.xxx.xxx.xxx" should be displayed below the start button, where xxx.xxx.xxx.xxx is the IP address of the ShadowMaster acting as the test server.

Start Stop Show Results

Results:

Step	Input (kbps)	Output (kbps)
TCP socket connected to 192.168.3.1		
1	14506.82	0.00
2	16379.78	0.00
3	16460.86	0.00
4	16281.31	0.00
average	15963.48	0.00

© 2008 WAVETEQ Communications Inc

Figure 4.5.7: Wireless Test Results

Start – click this button to begin the test.

Stop – click this button to stop the test.

Show Results – click this button only after the test has been started on both devices. The ShadowMaster might take a few seconds before completing the test, so if less than four results show, click this button once more.

Results – displayed are the wireless test results in kbps. The test is performed in 4 steps, and an average is calculated for user convenience.



Do not forget to stop Server's side after the throughput test is finished, as the test may influence the ShadowMaster's performance.

4.6 Logout

Click **LOGOUT** link on the top right corner of the main menu to leave the Web management interface:



Figure 4.6.1: Logout from the Web Management

Logout – click to leave the device Web management. When the **LOGOUT** button is clicked, the administrator is redirected to the login page.

5.0 Chapter 5 - SNMP Management

Another way to monitor the ShadowMaster over a TCP/IP network is **SNMP** (Simple Network Management Protocol).

SNMP is an application layer protocol that facilitates the exchange of management information between network devices. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP allows network administrators to monitor and manage network performance, find and solve network problems, and plan for network growth.

The SNMP agent and Management Information Base (MIB) reside on the ShadowMaster. To configure SNMP on the controller, you must define the relationship between the Network Management System (NMS) and the SNMP agent (ShadowMaster). The SNMP agent contains standard **MIB** and variables whose values the SNMP manager can request or change. A NMS can get a value from an agent. The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get data.



In order to manage the device you have to provide your Network Management System software with adequate MIB files. Please consult your management software manuals on how to do that.

5.1 SNMP Versions

The ShadowMaster supports the following versions of SNMP:

SNMPv1 – the Simple Network Management Protocol: A Full Internet Standard, defined in [RFC1157](#). (RFC1157 replaces the earlier versions that were published as [RFC1067](#) and [RFC1098](#).) Security is based on community strings.

SNMPv2c – the community-string based Administrative Framework for SNMPv2. SNMPv2c (the "C" stands for "community") is an experimental protocol defined in [RFC1901](#), [RFC1905](#), and [RFC1906](#). SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.

SNMPv3 – SNMP v3 is based on version 2 but with added security features. It addresses security requirements through encryption, authentication, and access control rules.

Both SNMPv1 and SNMPv2c use a community-based form of security. The community of managers able to access the agent's MIB is defined by an IP address access control list and password. SNMPv3 provides more robust security through the introduction of a "User Security Model" (USM) and through the encryption of SNMP protocol traffic.

The Access Controller implementation of SNMP supports all MIB II variables (as described in [RFC1213](#)) and defines all traps using the guidelines described in [RFC1215](#). The traps described in this RFC are:

coldStart

A coldStart trap signifies that the SNMP entity, acting in an agent role, is reinitialising itself and that its configuration may have been altered.

nsNotifyShutdown

An nsNotifyShutdown trap signifies that the SNMP entity, acting in an agent role, is being shut down.

5.2 SNMP Agent

The SNMP agent responds to SNMP manager requests using a **Get a MIB variable** – the SNMP agent begins this function in response to a request from the SNMP manager. The agent retrieves the value of the requested MIB variable and responds to the manager with that value.

The SNMP agent also sends unsolicited trap messages to notify an SNMP manager that a significant event has occurred (e.g. SNMP authentication failures) on the agent.

5.3 SNMP Community Strings

SNMP community strings authenticate access to MIB objects and function as embedded passwords. The ShadowMaster supports a **Read-only** community string that gives read access to authorized management stations to all objects in the MIB - except the community strings - but does not allow write access.

5.4 Use SNMP to Access MIB

As shown in Figure 5.4.1, the SNMP agent gathers data from the MIB. The agent can send traps (notification of certain events) to the SNMP manager, which receives and processes the traps. Traps are messages alerting the SNMP manager to a condition on the network such as improper SNMP manager authentication, restarts, link status (up or down), MAC address tracking, and so forth. The SNMP agent also responds to MIB-related queries sent by the SNMP manager in *get-request*, *get-next-request* and *get-bulk* format.

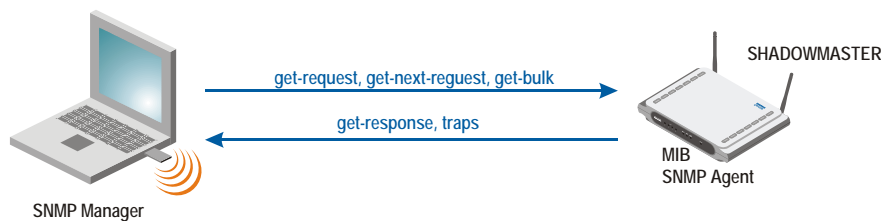


Figure 5.4.1: SNMP Network

6.0 Chapter 6 - Configuring the ShadowMaster

In order to configure the ShadowMaster properly, the user must have working knowledge of: the ShadowMaster's configuration file, and the Network, Network Access, Management Access and System Services configuration. The following sections will go over these aspects in detail.

6.1 ShadowMaster Configuration File



The keys of the configuration file in this manual are provided for ShadowMaster 5.x firmware version therefore they may differ from the keys of 3.5x firmware and former versions.

The ShadowMaster configuration file is a text file consisting of **<key>=<value>** assignments, one assignment per line. Modified configurations will become active after the device reboots. The keys are case sensitive. Whitespace around keys and values is insignificant and it will be removed automatically after reboot. If duplicate keys are found, the first one is left and all the others are removed, irrespective of the value assigned to those keys.

If the first character after whitespace on line is a "#" character, text between that character and the end of the same line is a comment. Comment lines and blank lines are ignored and may be added to make the file easier to read.

Example:

```
# this line is a comment
netconf.1.devname=ixp0
netconf.1.ip=192.168.2.5
netconf.1.netmask=255.255.255.0
```

In the example above keys have index "1" and describe the settings of ixp1 interface. The index indicates functionally similar items and it will be specified as **<index>** in the configuration file descriptions, e.g., **netconf.<index>.devname**, **netconf.<index>.ip**, **netconf.<index>.netmask**.

The configuration file location on local ShadowMaster file system is /tmp/system.cfg. The configuration file can be changed or a new file can be uploaded using Web interface. It is also possible to manually update device configuration. Follow these steps:

- login to device with secure SFTP client
- upload new configuration file to /tmp/system.cfg
- login through SSH, type shell command to exit to shell (see 3.2 CLI Access)
- execute `sysconf -w`
- reboot the device.

Some keys can have default values; others can be unused or have to be explicitly specified for some feature to work correctly. These keys and their values will be printed through local syslog facility to a system log file. The system log file on ShadowMaster is /var/log/messages. Logging can be redirected to a remote host (see section 6.6.4 Syslog).

Example:

An excerpt from default system log file:

```
Jan 1 00:00:06 sysconf[89]: Using default value: 'disabled' for non existing bool key:
'aaa.nas.1.verbose'
Jan 1 00:00:06 sysconf[89]: Unused key: netconf.1.type=Ethernet
```

6.2 Network Configuration

This section describes settings of physical and logical network interfaces. This includes physical LAN and WAN interface settings, DNS settings, DHCP settings, AAA settings, tunnels and wireless interface settings.

6.2.1 Interfaces

The physical network interfaces can be configured to work as either local area network (LAN) or wide area network (WAN) interfaces. LAN is used to connect hubs, switches, Access Points and other devices on a subscriber side, while the WAN port connects to the Internet service provider's (ISP) network.

All available keys of the network interface configuration are listed below:

netconf.status – specify the interface configuration feature status [enabled/disabled]. In general this key should always be specified and set to enabled.

netconf.<index>.status – specify current network interface status [enabled/disabled].

netconf.<index>.devname – specify the interface name [lo/ixp0/ixp1/ath0/ath1/logical interface name]. The physical interface names are:

- lo – local loopback interface
- ixp0 – first Ethernet interface
- ixp1 – second Ethernet interface
- ath0 – first wireless interface
- ath1 – second wireless interface

Logical interface names will be described in the following sections.

netconf.<index>.type - specify the interface type [loopback/wireless/ethernet/bridge/gre].

netconf.<index>.mode – specify the interface mode [lan/wan].

netconf.<index>.up – specify the interface status [enabled/disabled]. This value causes the interface to be activated, or the driver for this interface to be shut down.

netconf.<index>.ip – specify the interface IP address, eg. 192.168.5.1.

netconf.<index>.netmask – specify the interface subnet mask, eg. 192.168.5.0.

netconf.<index>.broadcast – specify the interface broadcast IP address, eg. 192.168.5.255.

netconf.<index>.alias.status – specify the interface alias functionality status [enabled/disabled]. This enables/disables all interface aliases. Default: disabled.

netconf.<index>.alias.<index>.status – specify current alias status [enabled/disabled].

netconf.<index>.alias.<index>.ip – specify the IP address for the interface alias. This key may be used as aliased IP range start, used together with *netconf.<index>.alias.<index>.ip_range_end* key.

netconf.<index>.alias.<index>.ip_range_end – specify the aliased IP range end. This key is used with *netconf.<index>.alias.<index>.ip* which means the aliased IP range start.

netconf.<index>.alias.<index>.netmask – specify the subnet mask for the interface alias, eg. 192.168.6.0.

netconf.<index>.alias.<index>.broadcast – specify the broadcast IP address for the interface alias, eg. 192.168.6.255.

netconf.<index>.mcast.status – specify the multicast address status [enabled/disabled]. Default: disabled. The multicast keys are used to attach a static link layer multicast address to listen on the interface. They only manage link layer addresses.

netconf.<index>.mcast.<index>.lladdress – specify the multicast link layer address.

netconf.<index>.mcast.<index>.address – specify the multicast IPv4 address, will be remapped by plugin to link layer.

```
netconf.2.mcast.status=enabled
netconf.2.mcast.1.address=01:00:5e:00:00:0a
netconf.2.mcast.1.address=224.192.16.1
```

netconf.<index>.allmulti - specify the status of all-multicast mode [enabled|disabled(default)]. default: disabled. If enabled, all multicast packets on the network will be received by the interface.

netconf.<index>.mac – specify the interface MAC address [colon-separated, 6 hexadecimal value pairs, eg. 03:FA:45:10:BA:44].

netconf.<index>.promisc – specify the promiscuous mode status [enabled/disabled]. If enabled, all packets on the network will be received by this interface.

netconf.<index>.mtu – specify the MTU size in B [integer]. Default: 1500. MTU is the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent.

The following keys, **autoneg**, **advertise**, **speed** and **duplex** in netconf.* section apply to Ethernet devices only. These keys allow you to control what speed and duplexity Ethernet devices are allowed to be connected in the network.

netconf.<index>.autonet – specify status of auto-negotiating [enabled/disabled]. Default: enabled.

netconf.<index>.advertise – specify advertise [auto/number]. Default: auto. This key is usable when **autoneg** key is enabled.

- 0x001** – 10baseT-HD'
- 0x002** – 10baseT-FD'
- 0x003** – 10baseT'
- 0x004** – 100baseTx-HD'
- 0x008** – 100baseTx-FD'
- 0x00C** – 100baseTx'
- 0x010** – 1000baseTx-HD'
- 0x020** – 1000baseTx-FD'
- 0x030** – 1000baseTx'
- 0x03F** – auto (combination of all the above)

ixp0 – first Ethernet interface
ixp1 – second Ethernet interface
ath0 – first wireless interface
ath1 – second wireless interface

netconf.<index>.speed – specify Ethernet link speed between switch and ShadowMaster device in Mbps [10/100/1000].

netconf.<index>.duplex – specify duplexity of the Ethernet link [half/full].

Example 1:

```
netconf.1.autoneg=disabled
netconf.1.advertise=auto
netconf.1.speed=10
netconf.1.duplex=half
```

Ethernet is allowed to connect at fixed 10 Mbps speed, duplex will be set to *half*. The *advertise* makes no sense when auto-negotiation (autoneg key) is disabled.

Example 2:

```
netconf.1.autoneg=enabled
netconf.1.advertise=auto
netconf.1.speed=10
netconf.1.duplex=half
```

Ethernet is allowed to negotiate best speed and duplexity. Parameters **speed** and **duplex** will be ignored when **autoneg** is enabled. It is up to the Ethernet driver to decide which speed, duplexity must be used according to **advertise** key value (default value is auto).

Example 3:

```
netconf.1.devname=ixp1
netconf.1.netmask=255.255.255.0
netconf.1.ip=192.168.2.220
netconf.1.up=enabled
netconf.1.mode=wan
netconf.1.type=Ethernet
netconf.1.promisc=disabled
netcont.1.alias.status=enabled
netcont.1.alias.1.status=enabled
netcont.1.alias.1.ip=192.168.2.16
netcont.1.alias.2.status=enabled
netcont.1.alias.2.ip=192.168.2.17
netcont.1.alias.3.status=enabled
netcont.1.alias.3.ip=192.168.2.200
netcont.1.alias.3.ip_range_end=192.168.2.210
```

The configuration in example 3 means that the ixp1 interface is configured to have *192.168.2.220* as a primary IP address on interface, netmask is set 255.255.255.0, default gateway 192.168.2.1, interface is up (enabled). Also, see *alias*, this tells to configure ixp1 to have other aliased ip addresses as well (192.168.2.16, 192.168.2.17, and 192.168.2.200-192.168.2.210 range). It is the user's responsibility to define routes for these addresses in configuration file.

6.2.2 The Bridge

A bridge transparently relays traffic between multiple network interfaces. Bridge is identified by a custom interface name. It is basically a container for other interfaces.

There are some restrictions for bridge management that shall be taken into account:

- It is not possible to add a device to multiple bridges.
- The WAN interface cannot be added into a bridge.
- VLANs cannot be created on bridge interfaces; they can only be added to them.
- A bridge cannot be included into another bridge.

All available keys of the bridge configuration are listed below:



The <index> range for bridge is 1-100.

bridge.status – specify the bridge feature status [enabled/disabled]. Default: disabled.

bridge.<index>.status – specify current entry status [enabled/disabled]. Default: enabled.

bridge.<index>.devname – specify the bridge interface name [custom string up to 15 characters in length, e.g. br0, mandatory].

bridge.<index>.stp.status – define the STP (Spanning Tree Protocol) status [enabled/disabled]. Default: disabled.

If you are running multiple or redundant bridges, then you need to enable Spanning Tree Protocol (STP) to optimize multiple hops and avoid bridging loops. Normally redundant bridges would result in duplicated packets, which would saturate the connected networks. Bridges configured to use STP negotiate the shortest possible link between the connected networks and disable all other possible links. If a link fails STP recalculates the links and can enable a workaround for the failed link. For the bridge to take part in this negotiation STP must be enabled. It is disabled by default when creating the bridge.

Each bridge has a relative priority and cost. Each interface is associated with a port (number) in the STP code. The priority and cost are used to decide which is the shortest path to forward a packet. The lowest cost path is always used unless the other path is down. If you have multiple bridges and interfaces you may need to adjust the priorities to achieve optimum performance.



If your bridge is not the only bridge on the LAN, or if there are loops in the LAN topology, STP is strongly recommended.

The STP protocol first elects a root bridge. The root bridge is the bridge with the lowest priority in the network. If several bridges have the same priority assigned, the bridge with the lowest MAC address is chosen. The root bridge is the "central" bridge in the spanning tree.



It is recommended not to use more than one VLAN or VSSID in the bridge, otherwise in some network topologies (using switches) the bridge may not work as expected.

bridge.<index>.priority – specify the bridge priority [0-65535]. Default: 32768.

bridge.<index>.fd – specify the forwarding delay time [0-65535]. Forwarding delay time is the time spent in each of the listening and learning states before the forwarding state is entered. Default: 15.

bridge.<index>.hello – specify the interval between hello packets in seconds [0-65535]. Hello packets are used to communicate information about the topology throughout the entire bridged LAN. Default: 2.

bridge.<index>.ageing – define the interface hardware (MAC) address ageing time, in seconds [0-65535]. The ageing time is the number of seconds that a MAC address will be kept in the forwarding database after receiving a packet from this MAC address. The entries in the forwarding database are periodically timed-out to ensure that old ones do not persist in the database. Default: 300.

bridge.<index>.maxage – specify the maximum bridge message age in seconds [0-65535]. If the last received hello packet is more than this value, the bridge in question will initiate the root bridge election procedure. Default: 20.

bridge.<index>.port.<index>.status – specify current bridge port status [enabled/disabled]. Default: disabled.

bridge.<index>.port.<index>.devname – specify the interface name to be added into bridge (physical interface, VLAN or GRE tunnel).

bridge.<index>.port.<index>.path.cost – specify the port's path cost on this interface [0-65535]. This metric is used in the designated port and root port selection algorithms. Default: 100.

bridge.<index>.port.<index>.priority – specify the priority of ports with equal cost [0-255]. You can use this to control which port gets used when there are redundant paths. Default: 128.

bridge.arptables – if enabled, it will pass bridged ARP traffic to arptables' FORWARD chain [enabled/disabled]. Default: enabled.

bridge.iptables – if enabled, it will pass bridged IPv4 traffic to iptables' chains [enabled/disabled]. Default: enabled.

bridge.vlan – if enabled, it will pass bridged vlan-tagged ARP/IP/IPv6 traffic to ARP/IP/IPv6 tables [enabled/disabled]. Default: enabled.

Example:

```
# create bridge br0 with ixp0 and ath0 interfaces
bridge.status=enabled
bridge.1.status=enabled
bridge.1.ageing=300
bridge.1.devname=br0
bridge.1.fd=1
bridge.1.hello=20
bridge.1.maxage=300
bridge.1.port.1.status=enabled
bridge.1.port.1.devname=ixp0
bridge.1.port.2.status=enabled
bridge.1.port.2.devname=ath0
bridge.1.priority=2
bridge.1.stp.status=disabled
```


6.2.3 DHCP

The ShadowMaster device can act as DHCP (Dynamic Host Configuration Protocol) client, DHCP server and/or as a DHCP relay gateway. The DHCP service is supported on both physical and logical interfaces.

6.2.3.1 DHCP Client



The <index> range for DHCP client is 1-50.

A configured DHCP client will try to get an IP lease immediately on ShadowMaster start-up.

All available keys of the DHCP client are listed below:

dhcpc.status – specify the service status [enabled/disabled]. Default: disabled.

dhcpc.background – allows to enable the device and not wait for an IP address before starting the boot process [enabled/disabled]. Default: disabled.



In case the key **dhcpc.background** is enabled and the device starts the boot process without an IP address, the following services **will not be started**:

- NTP server
- Static Routing feature
- DNS Forwarder
- Syslog
- Wireless Client Bridge
- Station Supervision
- AAA
- AutoLock WLAN

dhcpc.<index>.status – specify the DHCP client status [enabled/disabled]. Default: enabled.

dhcpc.<index>.devname – specify the interface on which you want to enable the DHCP client.

Example:

```
# enable DHCP client on ixp1 interface
dhcpc.status=enabled
dhcpc.1.devname=ixp1
```

6.2.3.2 DHCP Server

The DHCP server assigns clients on the LAN dynamic IP addresses. The server is supported on physical and logical LAN interfaces. Each LAN interface runs a separate DHCP server instance.

All available keys of the DHCP server are listed below:

dhcpcd.status – specify the feature status [enabled/disabled]. Default: disabled.

dhcpcd.<index>.status – specify the DHCP server status [enabled/disabled]. Default: enabled.

dhcpcd.<index>.devname – specify the name of interface on which you want to configure the DHCP service [interface name, mandatory].

dhcpcd.<index>.start – specify the starting IP address of the DHCP address pool [IP address, mandatory].

dhcpcd.<index>.end – specify the ending IP address of the DHCP address pool [IP address, mandatory].

dhcpcd.<index>.gateway – specify the gateway IP address.

dhcpcd.<index>.netmask – specify the netmask.

dhcpcd.<index>.dns.1.status – specify the primary DNS server status [enabled/disabled].
Default: enabled.

dhcpcd.<index>.dns.1.server – specify the primary DNS server IP address.

dhcpcd.<index>.dns.2.status – specify the secondary DNS server status [enabled/disabled].
Default: enabled.

dhcpcd.<index>.dns.2.server – specify the secondary DNS server IP address.

dhcpcd.<index>.lease_time – specify the IP address lease interval in seconds [1-4294967295].
Default: 86400.

dhcpcd.<index>.wins – specify WINS server IP address.

dhcpcd.<index>.domain – specify the DHCP domain name [1-128 character string].

Example:

```
# configure the DHCP server:
dhcpcd.status = enabled
dhcpcd.1.devname = ixp1
dhcpcd.1.start = 192.168.4.2
dhcpcd.1.end = 192.168.4.254
dhcpcd.1.gateway = 192.168.4.1
dhcpcd.1.netmask = 255.255.255.0
dhcpcd.1.dns.1.server = 212.59.0.1
dhcpcd.1.lease_time = 10000
```

6.2.3.3 DHCP Relay

DHCP relay forwards DHCP messages between subnets with different sub-layer broadcast domains.



DHCP relay won't work if there is a DHCP server or client started on the same LAN interface.



Depending on your network configuration, you may need to add firewall rules to allow clients unrestricted to have access to the DHCP service ports on the DHCP servers. This is needed because after negotiating a DHCP lease, a client talks to DHCP server directly and not through DHCP relay. See section *6.4.3 IP Firewall* for details.

The available keys of the DHCP Relay feature are listed below:

dhcpcd.fwd.status – specify the DHCP relay service status [enabled/disabled]. Default: disabled

dhcpcd.fwd.server.<index>.status – specify current service status [enabled/disabled]. Default: enabled.

dhcpcd.fwd.server.<index>.devname – specify the WAN interface name through which the DHCP server could be reached [string, interface name].

dhcpcd.fwd.server.<index>.ip – specify the DHCP server IP address [IP address or string "bcast"]. Specifying "bcast" allows broadcasting DHCP request on WAN when no unicast server address is known.

dhcp-fwd.client.<index>.status – specify the status of client interface [enabled/disabled].
Default: enabled.

dhcp-fwd.client.<index>.devname – specify the client interface name. This parameter defines a LAN interface where DHCP clients reside. A few interfaces may be defined.

dhcp-fwd.client.<index>.circuit_id – specify the client circuit id [string]. Every client interface (LAN) may have their unique identifier. As the circuit id could be used NAS-ID, NAS-MAC or NAS-IP. Refer to section 6.4.1.1 *Network Access Server (NAS)* for details about NAS settings. The DHCP servers can provide IP addresses from different address pools depending on a circuit id. Please refer to RFC 3046 for details.

Example 1:

```
# simple configuration with one client interface (LAN) and one server
# interface (WAN):
dhcp-fwd.status=enabled
dhcp-fwd.server.1.status=enabled
dhcp-fwd.server.1.devname=ixp1
dhcp-fwd.server.1.ip=bcast
dhcp-fwd.client.1.status=enabled
dhcp-fwd.client.1.devname=ath0
```

Example 2:

```
# configuration to show all the possible features:
dhcp-fwd.status=enabled
dhcp-fwd.server.1.status=enabled
dhcp-fwd.server.1.devname=ixp1
dhcp-fwd.server.1.ip=192.168.2.125
dhcp-fwd.server.2.status=enabled
dhcp-fwd.server.2.devname=ixp2
dhcp-fwd.server.2.ip=bcast
dhcp-fwd.client.1.status=enabled
dhcp-fwd.client.1.devname=ath0
dhcp-fwd.client.1.circuit_id=MY_NAS_ID_1
dhcp-fwd.client.2.status=enabled
dhcp-fwd.client.2.devname=ixp0
dhcp-fwd.client.2.circuit_id=MY_NAS_ID_2
```

6.2.4 DNS



A maximum of three name servers and six domain search entries can be specified.

The DNS (Domain Name Service) translates Internet host names (www.example.com) into their IP addresses.

All available keys of the DNS configuration are listed below:

resolv.status – specify the DNS status [enabled/disabled].

resolv.nameserver.<index>.status – specify current DNS server status [enabled/disabled].
Default: enabled.

resolv.nameserver.<index>.ip – specify the IP address of the DNS server [IP address, mandatory].

resolv.search.<index>.status – specify the status [enabled/disabled]. Default: enabled.

resolv.search.<index>.domain – specify the domain name to use for DNS lookups when no domain is specified [domain name, e.g. mycompany.net]. Specified domains will be checked in turn until a match is found.

resolv.host.<index>.status – specify current host entry status [enabled/disabled]. Default: enabled.

resolv.host.<index>.ip – specify the IP address of the hostname [IP address, mandatory].

resolv.host.<index>.name – specify the canonical hostname [hostname string, mandatory].

resolv.host.<index>.alias.<index>.status – specify the parameter status [enabled/disabled]. Default: enabled

resolv.host.<index>.alias.<index>.name – specify the alias [hostname string] Aliases are used for name changes, alternate spellings, shorter hostnames, or generic hostnames (eg. localhost).

Example:

```
resolv.status=enabled
resolv.nameserver.1.ip=204.74.112.1
resolv.nameserver.2.ip=204.74.112.2
resolv.search.1.domain=domain1.net
resolv.search.2.domain=domain2.net

resolv.host.1.ip=127.0.0.1
resolv.host.1.name=host.domain1.net
resolv.host.1.alias.1.name=fireball
resolv.host.1.alias.2.name=localhost.localdomain
resolv.host.1.alias.3.name=localhost
```

6.2.5 DNS Forwarder

DNS request forwarder, called DNSMASQ, intercepts all DNS requests from wireless/LAN clients and forwards them to a particular DNS server(s) which may be defined in the system configuration file or dynamically obtained through DHCP lease (forwarder will check for changes to system's DNS settings on every DNS request). Forwarder has a cache which speeds up DNS requests and reduces network traffic. It listens on the standard DNS TCP and UDP ports 53 on interfaces specified in the configuration file. Two firewall rules are required for forwarder to function correctly.

The available keys of the DNS forwarder feature are listed below:

dnsmasq.status – specify the DNSMASQ feature status [enabled/disabled].

dnsmasq.<index>.status – specify current DNSMASQ entry status [enabled/disabled].

dnsmasq.<index>.devname – specify the input interface name.

The example below shows setup of the firewall configuration specific to DNSMASQ. Refer to section 6.4.3 *IP Firewall* for further firewall configuration details.

Example:

```
# configure DNSMASQ on ath0 interface
# first configure redirection of DNS ports
firewall.status=enabled
firewall.rule.1.table=nat
```

```
firewall.rule.1.chain=PREROUTING
firewall.rule.1.protocol=TCP
firewall.rule.1.in=ath0
firewall.rule.1.dport=53
firewall.rule.1.target=REDIRECT
firewall.rule.2.table=nat
firewall.rule.2.chain=PREROUTING
firewall.rule.2.protocol=UDP
firewall.rule.2.in=ath0
firewall.rule.2.dport=53
firewall.rule.2.target=REDIRECT
```

```
# enable DNSMASQ on ath0
dnsmasq.status=enabled
dnsmasq.1.devname=ath0
```

6.2.6 VLANs



Up to 4094 VLANs can be created on the system.

Virtual Local Area Networks (VLANs) are logical groupings of network resources, e.g. public access users can be separated from company Intranet users using VLANs on the Ethernet interface. Access control policies can be applied on a per-VLAN basis. VLANs are uniquely identified by VLAN id number. Setting up a VLAN on physical interface will create virtual network interface named like a physical interface with dot and VLAN id appended, e.g. setting VLAN with id 10 on interface `ixp0` will create virtual interface called `ixp0.10`.

All available keys for VLAN configuration are listed below:

vlan.status – specify the VLAN feature status [enabled/disabled]. Default: disabled.

vlan.<index>.status – specify the VLAN status [enabled/disabled]. Default: enabled.

vlan.<index>.parent – specify the LAN interface name to make VLAN on.

vlan.<index>.id – assign ID for your VLAN network [2-4095]. Devices configured with the same ID (e.g. access points) are logically grouped into this VLAN.

Per-VLAN QoS offers differentiated quality of services to individual VLANs on a trunk port. A per-VLAN service policy can be separately applied to either ingress or egress traffic.

vlan.<index>.priority_in – specify either manual or auto mappings for egress packets will be set [auto/manual]. Default: manual.

vlan.<index>.priority_out – specify either manual or auto mappings for egress packets will be set [auto/manual]. Default: manual.

The ingress mapping – maps VLAN QoS field (3 bits) to local packet priority field (32 bits).

vlan.<index>.prio_in_map.<index>.vlan_qos – specify the ingress VLAN priority in bits [0...7].

vlan.<index>.prio_in_map.<index>.pkt_prio – specify the ingress packet priority in bits [0...0x7fffff].

The egress mapping – maps local packet priority field to VLAN QoS field:

vlan.<index>.prio_out_map.<index>.vlan_qos – specify the egress VLAN priority in bits [0..7].

vlan.<index>.prio_out_map.<index>.pkt_prio – specify the egress packet priority in bits [0..0x7fffff].

If vlan.<index>.priority_in/out=manual, user-configured mappings for ingress/egress packets will be set. If no mapping found, will map to 0 (same as default without any mappings); if vlan.<index>.priority_in=auto, 0:0, 1:1, ..7:7 mappings will be generated.

vlan.<index>.prio_out_map.<index>.vlan_qos – specify the egress VLAN priority in bits [0..7].

vlan.<index>.prio_out_map.<index>.pkt_prio – specify the egress packet priority in bits [0..0x7ffffff].

If vlan.<index>.priority_in/out=manual, user configured mappings for ingress/egress packets will be set. If no mapping found, will map to 0 (same as default without any mappings); if vlan.<index>.priority_in =auto, 0:0, 1:1,..7:7 mappings will be generated.

Example:

```
# configure VLAN id 10 on ixp0
vlan.status=enabled
vlan.1.devname=ixp0
vlan.1.id=10
```

6.2.7 IPsec

The IPsec protocol client enables the ShadowMaster to establish a secure connection to an IPsec peer via the Internet. IPsec is supported in two modes - transport and tunnel. Transport mode creates secure point to point channel between two hosts, eg. AP and client. Tunnel mode can be used to build a secure connection between two remote LANs serving as a VPN solution. A number of independent secure channels of either mode may be established simultaneously.

IPsec can be configured using the following keys:

ipsec.status – specify the IPsec service status [enabled/disabled].

ipsec.<index>.status – specify the IPsec entry status [enabled/disabled]. Default: disabled.

ipsec.<index>.mode – specify the IPsec operating mode for this entry [transport/tunnel].

ipsec.<index>.point_src.ip – specify the source IP address.

ipsec.<index>.point_dst.ip – specify the destination IP address.

ipsec.<index>.ah.in.spi – specify the inbound security parameter index [256-65535].

ipsec.<index>.ah.out.spi – specify the outbound security parameter index [256-65535].

ipsec.<index>.ah.algo – specify the authentication algorithm [hmac-md5/hmac-sha1/keyed-md5/keyed-sha1/null/hmac-sha2-256/hmac-sha2-384/hmac-sha2-512/hmac-ripemd160/aes-xcbc-mac].

ipsec.<index>.ah.secret – specify the authentication secret [string]. Secret's length depends on selected algorithm, eg. 128 bit long secret is 16 characters in length, 128 bits / 8 bits (one character) = 16. The algorithm key lengths in bits are:

- hmac-md5 - 128
- hmac-sha1 - 160
- keyed-md5 - 128
- keyed-sha1 - 160
- null - 0 to 2048
- hmac-sha2-256 - 256
- hmac-sha2-384 - 384
- hmac-sha2-512 - 512
- hmac-ripemd160 - 160
- aes-xcbc-mac - 128

ipsec.<index>.esp.in.spi – specify the inbound compression [256-65535].

ipsec.<index>.esp.out.spi – specify the outbound compression [256-65535].

ipsec.<index>.esp.auth.algo – specify the ESP authentication algorithm [hmac-md5/hmac-sha1/keyed-md5/keyed-sha1/null/hmac-sha2-256/hmac-sha2-384/hmac-sha2-512/hmac-ripemd160/aes-xcbc-mac].

ipsec.<index>.esp.auth.secret – specify the ESP authentication secret [string]. Secret's length depends on selected algorithm, eg. 128 bit long secret is 16 characters in length, 128 bits / 8 bits (one character) = 16. The algorithm key lengths in bits are:

- des-cbc - 64
- null - 0 to 2048
- blowfish-cbc - 40 to 448
- cast128-cbc - 40 to 128
- des-deriv - 64
- 3des-deriv - 192
- rijndael-cbc -128/192/256
- twofish-cbc - 0 to 256
- aes-ctr - 160/224/288

ipsec.<index>.ipcomp.in.spi – specify the inbound compression [256-65535].

ipsec.<index>.ipcomp.out.spi – specify the outbound compression [256-65535].

ipsec.<index>.ipcomp.compression – specify the compression mode [deflate/oui/lzs].

ipsec.<index>.spd.<index>.status – specify current SPD (security policy database) entry status [enabled/disabled].

ipsec.<index>.spd.<index>.src.ip – specify the SPD source IP address.

ipsec.<index>.spd.<index>.src.netmask – specify the source netmask bit-count [0-32].

ipsec.<index>.spd.<index>.dst.ip – specify the SPD destination IP address.

ipsec.<index>.spd.<index>.dst.netmask – specify the destination netmask bit-count [0-32].

ipsec.<index>.spd.<index>.protocol.<index>.status – specify current SPD protocol entry status [enabled/disabled]. Default: enabled.

ipsec.<index>.spd.<index>.protocol.<index>.name – specify the SPD protocol name [esp/ah/ipcomp]. The SPD protocol name is mandatory parameter.

ipsec.<index>.spd.<index>.protocol.<index>.level – specify the level [default/use/require/unique]. Default level "require" will be used for esp and ah protocols. Default level "use" will be added to ipcomp protocol.

Example:

The sample configuration below defines a policy, which allows the ShadowMaster device with IP address 192.168.4.8 to access stations on LAN2 (IP address range 192.168.2.0/24) behind IPsec supporting router 192.168.4.10. IPsec tunnel is set between the ShadowMaster device and the router. Do not forget to setup routing on 192.168.4.8 so it knows that LAN2 (192.168.1.0/24) network is reachable through 192.168.4.10. Otherwise packets leaving the device and destined for LAN2 will be routed through the default gateway (which might not be the case in your setup, be careful).

```
# 192.168.4.8 (ShadowMaster) <===== LAN1 =====> 192.168.4.10 (Router)
#                                     ^
# Station 1 (192.168.1.2) ----- LAN2 (192.168.1.0/24) -----
#
# Station 2 (192.168.1.103) -----+
#
ipsec.status=enabled
ipsec.1.mode=tunnel
```



```
# tunnel end point IP addresses : local/remote
ipsec.1.point_src.ip=192.168.4.8
ipsec.1.point_dst.ip=192.168.4.10

# Security Policy Indexes (SPI) (value in HEX)
ipsec.1.esp.out.spi=0x4000
ipsec.1.esp.in.spi=0x5000

# authentication key 'alabrstysaaslu!e' or hexadecimal
# 16c616272737479736161736c752165
ipsec.1.esp.auth.algo=hmac-md5
ipsec.1.esp.auth.secret=alabrstysaaslu!e

# encryption key 'alabrsty' or in hexadecimal 616c616272737479 ipsec.1.esp.enc.algo=des-cbc
ipsec.1.esp.enc.secret=alabrsty

# Security Policy Database (SPD) entries
ipsec.1.spd.1.src.ip=192.168.4.8
ipsec.1.spd.1.src.netmask=32
ipsec.1.spd.1.dst.ip=192.168.1.0
ipsec.1.spd.1.dst.netmask=24
ipsec.1.spd.1.protocol.1.name=esp
ipsec.1.spd.1.protocol.1.level=require

# install route telling 192.168.1.0/24 is behind 192.168.4.10
# do not forget to adjust 20 to a reasonable value
route.20.ip = 192.168.1.0
route.20.netmask = 24
route.20.devname = ixp1
route.20.gateway = 192.168.4.10
```



The IPSec Tunnel (VPN Gateway) should be configured at the remote router (192.168.4.10) side properly.

The valid configuration should include settings like:

- Local Secure Network (192.168.1.0/255.255.255.0)
- Remote Secure Gateway IP address (192.168.4.8)
- Key Exchange Method (Manual)
- Encryption Algorithm (DES)
- Encryption Key (value in hexadecimal is "616c616272737479")
- Authentication Algorithm (MD5)
- Authentication Key (value in hexadecimal is "616c616272737479736161736c752165")
- Inbound SPI (value in HEX is "4000")
- Outbound SPI (value in HEX is "5000")

6.2.8 IPsec Racoon

The establishment of the Security Association (IPsec-SA) between two peers is needed for IPsec communication. It can be done by using manual or automated configuration.

IPsec Racoon uses the Internet Key Exchange (IKE) for automatically keying IPsec connections.

Several parameters (Keys) are exchanged between peers in order to establish the IPsec-SA. The Racoon exchange routine by using IKE has two phases: establishing SA for own communication (IKE-SA) and establishing IPsec-SA.

The IPsec system maintains two databases: Security Policy Database (SPD) which defines whether to apply IPsec to a packet or not and specify which/how IPsec-SA is applied and Security Association Database (SAD), which contains a Key of each IPsec-SA.

The basic mechanism of applying the IPsec-SA to a packet is the following:

- The administrator sets a policy to SPD
- System refers to SPD in order to make a decision of applying IPsec to a packet
- If IPsec is required, then system gets the Key for IPsec-SA from SAD
- If it has failed, then system sends a request to get the Key to IPsec Racoon
- IPsec Racoon exchanges the Key by using IKE with the other to be established IPsec-SA
- IPsec Racoon put the Key into SAD
- System can now send a packet applied IPsec



Racoon needs access to UDP port 500. Make sure that your firewall configuration does not block this port.

IPsec Racoon can be configured using the following keys:

racoon.status – specify the status of racoon service [enabled/disabled].

racoon.psk.<index>.status – specify current configuration entry status [enabled/disabled].
Default: enabled.

racoon.psk.<index>.identifier – specify the remote host IP address.

racoon.psk.<index>.secret – specify the secret pre-shared key [string].

Example:

```
racoon.status=enabled
racoon.psk.1.status=enabled
racoon.psk.1.identifier=192.168.2.151
racoon.psk.1.secret=VeRy$ecr3t
```

6.2.9 GRE Tunnels

GRE (Generic Routing Encapsulation [RFC2784](#)) is a solution for tunnelling [RFC1812](#) private address-space traffic over an intermediate TCP/IP network such as the Internet. GRE tunnelling does not use encryption; it simply encapsulates data and sends it over the WAN. Administrators should therefore take care that no unencrypted private information passes through a GRE tunnel. Created GRE tunnels will appear as regular network interfaces, e.g., gre1, gre4.



The <index> range for GRE tunnels is 1-100.

tunnel.gre.status – specify the GRE tunnel status [enabled/disabled]. Default: disabled.

tunnel.gre.<index>.status – specify current GRE entry status [enabled/disabled]. Default: enabled.

tunnel.gre.<index>.devname – specify custom GRE tunnel interface name [custom string up to 15 characters in length]. Bind the tunnel to the specified interface so that tunnelled packets will only be routed through this interface and will not escape to another interface when the route to endpoint changes. If not specified, default interface name will be gre<index>.

tunnel.gre.<index>.local.ip – specify the fixed local IP address for tunnelled packets. It must be an address of another interface of the device. Default '0.0.0.0' means that no fixed address will be used for local endpoint. In this case local endpoint address for that tunnel will be automatically assigned by the routing process.

tunnel.gre.<index>.remote.ip – specify the remote tunnel endpoint IP address. Default '0.0.0.0' means accept any remote endpoint.

tunnel.gre.<index>.parent – specify the parent interface name. Bind the tunnel to the specified interface so that tunnelled packets will only be routed through this interface and will not be able to escape to another interface when the route to endpoint changes.

tunnel.gre.<index>.ttl – specify the fixed time-to-live (TTL) value on tunnelled packets [0-255]. The 0 is a special value meaning that packets inherit the TTL value. Default: 0.

tunnel.gre.<index>.pmtudiscovery – the Path Maximum Transmission Unit Discovery (PMTUD) status on this tunnel [enabled/disabled]. Default: enabled.

Example:

```
tunnel.gre.status=enabled
tunnel.gre.1.status=enabled
tunnel.gre.1.devname=gre_1
tunnel.gre.1.local.ip=192.168.2.12
tunnel.gre.1.parent=ixp1
tunnel.gre.1.remote.ip=192.168.2.13
tunnel.gre.1.pmtudiscovery=disabled
```

This configuration will create a GRE tunnel with following parameters: gre_1 – remote end IP 10.15.14.1, local end will use IP address 192.168.2.12 bound to ixp1 interface (it should already be configured), TTL value will be inherited, path MTU discovery disabled.

6.2.10 PPPoE Settings

PPPoE is a protocol typically used by DSL providers to manage IP addresses and authenticate users. Essentially, PPPoE provides for a PPP connection to be established not over a physical serial-line or mode, but over a logical connection between two unique MAC addresses on an Ethernet network.

pppoe.status – specify the status of the PPPoE [enabled/disabled]. Default: disabled.

pppoe.<index>.status – specify the status of the particular PPPoE profile [enabled/disabled].

pppoe.<index>.name – specify name of the PPPoE profile [string]

pppoe.<index>.devname – specify name of the interface peer can be connected through [string]. The interface should be "up" before you start PPPoE, but should not be configured to have an IP address (refer to the section *Interface* for detailed information on interface configuration).

pppoe.<index>.user – specify name which will be used for authenticating the local system to the peer [string].

pppoe.<index>.password – specify the password for the user authentication [string].

pppoe.<index>.service_name – specify the service name set on the access concentrator [string]. PPPoE will only initiate sessions with access concentrators which can provide the specified service.

pppoe.<index>.ac_name – specify the desired access concentrator name [string]. PPPoE will only initiate sessions with the specified access concentrator.

pppoe.<index>.maxfail – terminate after n consecutive failed connection attempts [integer]. Default: 0.

pppoe.<index>.mtu – specify the Maximum Transmission Unit [integer]. Default: 1500.

pppoe.<index>.mru – specify the Maximum Received Unit [integer]. Default: 1500.

pppoe.<index>.add_default_route – set enabled to add a default route to the system routing tables using the peer as the gateway, when IPCP negotiation is successfully completed [enabled/disabled]. Default: enabled.

pppoe.<index>.use_peer_dns – specify to use peer's DNS servers [enabled/disabled] Default: enabled.

pppoe.<index>.lcp_echo_failure – specify the number of LCP echo-requests that will be sent without receiving a valid LCP echo-reply at which the pppd will consider the peer to be dead [integer]. If this happens, pppd will terminate the connection. Use of this option requires a non-zero value for the lcp-echo-interval parameter. This option can be used to enable pppd to terminate after the physical connection has been broken (e.g., the modem has hung up) in situations where no hardware modem control lines are available.

pppoe.<index>.lcp_echo_interval – Specify the time interval in seconds at which an LCP echo-request frame will be sent by the pppd to the peer [integer]. Normally the peer should respond to the echo-request by sending an echo-reply. This option can be used with the lcp-echo-failure option to detect that the peer is no longer connected.

pppoe.<index>.debug – specify connection debugging status [enabled/disabled]. Default: disabled]. If this option is given, pppd will log the contents of all control packets sent or received in a readable form. The packets are logged through syslog with facility daemon and level debug.

Example:

```
pppoe.status=enabled
pppoe.1.status=enabled
pppoe.1.name=pppoe
pppoe.1.user=user_name
pppoe.1.password=user_password
pppoe.1.devname=ixp0
pppoe.1.mtu=1460
pppoe.1.mru=1460
```

6.3 Wireless Settings

This section describes radio hardware (**Wireless Radio**) and wireless interface settings (**Wireless Interface**), WLAN locking, VSSID, wireless access control list (ACL), client bridge, station supervision settings.

6.3.1 Wireless Radio

This section provides the description of the general parameters of the radio hardware such as:

- Country code
- IEEE mode
- Auto channel selection
- Radio operating mode
- Turbo mode
- Data transfer rate
- Fragmentation
- Distance settings (ACK timeout, RTS, CTS)
- Transmit power (dBm)
- RX/TX antenna diversity
- Half and quarter rate channel support
- FCC security band support

All available keys of the radio hardware configuration are listed below:

radio.status – specify the radio module status [enabled/disabled]. Default: disabled.

radio.countrycode – specify the device's country code. Refer to *Appendix E: ISO Country Codes* for your country code. The country code can be specified as 2 or 3 letters or number code. The country code helps to ensure compliance with your local regulatory requirements. Ensure that you set this to your operating country.

radio.outdoor – specify the operation mode [0/1]. 0 is indoor, 1 is outdoor. Default: 0.

radio.xchanmode – specify the extended channel mode status [0/1]. 0 is disabled, 1 is enabled. Default: 1.

radio.<index>.status – specify current radio configuration entry status [enabled/disabled].

radio.<index>.devname – specify current wireless interface name.

radio.<index>.parent – the hardware wireless interface name, eg. wifi0, wifi1 [string].

radio.<index>.mode – specify the operating mode of the device [Managed/Master]. The device mode depends on the network topology.

- **Managed.** In this mode node connects to a network composed of many access points with roaming.
- **Master.** In this mode node is the synchronization master or acts as an access point.

radio.<index>.channel – specify the wireless channel [auto/number]. Multiple channels are available to avoid interference between nearby access points. If you wish to operate more than one access point in overlapping coverage areas, we recommend a distance of at least four channels between the chosen channels. The list of available channels is in *Appendix B: Regulatory Domain/Channels*. Ensure that the channel you have selected meets your specific regulatory requirements for power levels, indoor/outdoor usage.

In the **master** operating mode the ShadowMaster has the **auto channel** function. It is used to find the best channel for client-access point communication (either an unused channel or if all are in use the least occupied one - that with the lowest measured signal strength). The channel list to select channels from can be specified for auto channel.

radio.<index>.autochannel.status – specify the auto channel status [enabled/disabled].

radio.<index>.autochannel.<index>.status – specify current auto channel entry status [enabled/disabled].

radio.<index>.auto channel.<index>.channel – specify one channel from auto channel list [number, depends on country code settings and operation mode]. The list of available channels is in the appendix B) Regulatory Domain/Channels.

radio.<index>.rate.max – specify the wireless transmission speed (in bits/sec, by default). Real data transmission speed will be lower due to distance, obstacles in wireless signal path and wireless protocol overhead. You may append the suffix k, M or G to the value (decimal multiplier: 10^3 , 10^6 and 10^9 bits/s), or add enough zeros.

Wireless Network Mode	The Bit-Rates (Mbps)
B	1Mbps 2Mbps 5.5Mbps 11Mbps
G	1Mbps 2Mbps 5.5Mbps 11Mbps 6Mbps 9Mbps 12Mbps 18Mbps 24Mbps 36Mbps 48Mbps 54Mbps
A	6Mbps 9Mbps 12Mbps 18Mbps 24Mbps 36Mbps 48Mbps 54Mbps

radio.<index>.rate.auto – specify the automatic bit-rate mode status [enabled/disabled]. Default: enabled. This setting sets automatic bit-rate mode with fallback to lower rate on noisy channels. If you specify a bit-rate value (*radio.<index>.rate.max*) and set auto to enabled, the ShadowMaster will use all bit-rates lower or equal to this value.

radio.<index>.frag – specify the fragmentation threshold (in bytes), which determines whether data frames will be fragmented and at what size [256-2346/off/auto]. On an 802.11 wireless LAN, frames exceeding the fragmentation threshold will be fragmented, i.e., split into smaller units suitable for the circuit size. Data frames smaller than the specified fragmentation threshold value is not fragmented. Default: auto.

Setting a lower fragmentation threshold value can help improve connection reliability in noisy environments (where radio interference is present). This mechanism does add overhead and therefore reduces effective throughput.

radio.<index>.rts – specify the maximum packet size beyond which the wireless LAN card invokes its RTS/CTS mechanism [0-2347/off/auto]. Packets that exceed the specified RTS threshold trigger the RTS/CTS mechanism. The card transmits packets smaller than this threshold without using RTS/CTS. Default: off.

Setting a lower RTS threshold value can improve connection reliability and throughput in crowded wireless LAN environments (where many clients are trying to communicate simultaneously). It adds a certain amount of overhead, but can compensate for this by reducing bandwidth lost due to collisions.

radio.<index>.txpower – specify the wireless card transmission power in dBm [auto/off/number]. Default: auto. Ensure that the transmit power meets your specific regulatory requirements for your particular country, antenna and channel.

radio.<index>.ieee_mode – specify the wireless network mode [auto/A/AST/B/G/PUREG]. Default: auto. Meaning of auto depends on operating mode (*radio.<index>.mode*). If operating mode is Master then A mode will be set. For B/G-only radios, G mode will be set. If operating mode is Managed, radio will begin searching for AP starting with A mode and then switching to B and G until it finds an AP to associate to. PUREG mode means accepting only G clients (aka G-only mode). AST means 802.11a Static Turbo mode.



Check with your country regulations before setting Static Turbo mode.

radio.<index>.turbo – specify the status of dynamic turbo mode [enabled/disabled]. Default: disabled. Set dynamic turbo mode with combination of throughput enhancement functionality (see: *wireless.<index>.fastframes*, *wireless.<index>.frameburst*, *wireless.<index>.compression* keys description in next section)



Turbo mode is available only for 802.11a and 802.11g.

radio.<index>.rx_antenna – specify antenna for receiving [1/2]. Default: 1. 1 is for the external antenna, 2 is for the internal 5 GHz antenna. Radio 1 can be set to either 1 or 2. Radio 2 can only be set to 1.

radio.<index>.rx_antenna_diversity – specify receiving antenna diversity status [enabled/disabled]. Default: enabled. Antenna diversity controls the signal strength on each

antenna and switches to the one with better strength. This works if `radio.<index>.rx_antenna` is set to 2.

radio.<index>.tx_antenna – specify antenna for transmitting [1/2]. Default: 1. 1 is for the external antenna, 2 is for the internal 5 GHz antenna. Radio 1 can be set to either 1 or 2. Radio 2 can only be set to 1.

radio.<index>.tx_antenna_diversity –specify the transmitting antenna diversity status [enabled/disabled]. Default: enabled. Antenna diversity controls the signal strength on each antenna and switches to the one with better strength. This works if `radio.<index>.tx_antenna` is set to 2.

radio.<index>.slottime -- specify the Slot time value [numeric]. Value = $9 + (\text{distance} / 300)$, rounded up, where distance is in meters (eg. slot time for 1 kilometre is 12.333, rounded up to 13).

radio.<index>.acktimeout – specify the ACK timeout value [numeric value]. Value = $3 + (\text{slottime} * 2)$ (eg. if distance is 1 kilometre, then slot time is 13 and ACK timeout value is 29).

radio.<index>.ctstimeout -- specify the CTS timing value [numeric]. Value = $3 + (\text{slottime} * 2)$ (eg. if distance is 1 kilometre, then slot time is 13 and so the ACK timeout value is 29).



Hint for setting appropriate `slottime`, `acktimeout` and `ctstimeout` values

Distance	5GHz	5GHz-turbo	2.4GHz-G
-2km	ack/ctstimeout=33 slottime=15	ack/ctstimeout=31 slottime=14	ack/ctstimeout=48 slottime=23
-5km	ack/ctstimeout=53 slottime=25	ack/ctstimeout=30 slottime=14	ack/ctstimeout=62 slottime=30
-10km	ack/ctstimeout=88 slottime=43	ack/ctstimeout=48 slottime=23	ack/ctstimeout=100 slottime=49
-15km	ack/ctstimeout=125 slottime=61	ack/ctstimeout=68 slottime=33	ack/ctstimeout=135 slottime=66
-20km	ack/ctstimeout=160 slottime=79	ack/ctstimeout=90 slottime=44	ack/ctstimeout=175 slottime=86
-25km	ack/ctstimeout=205 slottime=101	ack/ctstimeout=110 slottime=54	ack/ctstimeout=220 slottime=109

Basic ack-timeout setting methodology is this:

1. *Boost the value to the approximate value as above +20% on both endpoints*
2. *Evaluate link throughput*
3. *Decrease the value by 5% and evaluate link throughput*
4. *If the throughput has dropped rapidly, increase the value by 3-5%*
5. *Repeat the step 3*

radio.<index>.chanattr.<index>.status – specify the status of special channel attribute usage: channel bandwidth [enabled/disabled]. Default: enabled.

radio.<index>.chanattr.<index>.channel – specify one channel number on which bandwidth narrowing (half/quarter) will be set [channel].

radio.<index>.chanattr.<index>.bw -- specify desirable channel bandwidth for specified channel [full/half/quarter]. Default: full. Default channel bandwidth for 802.11 radio is 20MHz for

11a mode and 22 MHz for 11g mode (for turbo modes they double). It is possible to narrow it 2x or 4x times. Though this will drop data transfer rates accordingly, it will increase power density and may help to achieve greater operation distances.



Do not use channel bandwidth narrowing in turbo modes.

Example:

```
radio.status=enabled
radio.1.status=enabled
radio.1.acktimeout=55
radio.1.ctstimeout=55
radio.1.slottime=26
radio.1.autochannel.status=enabled
radio.1.autochannel.1.status=enabled
radio.1.autochannel.1.channel=1
radio.1.autochannel.2.status=enabled
radio.1.autochannel.2.channel=6
radio.1.autochannel.3.status=enabled
radio.1.autochannel.3.channel=11
radio.1.devname=ath0
radio.1.frag=off
radio.1.ieee_mode=G
radio.1.mode=master
radio.1.rate.auto=enabled
radio.1.rate.max=54M
radio.1.rts=off
radio.1.rx_antenna=1
radio.1.rx_antenna_diversity=disabled
radio.1.tx_antenna=1
radio.1.tx_antenna_diversity=disabled
radio.1.txpower=auto
```

6.3.2 Wireless Interface

This section provides the description of the general wireless LAN interface parameters. The administrator is able to setup using this section:

- WEP encryption
- SSID and broadcasting suppression
- Maximum number of clients
- Country element (IEEE 802.11d)
- Power constrain and channel switch for IEEE 802.11h
- Layer 2 isolation
- Throughput enhancements (fast frames, packet bursting, compression)
- WMM

All available wireless interface configuration keys are listed below:

wireless.status – specify the wireless interface function status [enabled/disabled]. Default: disabled.

wireless.<index>.status – specify the wireless interface entry status [enabled/disabled]. Default: enabled.

wireless.<index>.devname – specify the wireless interface name (eg. “ath0” or “ath1”).

wireless.<index>.ssid – specify a unique name for your wireless network. The string is case sensitive and up to 32 characters in length [printable characters and spaces, no control characters, mandatory].

wireless.<index>.ssid_broadcast – specify the master operating mode SSID broadcasting status [enabled/disabled]. When disabled the AP’s SSID will not show up in the network list when a client scans for available networks. By default SSID broadcasting is enabled. Do not use this feature as a security measure.

wireless.<index>.l2_isolation – specify the layer 2 wireless client separation status [enabled/disabled]. Layer 2 isolation blocks the wireless clients from communicating with each other.

wireless.<index>.max_clients – specify maximum number of connected clients [0-2147483647]. Default: 64.

wireless.<index>.security – specify the Wired Equivalent Privacy (WEP) encryption method [wep64/wep128/none]. Default mode is none.

wireless.<index>.security.mode – specify the security mode [restricted/open]. The default mode is restricted.

- **Restricted.** In this mode clients can connect only with WEP encryption configured.
- **Open.** This mode allows clients with WEP security or without any security to connect.

wireless.<index>.security.<index>.key – specify the WEP security keys. WEP keys should be entered as a series of colon-separated hexadecimal (0-9, A-F, and a-f) pairs:

- 5 pairs for 64-bit WEP security (e.g. 00:AC:01:35:FF)
- 13 pairs for 128-bit WEP security (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC)



You can configure up to 4 security keys.

wireless.<index>.security.default_key – specify the index of the default key, used to encrypt the data before it is transmitted [1-4].



The same key value must also be entered in the WLAN card configuration for each of the wireless clients.

wireless.<index>.authmode – specify the authentication mode of the AP [1/2/4]. Default: 4.

- **1 – Open system.** This setting allows any device, regardless of its WEP keys, to authenticate and attempt to associate.
- **2 – Shared key.** This setting tells the AP to send a plain-text, shared key query to any device that attempts to associate with the AP.
- **4 – Auto.** This setting uses both modes (Open system and Shared key).

wireless.<index>.country_element – specify the country element status [enabled/disabled]. Default: disabled. With this key enabled, system adds Country Element to beacons and probe responses according to IEEE 802.11d.

wireless.<index>.power_constrain – specify the power constrain status [enabled/disabled]. Default: disabled. With this key enabled, system adds Power Constrain to beacons and probe responses according to IEEE 802.11h.

wireless.<index>.chanswitch – specify the channel switch status [enabled/disabled]. Default: disabled. With this key enabled, system adds Channel Switch notification to beacons according to IEEE 802.11h.

wireless.<index>.fastframes – specify the fast frame status [enabled/disabled]. Default: disabled. Frame aggregation to super frame up to 3000B, thus maximizing efficiency via less overhead. Requires AP that supports fast frame functionality.

wireless.<index>.frameburst – specify the frame burst status [enabled/disabled]. Default: disabled. This technique allows transmitting more than one data frame during each transmission opportunity before station defers access to medium. Available for any capable station.

wireless.<index>.compression – specify packet compression status [enabled, disabled]. Default: disabled. real-time hardware Lempel Ziv data compression that increases data throughput using pre-compressed frames. Requires an AP that supports compression.

wireless.<index>.wmm – specify the WMM status [enabled/disabled]. Default: disabled. Wi-Fi Multimedia (WMM) is based on the IEEE 802.11e draft standard. It provides basic quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to 4 AC (Access Categories) - voice, video, best effort, and background.



WMM does not provide guaranteed throughput. It is suitable for simple applications that require QoS, such as Wi-Fi Voice over IP (VoIP) phone.

The keys of the QoS based on the DiffServ architecture:

wireless.<index>.tos2ac.<index>.status – specify the status of QoS [enabled/disabled]. Default: enabled. Enables packet classification on TOS value in IP header and dispatching to according radio queues. AC values 1..4 corresponds BK, BE, VO, VI queues. 2 LS bits in TOS not used and are masked out. Mapping record with tos=0 will be used as default rule for packets not matching any other configured mapping.

wireless.<index>.tos2ac.<index>.tos – specify the IP header TOS value, HEX format can be used, internally this value is masked with 0xfc, thus last 2 bits not used [HEX format].

wireless.<index>.tos2ac.<index>.ac – specify the queue in radio HW to select [1-4]. The queue value 4 means the highest priority.

wireless.<index>.tos2ac.<index>.drop – specify drop probability [0-2]. The value 2 means highest drop probability when queue getting full.

wireless.<index>.ap – specify the MAC address of the device to which the particular device will connect to [MAC address].

wireless.<index>.igmp_snooping – specify the IGMP snooping status [enabled/disabled]. Default: disabled. When enabled, AP will passively snoop on IGMP Report and Leave packets transferred between its clients and IP Multicast hosts. It checks IGMP packets passing through it, picks out the group registration information and generates internal L2 MAC forwarding table. Then it forwards multicast traffic using unicast packets directed according to forwarding table.

Example:

```
wireless.status = enabled
wireless.1.status = enabled
wireless.1.devname = ath0
wireless.1.ssid = my ssid
wireless.1.max_clients = 100
wireless.1.security = wep64
wireless.1.security.1.key = 00:AC:01:25:F2
wireless.1.security.2.key = 00:AC:01:35:F3
wireless.1.security.3.key = 00:AC:01:55:F5
wireless.1.security.default_key = 2
```

6.3.3 AutoLock WLAN

The ShadowMaster based device has the possibility to lock the WLAN. This feature checks (using ICMP echo request, like ping utility) if specific hosts are accessible on the network. When network goes down - wireless service will be disabled. When network is up again - wireless service will be re-enabled.

All available keys of the AutoLock WLAN feature are listed below:



The <index> range for AutoLock feature is 1-255.

autolock.status – specify the autolock feature status [enabled/disabled]. Default: disabled.

autolock.interval – specify the monitoring time period in seconds [number]. Default: 300 (5 min.).

autolock.retry_count – specify the number of failed reach ability checks, after which the wireless service will be disabled [0-3]. Default: 3.

autolock.verbose – specify verbose status [enabled/disabled].

autolock.<index>.status – specify current server entry status [enabled/disabled]. Default: enabled.

autolock.<index>.server – specify the IP address to be checked.

autolock.lock.action – specify the action on the lock event [none/down/up/kick/reboot]. Default: down.

none – no action will be applied on the interface.

down – bring the interface down

up – bring the interface up

kick – kick all wireless clients.

reboot – reboot the device

autolock.unlock.action – specify the action when connection to the network is re-established [none|down|up|kick|reboot]. Default: reboot.

none – no action will be applied on the interface.

down – bring the interface down

up – bring the interface up

kick – kick all wireless clients.

reboot – reboot the device

autolock.control.<index>.status – specify the status of the wireless interface control [enabled/disabled]. Default: enabled.

autolock.control.<index>.devname – specify the name of interface for control. If the interface is not specified, all wireless interfaces will be used from the file `/proc/net/wireless`.



AutoLock has no influence on routes. As soon as interfaces are brought down the routes will be deleted.

Example:

```
autolock.status = enabled
autolock.interval = 600
autolock.retry_count = 3
autolock.1.status = enabled
autolock.1.server = 213.29.25.154
autolock.2.status = enabled
autolock.2.server = 213.29.25.33
autolock.3.status = disabled
autolock.3.server = 212.22.99.66
autolock.4.status = enabled
autolock.4.server = 212.25.19.6
autolock.lock.action = down
autolock.unlock.action = reboot
autolock.control.1.status = enabled
autolock.control.1.devname = ath0
autolock.control.2.status = enabled
autolock.control.2.devname = ath1
```

In this configuration, 3 servers are pinged every 10 minutes (600s). One server checking is disabled. When at least one server does not respond 3 times - wireless interfaces ath0 and ath1 are brought down and wireless service will be disabled. When the service becomes available again - the device will be rebooted.

6.3.3.1 Virtual SSID (VSSID)



The master SSID should be preconfigured before adding VSSID.

The Service Set Identifier (SSID) defines a logical wireless network, and the ShadowMaster can be configured to provide another 15 wireless networks in addition to that defined by the primary SSID. Each additional SSID may be configured for different security settings (SSID, encryption, SSID broadcasting, layer 2 isolation, client limitation per SSID). All the SSIDs may be active at the same time meaning that client devices can associate to the access point using any of the SSIDs. In order to add/delete VSSID, the wireless card must be in master mode and the VSSID interfaces must be created before configuring them. Remember to create a *wireless* set of keys for each VSSID.

All available VSSID configuration keys are listed below:

vssid.status – specify the VSSID feature status [enabled/disabled].

vssid.<index>.status – specify current VSSID entry status [enabled/disabled].

vssid.<index>.parent – specify the master interface on which the VSSID will be created (eg. "ath0")

vssid.<index>.devname – specify the VSSID interface name [custom string up to 15 characters in length]. If not specified, default interface name will be ath0_<index>.

vssid.<index>.mode – specify the VSSID wireless mode [managed/master]. If this key is not specified, the VSSID will inherit the mode of the parent SSID. If you are planning to use VSSIDs with different modes (STA and AP) on the same physical radio, first interface must be configured in AP mode



The key `vssid.<index>.mode` affects the wireless throughput therefore this key must be used only if you are aware of the key use.

Example:

```
# create 2 new virtual wireless devices
vssid.status = enabled
vssid.1.status = enabled
vssid.1.parent = ath0
vssid.1.devname = ath0.v1
vssid.2.status = enabled
vssid.2.parent = ath0
vssid.2.devname = ath0.v2
```

6.3.4 Wireless Distribution System (WDS)

A **Wireless Distribution System (WDS)** allows you to create a wireless network infrastructure. Normally the access points must be connected to a wired network (LAN), which is generally an Ethernet. Once connected, these access points create wireless cells allowing wireless connection to the wired network. The WDS feature allows the access points to be wirelessly connected to another access point, eliminating the need for a wired connection between them.

Use the following tips when configuring WDS:

- WDS mode can be enabled on each wireless interface (including virtual interface: VSSID)
- In order for WDS peers to communicate, all the WDS network peers must operate on the same channel (frequency) and have the same security settings
- Both sides have to be connected (AP-STA infrastructure) prior to turning WDS mode on
- If you need only to bridge two wired networks, use *Wireless ACL* configuration to prevent undesired association of other clients



In case you don't use WPA security, create an ACL rule(s) to prevent undesired client association to the WDS.

Follow the steps to configure WDS link:

1. select the check-box to **enable** WDS service,
2. click the **New** button to add the new entry for WDS,
3. specify the **Parent device** - the interface name on which the WDS will be created,

All available keys of the WDS feature are listed below:

wds.status – specify the WDS feature status [enabled/disabled].

wds.<index>.status – specify the status of the particular WDS link [enabled/disabled].

wds.<index>.parent – specify the interface name on which the WDS will be created [string].

Example:

```
# Enable WDS mode on ath0 interface
wds.status = enabled
wds.1.status = enabled
wds.1.parent = ath0
```

6.3.5 Wireless ACLs

Use the wireless access control list (ACL) service to control default access to the wireless network interfaces (ath0, ath1 and VSSIDs) or to define special access rules for wireless clients.

All available keys of the wireless ACL feature are listed below:

wacl.status – specify the ACL service status [enabled/disabled].

wacl.<index>.status – specify current ACL rule status [enabled/disabled]. Default: enabled.

wacl.<index>.devname – specify the wireless interface name on which the wireless interface rules will be assigned.

wacl.<index>.policy – specify the policy for *wacl.<index>.acl.<index>.mac* entries [open/allow/deny]. Default: open.

- open – policy means that no ACL will be used and ACL MAC entries will be ignored.
- allow – policy means that all clients are allowed except the ones in a list.
- deny – policy means that all clients are denied, only the ones in a list are allowed.

wacl.<index>.acl.<index>.status – specify current ACL entry status [enabled/disabled]. Default: enabled.

wacl.<index>.acl.<index>.mac – specify the MAC address of the wireless client [colon separated 6 hexadecimal value pairs].

Example:

```
# allow access to ath0 only from 1 MAC address
wacl.status = enabled
wacl.1.devname = ath0
wacl.1.policy = deny
wacl.1.acl.1.mac = 00:02:6f:22:32:d9
```

6.3.6 Wireless Client Bridge

The concept behind making a wireless client work as a bridge is to send all packets coming from the Ethernet side as wireless client packets. In order to do this, the MAC address of the Ethernet packets must be changed to the MAC address of the wireless packets (this is because the 802.11 standard says that AP's will not accept any packet not coming from an associated wireless client).

The configuration of a Wireless Client Bridge contains Ethernet bridge table (ebtable) rules for packets (passing through the client's wireless interface), designed to control Layer 2 packets.

Follow the steps to configure the wireless client bridge service on the ShadowMaster device:

1. Setup wireless device (i.e. VSSID "ms1") in wireless client mode (refer to the section 6.3.2

Configuration file example:

```
vssid.status=enabled
vssid.1.status=enabled
vssid.1.parent=ath0
vssid.1.devname=ms1
wireless.2.status=enabled
wireless.2.devname=ms1
wireless.2.ssid=SSID_of_the_AP
```

2. Setup network devices (i.e.: ixp0, ath0, ms1 and br0) refer to the section Interface for more information). Configuration file example:

```
netconf.4.status=enabled
netconf.4.ip=192.168.2.184
netconf.4.netmask=255.255.255.0
netconf.4.up=enabled
netconf.4.devname=br0
```



Current STA bridge system implementation requires that bridge interface must have the IP address assigned.

3. Setup bridge device (refer to section 6.2.2 *The Bridge* for more information), add wireless interface and Ethernet interface(s) to the bridge. The configuration file example:

```
bridge.status=enabled
bridge.1.status=enabled
bridge.1.devname=br0
bridge.1.port.1.status=enabled
bridge.1.port.1.devname=ixp0
bridge.1.port.2.status=enabled
bridge.1.port.2.devname=ms1
```

4. Add client bridging firewall entries:

```
eatables.status=enabled
eatables.rule.1.table=nat
eatables.rule.1.chain=PREROUTING
eatables.rule.1.in=ms1
eatables.rule.1.target=arpnat
eatables.rule.1.t.arpnat_target=ACCEPT
eatables.rule.2.table=nat
eatables.rule.2.chain=POSTROUTING
eatables.rule.2.out=ms1
eatables.rule.2.target=arpnat
eatables.rule.2.t.arpnat_target=ACCEPT
```

6.3.7 Static Supervision

The station supervision service complements authentication, authorization and accounting (AAA) service (see Section 6.4.1 Authentication, Authorization and Accounting for details). AAA service notifies station supervision service which client stations should be monitored for availability. If no response is received from station after specified number of retries, user authenticated from that station is logged out. Basically there should always be station supervision service running for every interface the AAA service is running on.

ssid.status – specify the feature status [enabled/disabled]. Default: disabled.

ssid.<index>.status – specify the station supervision entry status [enabled/disabled]. Default: enabled.

ssid.<index>.devname – specify the interface name for supervision.

ssid.<index>.check.interval – specify the interval to check for client availability, in seconds [number]. Default: 20.

ssid.<index>.check.count – specify the number of retries after which a user is logged out from the system [1-99]. Default: 3.

Example:

```
# check stations on ath0 every minute
# after 5 failed retries user will be logged out
ssid.status=enabled
ssid.1.status=enabled
ssid.1.devname=ath0
ssid.1.check.interval=60
ssid.1.check.count=5
```

6.3.8 Static Routing



The <index> range for route entries is 1-100.

This service is used to set up static routes to specific hosts or networks through an interface. The interface must already be configured and enabled. While data packets travel through the ShadowMaster, the system examines the "destination IP address" of each packet and chooses an interface to forward the packet to. The system choice depends on static routing rules – entries, known as a routing table.

route.status – specify the status of routing service [enabled/disabled]. Default: disabled.

route.ip_forward – specify the IP forwarding status [enabled/disabled]. The disabled IP forward means that no routing or bridging will take place - packet received on one interface will not be forwarded through another interface.

route.<index>.status – specify current routing entry status [enabled/disabled]. Default: enabled.

route.<index>.devname – specify the network interface name.

route.<index>.gateway – specify the gateway IP address.

route.<index>.ip – specify the destination IP address. The destination address can be a network address or host IP address.

route.<index>.netmask – specify the destination netmask length in bits [bitmask number, e.g. 24]. The netmask is unnecessary for host routes.

route.<index>.type – specify the route type [unicast/local/broadcast/multicast/throw/unreachable/prohibit/blackhole]. Route type:

unicast – the route entry describes real paths to the destinations covered by the route prefix.

local – the destinations are assigned to this host. The packets are looped back and delivered locally.

broadcast – the destinations are broadcast addresses. The packets are sent as link broadcasts.

multicast – a special type used for multicast routing. It is not present in normal routing tables.

throw – a special control route used together with policy rules. If such a route is selected, lookup in this table is terminated pretending that no route was found. Without policy routing it is equivalent to the absence of the route in the routing table. The packets are dropped and the ICMP message net unreachable is generated. The local senders get an ENETUNREACH

unreachable – these destinations are unreachable. Packets are discarded and the ICMP message host unreachable is generated. The local senders get an EHOSTUNREACH error.

prohibit – these destinations are unreachable. Packets are discarded and the ICMP message communication administratively prohibited is generated. The local senders get an EACCES error.

blackhole – these destinations are unreachable. Packets are discarded silently. The local senders get an EINVAL error.

Example:

```
# the configuration of the default route
route.status=enabled
route.1.status=enabled
route.1.devname=ixpl
route.1.gateway=192.168.2.1
route.1.ip=0.0.0.0
route.1.netmask=0
route.ip_forward=enabled
```

6.3.9 Static Source Routing

Source routing is a routing method where a routing decision is made depending not only on packet's destination address, but also on source IP address.

Static source routing method enables routing certain packets to specified interfaces (GRE or IPsec tunnels, VLAN interfaces) according to the static source **Routing rules** and **Routing entries** in the table. Each routing table for identification purposes should have the "Name" and "ID" attributes.

Source Routing tables can be defined using the following keys:

route.table.<index>.status – specify the table entry status [enabled/disabled]. Default: enabled.

route.table.<index>.id – specify the table number [0-255]. The table numbers 0, 253-255 are reserved.



We strongly recommend not using the reserved table numbers. In case of misuse, the device can become unreachable and therefore it will need to be reset to factory defaults.

route.table.<index>.name – specify the table name [string without spaces].

route.<index>.table – specify the table number or name [0-255 or string without spaces]. Reserved numbers are 255 - local table, 254 - main table, 253 default table and 0 for unspecified table. Preferably use table name instead of number.

All the static source routing rules should be defined in **Routing rules** section or by using the key:

route.rule.<index>.status – specify the rule status [enabled/disabled]. Default: enabled.

route.rule.<index>.ip – specify the packet source IP address [IP address].

route.rule.<index>.netmask – specify the netmask length in bits [bitmask number, eg. 24].

route.rule.<index>.table – specify the existing table number or name for current rule [0-255 or string without spaces].

route.rule.<index>.prio – specify the rule priority [0-32767]. By default local table lookup priority is 0, main - 32766, and default - 32767. Priority allows the ShadowMaster to control the performed matching order (priorities are tested from the lowest to the highest until a match is found).

Example:

LAN interface has IP addresses 192.168.55.0/24. There is a GRE tunnel gre0001 with an IP address 10.0.0.2/24 set. The following rules create routing setup where 192.168.55.0/24 LAN stations are routed via a GRE tunnel.

```
# define "wisp1" routing table
route.table.1.id = 100
route.table.1.name = wisp1

# create static route entries in the table
route.1.devname = ixp0
route.1.ip = 192.168.55.0
route.1.netmask = 24
route.1.table = 100

# Set the default gateway
route.2.devname = gre0001
route.2.ip = 0.0.0.0
route.2.netmask = 0

# Set the gateway (GRE tunnel) IP address
route.2.gateway = 10.0.0.2
route.2.table = wisp1

# Set the decision how to route packets from 192.168.55.0/24:
route.rule.1.ip = 192.168.55.0
route.rule.1.netmask = 24
route.rule.1.table = wisp1
route.rule.1.prio = 100
```

6.3.10 Selective Source Routing

Selective Source Routing is referring to a dynamic routing capability. In particular, client station traffic will be routed according to RADIUS authentication request-response. The system routing mechanism works in the same manner as the static source routing, except the fact that the routing rules will be defined automatically during the authorization routines.

Each routing table is dedicated for separate tunnel (IPsec, GRE, VSSID or VLAN interface) while having the unique name, which is used as Tunnel-ID.

Selection of the route successful only if there exists a Tunnel-ID which corresponds to the "Tunnel-Assignment-ID" attribute provided by RADIUS on Access-Accept.



The same Tunnel-Assignment-ID RADIUS attribute value should be used in all the RADIUS accounting requests if it was available in the RADIUS Access-Accept packet.

In the provided example, the device should have configured tunnels while each of them should have assigned Tunnel-ID's. If there is no existing tunnel with corresponding Tunnel-ID, the authentication will fail and the client station will be denied any network access beyond the NAS device.



With source routing enabled, administrator must make sure that all source routing keys *route.rule.<index>.prio* values are in 10000-20000 range. The system authenticator will create dynamically source routes with priority in range 900-1000.

If there will be a few Tunnel-Assignment-ID alternatives matching available Tunnel-ID's on a device the first matching Assigned Tunnel ID will be selected with the lowest Tunnel-Preference RADIUS attribute value for the client source routing.

The default routing rules will be applied for the clients, which will get empty or no Tunnel-Assignment-ID on RADIUS Access-Accept packet.

Example 1:

Clients are coming on LAN interface, which has a DHCP server configured to lease IP addresses in the range of 192.168.3.0/24. By default, clients have 192.168.3.1 assigned as a default gateway. WAN interface ixp0 has 192.168.2.110 IP address. Also, there are a couple of GRE tunnel devices configured on device configured like this:

```
# WISP#1, creates tunnel interface 'GRE1'
tunnel.gre.1.status=enabled
tunnel.gre.1.remote.ip=192.168.2.253
tunnel.gre.1.ttl=64

# WISP#2, creates
tunnel interface 'GRE2'
tunnel.gre.2.status=enabled
tunnel.gre.2.remote.ip=192.168.2.252
tunnel.gre.2.ttl=64
```

Configure GRE1 and GRE2 interfaces:

```
# 192.168.2.110 (ixp0) <--- GRE tunnel ---> 192.168.2.252 (WISP#1-remote) -- / -- >
(WISP#1 NOC)
# 10.0.1.2 (gre1) <-----> (greX 10.0.1.1)
# so 172.16.1.x particular IP address is routed via 10.0.1.2 (which is default
gateway in case of selective routing)
#
# assign gre1 and gre2 ip addresses
netconf.dev.1.name=gre1
netconf.dev.1.type=tunnel
netconf.dev.1.mode=wan
netconf.dev.1.state=up
netconf.dev.1.ip=10.0.1.2
netconf.dev.1.netmask=255.255.255.0
netconf.dev.1.broadcast=10.0.1.255

netconf.dev.2.name=gre2
netconf.dev.2.type=tunnel
netconf.dev.2.mode=wan
netconf.dev.2.state=up
netconf.dev.2.ip=10.0.2.2
netconf.dev.2.netmask=255.255.255.0
netconf.dev.2.broadcast=10.0.2.255
```

Install a default route in each source routing table. Use a GRE tunnel's IP address as a default gateway (so that all traffic traversing these tables is routed through GRE tunnel). The system authenticator will create particular rules per IP address that depends on tunnel-id.

```
route.entry.1.enabled = true
route.entry.1.ip = 0.0.0.0
route.entry.1.netmask = 0
route.entry.1.interface = gre1
route.entry.1.gateway = 10.0.1.2
# important!
route.entry.1.table = 101

route.entry.2.enabled = true
route.entry.2.ip = 0.0.0.0
route.entry.2.netmask = 0
route.entry.2.interface = gre2
```

```
route.entry.2.gateway = 10.0.2.2
# important!
route.entry.2.table = 102
```

```
route.table.1.id=101
route.table.1.name=WISP1
```

```
route.table.1.id=102
route.table.1.name=WISP2
```

This creates GRE1 tunnel from 192.168.2.110 <-> 192.168.2.253 for a WISP1 clients traffic to transport. The same goes for GRE2 (192.168.2.110 <-> 192.168.2.252) for a WISP2 clients to transport. While client attempts to authenticate, RADIUS server reports tunnel-id "WISP1". Assuming that interface is present on device and configured properly, system authenticator adds the route on WISP1 table. When client is gone, system authenticator deletes the route automatically.

Example 2:

Enabled WAN interface gre0001 has Assigned Tunnel ID (table name) set to "WISP1". Other WAN's have empty Tunnel-ID. Assume that client has provided valid login credentials and RADIUS server is responding with Access-Accept.

Received RADIUS Access-Accept contains Tunnel-Assignment-ID:

- with value "WISP1" and client is successfully authenticated;
 - source route for that client is created through routing table named "WISP1";
 - all client traffic is routed through gre0001 interface using routing table "WISP1";
 - RADIUS accounting packets for that client include Tunnel-Assignment-ID attribute which contains the same value as it was in the Access-Accept: "WISP1";
 - after client session end source-route is removed;
- with value "BadWISP" and such routing table does not exist:
 - client authorization is refused and no source route is set up;
 - client session ends immediately.

6.4 Network Access Configuration

This section describes configuration keys for:

- AAA (authentication, authorization, accounting) including NAS, RADIUS servers and proxy configuration, RADIUS domains, Dynamic WEP
- WPA/802.1x supplicant
- IP and bridging firewall settings
- SMTP redirection

6.4.1 Authentication, Authorization and Accounting

AAA (Authentication, Authorization and Accounting) service configuration settings are split into three groups.

- Authentication configuration includes authentication backend (RADIUS) server settings and local security profiles (e.g. WPA for wireless station handling)

- Authorization configuration includes settings for authenticated users (like default bandwidth, session time limits, etc.)
- Accounting configuration includes accounting backend (RADIUS) server and accounting functionality related settings (failovers/backups, transmit/receive information sending)

To configure a fully functioning AAA service you must first create profiles, itemized below:

5. configure RADIUS authentication servers (refer to the respective section 6.4.1.2 RADIUS Authentication Servers)
6. configure RADIUS accounting servers (refer to the respective section 6.4.1.3 RADIUS Accounting Servers)
7. group authentication and accounting servers into RADIUS Domain(s) (refer to the respective section 6.4.1.4 RADIUS Domains (WISPs)),
8. create security profiles: WEP (refer to the respective section 6.4.1.5 Dynamic WEP Security) or WPA (see chapter 6.4.1.6 WPA/WPA2 Security),
9. create NAS entries for each interface on which Network Access Server (NAS) will be running (refer to the respective section 6.4.1.1 Network Access Server (NAS))
10. group NAS entries into AAA services (see information below)
11. if not yet created, configure wireless interfaces on which NAS will be running (refer to the respective section 6.3 Wireless Settings):

```
wireless.1.devname=<aaa.nas.<index>.devname>
wireless.1.security=wep64 | wep128 | none
wireless.1.security.1.key=xx:xx:xx:xx:xx | xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
wireless.1.security.default_key=1
```

12. create firewall chains that AAA service depends on (refer to the respective section 6.4.3 IP Firewall):

```
firewall.chain.1.name=acctin
firewall.chain.1.table=mangle
firewall.chain.1.parent=PREROUTING
```

```
firewall.chain.2.name=acctout
firewall.chain.2.table=mangle
firewall.chain.2.parent=POSTROUTING
```

```
firewall.chain.3.name=fwdusers
firewall.chain.3.table=filter
firewall.chain.3.parent=FORWARD
```

```
firewall.filter.FORWARD.policy=DROP
```

13. setup firewall rules for each AAA interface entry (refer to the respective section 6.4.3 IP Firewall):

```
firewall.rule.1.table=mangle
firewall.rule.1.chain=acctin firewall.rule.1.acct.in=<aaa.<index>.devname>
```

```
firewall.rule.2.table=mangle
firewall.rule.2.chain=acctout
firewall.rule.2.acct.out=<aaa.<index>.devname>
```

```
firewall.rule.3.table=filter
firewall.rule.3.chain=fwdusers
firewall.rule.3.auth.in=<aaa.<index>.devname>
```

```
firewall.rule.3.target=ACCEPT
```

```
firewall.rule.4.table=filter
firewall.rule.4.chain=fwdusers
firewall.rule.4.auth.out=<aaa.<index>.devname>
firewall.rule.4.target=ACCEPT
```

```
firewall.rule.5.status=enabled
firewall.rule.5.table=mangle
firewall.rule.5.chain=PREROUTING
firewall.rule.5.auth=auth
firewall.rule.5.auth.in=ath0
firewall.rule.5.target=NAS_MARK
```

14. if AAA interface is added to the bridge, setup bridging firewall rule (refer to the respective section 6.4.4 Bridging Firewall)

```
ebtables.rule.1.table=broute
ebtables.rule.1.chain=BROUTING
ebtables.rule.1.in=<aaa.nas.<index>.devname>
ebtables.rule.1.protocol=0x888e
ebtables.rule.1.target=DROP
```

aaa.status – specify the AAA service status [enabled/disabled, mandatory]. Default: disabled.

aaa.<index>.status – specify current AAA profile status [enabled/disabled]. Default: enabled.

aaa.<index>.name – specify the AAA profile name [string].

aaa.<index>.devname – specify the interface name to start AAA service on [string].

aaa.<index>.nas.<index>.status – specify the NAS profile entry status [enabled/disabled]. Default: enabled.

aaa.<index>.nas.<index>.profile – specify the NAS profile name [string].

aaa.<index>.wan.<index>.status – specify the WAN interface entry status [enabled/disabled]. Default: enabled. Enable this parameter and specify which interfaces have to be set up for outgoing traffic bandwidth control if you intend to use bandwidth control for users of AAA service,.

aaa.<index>.wan.<index>.devname – specify the WAN interface name for AAA [string].

Example:

Configuration file snapshot for an example described above should be like this:

```
aaa.status=enabled
aaa.1.status=enabled
aaa.1.devname=ath0
aaa.1.name=ath0-UAM-ixp1
aaa.1.nas.1.status=enabled
aaa.1.nas.1.profile=ath0-UAM
aaa.1.wan.1.status=enabled
aaa.1.wan.1.devname=ixp1
```

6.4.1.1 Network Access Server (NAS)

All available keys of the NAS configuration are listed below:

aaa.nas.<index>.status – specify the NAS profile status [enabled/disabled]. Default: disabled.

aaa.nas.<index>.verbose – specify verbose logging for the NAS status [enabled/disabled]. This setting may be useful for AAA troubleshooting. Default: disabled.

aaa.nas.<index>.name – specify the NAS profile name [string]. Default is same as *aaa.nas.<index>.devname*.

aaa.nas.<index>.identifier – specify the NAS identifier [string]. Default: <MAC address>: <SSID>.

aaa.nas.<index>.devname – specify the interface name to start NAS on.

aaa.nas.<index>.maxclients – specify a number of maximum simultaneous clients to be accepted on current NAS [number, limited by HW capabilities]. Default: 64. Value of 0 disables client limit checking - the system will allow as many clients simultaneously as it can handle.

aaa.nas.<index>.auth.status – specify the authentication status on NAS server [enabled/disabled]. Default: disabled.

aaa.nas.<index>.auth.<index>.status – specify current authentication entry status [enabled/disabled].

aaa.nas.<index>.auth.<index>.type – specify current authentication type [ieee802.1x/uam/radius_proxy]. The radius_proxy type instructs the NAS to act as a RADIUS proxy. This requires additional radius proxy settings to be configured. See section 6.4.1.4 *RADIUS Domains* (WISPs)

aaa.nas.<index>.auth.<index>.profile – specify the profile name [string].

aaa.nas.<index>.acct.status – specify the accounting status on NAS server [enabled/disabled]. Default: disabled.

aaa.nas.<index>.domain.<index>.status – specify current domain entry status [enabled/disabled].

aaa.nas.<index>.domain.<index>.profile – specify the domain (WISP) name [string]. This should be equal to *aaa.domain.<index>.domain* (see section 6.4.1.4 *RADIUS Domains* (WISPs)).

aaa.nas.<index>.domain.default – specify the default domain (WISP) index [number]. Default: 1.

aaa.nas.<index>.security.type – specify the security type [none/wep/wpa]. Default: none.

aaa.nas.<index>.security.profile – specify the security profile name [string]. This may be omitted if security type is none. It should be equal to *aaa.security.wep.<index>.name* or *aaa.security.wpa.<index>.name* (see sections 6.4.1.5 *Dynamic WEP Security* and 6.4.1.6 *WPA/WPA2 Security*)

The following properties are reported in RADIUS request packets. Most of them are used for WISPr compliance.

aaa.nas.<index>.properties.location.isocc – specify the location ID attribute, country code of the NAS location according ISO standards [2 characters].

aaa.nas.<index>.properties.location.cc – set the location ID attribute, country code according E.164 specification [1-3 digits].

aaa.nas.<index>.properties.location.ac – s set the location ID attribute, area code according E.164 specification of the NAS location [up to 8 digits].

aaa.nas.<index>.properties.location.network – specify the name of the location network zone [1-64 characters]. This may be equal to the SSID for wireless networks and domains for wired networks.

aaa.nas.<index>.properties.operator – specify the name of the operator owning this NAS zone [1-64 characters].

aaa.nas.<index>.properties.location – specify the detailed description of the location [1-128 characters].

aaa.nas.<index>.dynvlan.status – specify status of the dynamic VLAN service on the system [enabled/disabled]. Default: disabled

aaa.nas.<index>.dynvlan.default – specify the name of default VLAN interface [string]. If dynamic VLAN functionality is enabled on device, during authentication RADIUS server should respond with VLAN tag id. After successful authentication all client traffic will be tagged to specified VLAN. In case RADIUS server doesn't respond with VLAN id, the preconfigured VLAN will be used by default.

Example:

```
aaa.nas.<index>.dynvlan.status=enabled
```

```
aaa.nas.1.dynvlan.default=ixp0.3000
```

Clients that are authenticated, but RADIUS server doesn't specify VLAN id , VLAN 3000 will be used on ixp0 interface.

6.4.1.2 RADIUS Authentication Servers

All available keys of the RADIUS authentication server are listed below:

aaa.auth.<index>.status – specify the RADIUS authentication server profile status [enabled/disabled]. Default: enabled.

aaa.auth.<index>.name – specify the RADIUS authentication server profile name [string, mandatory].

aaa.auth.<index>.host – specify the RADIUS authentication server host name or IP address [hostname string or IP address, mandatory].

aaa.auth.<index>.port – specify the network port used to communicate with the RADIUS authentication server [0-65535]. Default is 1812.



The default port value of 1812 is set according to [RFC2138](#) "Remote Authentication Dial-in User Service (RADIUS)".

aaa.auth.<index>.timeout – specify the authentication request timeout in seconds [1-999]. Default: 2. If RADIUS response is not received during timeout period, request is retransmitted.

aaa.auth.<index>.retry – specify the number of times authentication request is retransmitted [0-99]. Default: 2. When all retry attempts are exhausted, authentication with this server is treated as failed.

aaa.auth.<index>.secret – specify the shared secret of the authentication server [string, mandatory]. The shared secret is used to encrypt data packets transmitted between RADIUS server and client.



Shared secrets must be the same on the RADIUS servers and the RADIUS client.

aaa.auth.<index>.stripdomain – specify the strip domain function status [enabled/disabled]. Default: disabled. Enabling this option removes the WISP domain prefix from the username before sending it to the RADIUS server (see section 6.4.1.4 *RADIUS Domains (WISPs)* for details). Default action is to send the username as is.



Some RADIUS servers can be configured to require the full-unmodified user name to be sent.

aaa.auth.<index>.authtype – specify the authentication type [PAP/CHAP/MSCHAP/MSCHAPV2]. Default: PAP.

PAP – Password Authentication Protocol

CHAP – Challenge Handshake Authentication Protocol

MSCHAP – Microsoft Challenge Handshake Authentication Protocol version 1

MSCHAPV2 – Microsoft Challenge Handshake Authentication Protocol version 2

Example:

```
aaa.auth.1.status=enabled
aaa.auth.1.host=192.168.2.182
aaa.auth.1.name=AUTH
aaa.auth.1.port=1812
aaa.auth.1.retry=5
aaa.auth.1.secret=password
aaa.auth.1.stripdomain=disabled
aaa.auth.1.timeout=15
aaa.auth.1.authtype=PAP
```

6.4.1.3 RADIUS Accounting Servers

All available keys of the RADIUS accounting server are listed below:

aaa.acct.<index>.status – specify the RADIUS accounting server profile status [enabled/disabled]. Default: enabled.

aaa.acct.<index>.name – specify the RADIUS accounting server profile name [string, mandatory].

aaa.acct.<index>.host – specify the RADIUS accounting server host name or IP address [string or IP address, mandatory].

aaa.acct.<index>.port – specify the network port used to communicate with the RADIUS accounting server [0-65535]. Default is 1813.



The default port value of 1813 is set according to [RFC2866](#) "RADIUS Accounting".

aaa.acct.<index>.timeout – specify the accounting request timeout in seconds [1-999]. Default: 2. If RADIUS response is not received during timeout period, request is retransmitted.

aaa.acct.<index>.retry – specify the number of times accounting request is retransmitted [0-99]. Default: 2.

aaa.acct.<index>.secret – specify the shared secret of the accounting server [string, mandatory]. The shared secret is used to encrypt data packets transmitted between RADIUS server and client.

aaa.acct.<index>.stripdomain – specify the strip domain function status [enabled/disabled]. Default: disabled. Enabling this option removes the WISP domain prefix from the username before sending it to the RADIUS server (see section 6.4.1.4 *RADIUS Domains (WISPs)* for details). Default action is to send the username as is.



Some RADIUS servers can be configured to require the full-unmodified user name to be sent.

Example:

```
aaa.acct.1.secret=password
aaa.acct.1.status=enabled
aaa.acct.1.host=192.168.2.182
aaa.acct.1.name=ACCT
aaa.acct.1.port=1813
aaa.acct.1.stripdomain=disabled
```

6.4.1.4 RADIUS Domains (WISPs)

The domain name is a string, uniquely identifying the Wireless Internet Service Provider (WISP). Access Controller can be shared between different WISPs. In this case the domain name can be appended to username to specify which WISP user is trying to authenticate to:

username@WISPdomain,
WISPdomain/username.

All available keys are listed below:

aaa.domain.<index>.status – specify the domain profile status [enabled/disabled]. Default: enabled.

aaa.domain.<index>.name – specify the domain (WISP) profile name [string].

aaa.domain.<index>.domain – specify the domain (WISP) name [string].

aaa.domain.<index>.auth.<index>.status – specify current authentication entry status [enabled/disabled]. Default: enabled.

aaa.domain.<index>.auth.<index>.profile – specify the authentication server profile for this domain [string]. This should be equal to *aaa.auth.<index>.name* (see section 6.4.1.2 *RADIUS Authentication Servers*).

aaa.domain.<index>.acct.<index>.status – specify current accounting entry status [enabled/disabled]. Default: enabled.

aaa.domain.<index>.acct.<index>.profile – specify the accounting server profile for this domain [string]. This should be equal to *aaa.acct.<index>.name* (see section 6.4.1.3 *RADIUS Accounting Servers*).

aaa.domain.<index>.acct.mode – specify the accounting mode [failover/backup]. Default: failover. This setting works when multiple accounting servers are specified. In backup mode the accounting information will be send to all servers at once, without waiting for accounting responses (assuming that accounting requests will be received by at least one server). In failover mode the accounting information will be sent to another RADIUS server only if the primary RADIUS server does not respond.

aaa.domain.<index>.default.sessiontimeout – specify the default user session timeout in seconds on particular domain [1-2147483647]. Default is 18000 (5 hours).

aaa.domain.<index>.default.idletimeout – specify the default user idle timeout in seconds on particular domain [1-999999999]. Default is 300 (5 minutes).

aaa.domain.<index>.default.maxrxbandwidth – specify the default maximum reception bandwidth in bps for a user on a particular domain [0-2147483647]. The default value is 0 and means unlimited bandwidth.

aaa.domain.<index>.default.maxtxbandwidth – specify the default maximum transmission bandwidth in bps for a user on a particular domain [integer]. The default value is 0 and means unlimited bandwidth.

aaa.domain.<index>.default.minrxbandwidth – specify the default minimum reception bandwidth in bps for a user on a particular domain [integer]. The default value is 0.

aaa.domain.<index>.default.mintxbandwidth – specify the default minimum transmission bandwidth in bps for a user on a particular domain [integer]. The default value is 0

aaa.domain.<index>.default.interim_update – specify default accounting interim update interval, in seconds [integer]. Default: 300. value 0 means disabled, minimum 60 seconds interval. By standard RADIUS server must be configured to send desired interim update interval in "Acct-Interim-Interval" request attribute. This value can only appear in the "Access-Accept" message. If such attribute is present, it overrides configured value. If attribute "Acct-Interim-Interval" was missing on "Access-Accept", default value will be used.

Example:

```
aaa.domain.1.status=enabled
aaa.domain.1.name=AAA
aaa.domain.1.acct.1.status=enabled
aaa.domain.1.acct.1.profile=ACCT
aaa.domain.1.acct.mode=failover
aaa.domain.1.auth.1.status=enabled
aaa.domain.1.auth.1.profile=AUTH
aaa.domain.1.default.idletimeout=300
aaa.domain.1.default.sessiontimeout=30000
aaa.domain.1.default.maxrxbandwidth=250000
aaa.domain.1.default.maxtxbandwidth=500000
aaa.domain.1.default.minrxbandwidth=0
aaa.domain.1.default.mintxbandwidth=0
aaa.domain.1.default.interim_update=240
```

6.4.1.5 Dynamic WEP Security Profile

This section describes configuration of dynamic WEP security for usage with AAA service. WEP is a data privacy mechanism based on a 64-bit or 128-bit shared key algorithm as described in the IEEE 802.11 standard.

All available keys of the Dynamic WEP configuration are listed below:

aaa.security.wep.<index>.status – specify current profile status [enabled/disabled].

aaa.security.wep.<index>.name – specify current WEP security profile name [string, mandatory].

aaa.security.wep.<index>.keylen.unicast – specify the length of individual/unicast key [0/5/13]. Default: 0.

0 – none,

5 – 40-bit WEP (also known as 64-bit WEP with 40 secret bits),

13 – 104-bit WEP (also known as 128-bit WEP with 104 secret bits).

aaa.security.wep.<index>.keylen.broadcast – specify the length of default/broadcast key [0/5/13]. Default value is equal to *aaa.security.wep.<index>.keylen.unicast* value.

0 – none,

5 – 40-bit WEP (also known as 64-bit WEP with 40 secret bits),

13 – 104-bit WEP (also known as 128-bit WEP with 104 secret bits).

aaa.security.wep.<index>.rekey.period – specify the rekeying period in seconds [0-3600]. Default value is 0 and means that rekeying is not used.

6.4.1.6 WPA/WPA2 Security Profile

Wi-Fi Protected Access (WPA) provides a higher level of protection for wireless LAN client stations as it includes methods for mutual authentication, strong encryption, and data integrity. WPA takes the original master key only as a starting point and derives its encryption keys dynamically from this master key. WPA regularly changes and rotates the encryption keys so that the same encryption key is never used twice. Key exchange is done automatically transparent to the user.

The WPA2 is the second generation of WPA security; providing enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. WPA2 is based on the final IEEE 802.11i amendment to the 802.11 standard.

All available keys of the WPA/WPA2 profile are listed below:

aaa.security.wpa.<index>.status – specify the WPA/WPA2 security profile status [enabled/disabled]. Default: enabled.

aaa.security.wpa.<index>.name – specify the WPA/WPA2 security profile name [string].

aaa.security.wpa.<index>.mode – specify the security mode [WPA/WPA2/ALL].

aaa.security.wpa.<index>.psk – specify the WPA pre-shared keys for WPA-PSK [64 hexadecimal values]. This value can be overridden by specifying *aaa.security.wpa.<index>.passphrase* described below.

aaa.security.wpa.<index>.passphrase – specify the WPA passphrase [8-63 characters]. The passphrase will be converted to pre-shared key format. This conversion uses SSID, so the key changes when ASCII passphrase is used and the SSID is changed. Provided passphrase overrides value of the *aaa.security.wpa.<index>.psk*.

aaa.security.wpa.<index>.key.method – specify the WPA key selection method [PSK/EAP/ALL]. PSK requires for keys *aaa.security.wpa.<index>.psk* or *aaa.security.wpa.<index>.passphrase* to be specified. When EAP is selected the NAS instance, which uses this profile, must support the IEEE 8021.x authentication method.

aaa.security.wpa.<index>.key.cipher – specify the encryption algorithms for pair-wise keys (unicast packets) [TKIP/CCMP/ALL].

TKIP = Temporal Key Integrity Protocol [IEEE 802.11i/D7.0],

CCMP = AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0],

ALL = includes CCMP and TKIP.

Group cipher suite (encryption algorithm for broadcast and multicast frames) is automatically selected based on this configuration. If only CCMP is allowed as the pair-wise cipher, group cipher will also be CCMP. Otherwise, TKIP will be used as the group cipher.

aaa.security.wpa.<index>.rekey.group.period – specify the time interval for rekeying the Group Temporal Key (GTK is used to decrypt broadcast/multicast traffic) in seconds [0-3600]. The default value is 0, meaning no rekeying.

aaa.security.wpa.<index>.rekey.gmk.period – specify the time interval for rekeying the Group Master Key (GMK is used internally to generate GTKs), in seconds. The default value is 0 and means no rekeying.

The IEEE 802.11i/RSN/WPA2 pre-authentication feature is used to speed up roaming by pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP.

aaa.security.wpa.<index>.rsn.preauth.status – specify the IEEE 802.11i/RSN/WPA2 pre-authentication status [enabled/disabled]. Default: enabled.

aaa.security.wpa.<index>.rsn.preauth.<index>.status – specify the pre-authentication interface list status [enabled/disabled]. Default: enabled.

aaa.security.wpa.<index>.rsn.preauth.<index>.status – specify the pre-authentication interface list status [enabled/disabled]. Default: enabled.

aaa.security.wpa.<index>.rsn.preauth.<index>.devname – specify the list of interfaces from which pre-authentication frames are accepted [interface name list, e.g., 'ixp0' or 'ixp0.1 xip0.2']. This list should include all interfaces that are used for connections to other APs. The normal wireless data interface towards associated stations (ath0) should not be added, since pre-authentication is only used with APs other than currently associated one.

Example:

```
aaa.security.wpa.1.status=enabled
aaa.security.wpa.1.name=WPASEC
aaa.security.wpa.1.mode=WPA
aaa.security.wpa.1.key.method=PSK
aaa.security.wpa.1.key.cipher=ALL
aaa.security.wpa.1.passphrase=the_secret_phrase
aaa.security.wpa.1.rekey.group.period=0
aaa.security.wpa.1.rekey.gmk.period=0
```

6.4.1.7 RADIUS Proxy

The ShadowMaster can forward RADIUS authentication and accounting packets between attached access points and RADIUS server reachable through the WAN interface.

The requirements for RADIUS proxy feature to work correctly are:

1. The AP should be operating in bridge mode and be connected to Access Controller's LAN port.
2. The ShadowMaster should have these RADIUS proxy parameters configured:
 - RADIUS authentication port (UDP)

- RADIUS accounting port (UDP)
 - accounting detection timeout
3. AP should have NAS configured specifically for RADIUS proxy feature (see chapter 6.4.1.1 Network Access Server (NAS)).
 4. The AP, which will use RADIUS proxy feature, should send RADIUS authentication and accounting packets to the preconfigured proxy ports on ShadowMaster LAN IP address.
 5. The ShadowMaster will forward RADIUS authentication and accounting packets according to RADIUS domain server settings in the ShadowMaster configuration without any modification (as is).
 6. The RADIUS secret on AP should be the same as real RADIUS server secret to which the packets will be forwarded.
 7. The ShadowMaster RADIUS proxy authentication port will accept only RADIUS authentication packets and the RADIUS proxy accounting port will accept only RADIUS accounting packets.
 8. The RADIUS proxy will ignore RADIUS Access-Request packets without the Calling-Station-Id containing valid MAC address.
 9. The RADIUS proxy will use retransmission policies as configured per NAS radius domains and will ignore retransmissions from AP when internal retransmission will be in progress.
 10. The RADIUS proxy can do accounting detection. This will be done by looking for Accounting-Start packets for client who previously got Access-Accept. Lookup is done by Calling-Station-Id MAC address value and Acct-Session-Id if it was available in the last Access-Request packet for that client.
 11. The RADIUS proxy will not start internal RADIUS accounting if there will be no RADIUS accounting information detected within specified accounting detection timeout period or accounting detection is turned off.
 12. The RADIUS proxy will leave Acct-Session-Id unchanged (which is generated internally by NAS), unless Acct-Session-Id attribute will be available in the last RADIUS Access-Request packet from AP.
 13. The RADIUS proxy will logout client on Acct-Stop, if no accounting information is detected for that client.

All available keys of the RADIUS Proxy feature are listed below:

aaa.radiusproxy.<index>.status – specify the RADIUS proxy status [enabled/disabled].

aaa.radiusproxy.<index>.name – specify the RADIUS proxy profile name [string]. This should be equal to *aaa.nas.<index>.auth.<index>.profile* (see chapter 6.4.1.1 Network Access Server (NAS)).

aaa.radiusproxy.<index>.auth.port – specify the UDP port for the ShadowMaster to listen on for RADIUS authentication packets. The ShadowMaster RADIUS proxy authentication port will accept only RADIUS authentication packets [0-65535]. Default: 1812.

aaa.radiusproxy.<index>.acct.port – specify the UDP port for the ShadowMaster to listen on for RADIUS accounting packets. The ShadowMaster RADIUS proxy accounting port will accept only RADIUS accounting packets [0-65535]. Default: 1813.

aaa.radiusproxy.<index>.acct.timeout – specify the RADIUS proxy accounting detection timeout in seconds [0-999999]. Default: 30. The ShadowMaster will wait the specified period of time for a RADIUS accounting start packet from the AP following a successful authentication. If no RADIUS accounting start packet is received within this time interval, the ShadowMaster will send one for the user on the AP's behalf. ShadowMaster will continue to maintain accounting data for the duration of the user's session. To disable accounting detection and internal accounting, set this value to 0.

Example:

```
aaa.nas.1.auth.1.type=radius_proxy
aaa.nas.1.auth.1.profile=rp_ixp0
aaa.radius.proxy.1.name=rp_ixp0
aaa.radius.proxy.1.auth.port=1812
aaa.radius.proxy.1.acct.port=1813
aaa.radius.proxy.1.acct.timeout=30
```


6.4.2 WPA/802.1x Supplicant

IEEE 802.1x is the standard defining port-based authentication and infrastructure for doing key management. Extensible Authentication Protocol (EAP) messages are sent over an 802.11 wireless network using an EAPOL protocol. IEEE 802.1x provides dynamically-generated keys that are periodically refreshed.

EAP/802.1x authentication and dynamic key management enables stronger data encryption. Once an EAP/802.1x association is made between the client (WPA-compliant ShadowMaster supplicant) and the authentication server, WPA key management can be negotiated.

The ShadowMaster can be configured to act as a supplicant (a client to 802.1x protocol authenticator). It supports multiple EAP based authentication types, such as: EAP-TLS, EAP-TTLS, and EAP-MD5. The client transfers all authorization and accounting information to a RADIUS server.



The RADIUS server must be installed and properly configured to accept requests from the ShadowMaster RADIUS client.

These keys are shared by all network blocks:

wpasupplicant.status – specify the WPA Supplicant status [enabled/disabled]. Default: disabled.

wpasupplicant.wait_for_interface – specify to wait for all configured interfaces to become available [enabled/disabled]. Default: disabled.

wpasupplicant.verbose – specify the logging verbosity level [0-4]. Default: 2. Verbosity levels are:

- 0 – quiet,
- 1 – somewhat quiet,
- 2 – normal,
- 3 – somewhat verbose,
- 4 – verbose.

wpasupplicant.keys – specify to include the secret keys, passwords, etc. into verbose output [enabled/disabled]. Default: disabled.

wpasupplicant.timestamp – specify to include the timestamp into verbose output [enabled/disabled]. Default: disabled.

wpasupplicant.device.<index>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.device.<index>.devname – specify the name of the ShadowMaster network interface, on which WPA/802.1x supplicant will be started.

wpasupplicant.device.<index>.driver – specify the name of network interface driver to be used [string]. Available driver names: hostap, prism54, madwifi, atmel, wext, ndiswrapper, broadcom, ipw2100, bsd, ndis. If not specified, first in the list of compiled in drivers will be used by default.

wpasupplicant.device.<index>.profile – specify the profile name to use for the ShadowMaster network interface [string]. This should be equal to *wpasupplicant.profile.<index>.name* described in next section *802.1x Supplicant Profile*.

6.4.2.1 802.1x Supplicant Profile

In addition to enterprise level security (WPA-802.1x), ShadowMaster supplicant supports the Pre-Shared Key WPA version (WPA-PSK) also, intended for use in SOHO or home wireless networks.

All available keys of the profile of the 802.1x Supplicant are listed below:

wpasupplicant.profile.<index>.status – specify current profile entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.name – specify the configuration profile name [string].

wpasupplicant.profile.<index>.eapol_version – specify the IEEE 802.1X/EAPOL version [1/2]. The supplicant implementation is based on IEEE 802-1X-REV-d8, which defines EAPOL version 2. However, there are many APs that do not handle the new version number correctly (they seem to drop the frames completely). In order to allow supplicant to interoperate with these APs, the version number is set to 1 by default. This configuration value can be used to set it to the new version (2).

wpasupplicant.profile.<index>.ap_scan – specifies the AP scanning/selection [enabled/disabled]. Default: enabled. By default supplicant requests drivers to perform AP scanning and then uses the scan results to select a suitable AP. Another alternative is to allow the drivers to take care of AP scanning and selection, and use supplicant just to process EAPOL frames based on IEEE 802.11 association information from the driver.

enabled - (default) - supplicant initiates scanning and AP selection;

disabled - driver takes care of scanning, AP selection, and IEEE 802.11 association parameters (e.g., WPA IE generation); this mode can also be used with non-WPA drivers when using IEEE 802.1X mode.

wpasupplicant.profile.<index>.fast_reauth – specify the EAP fast re-authentication [enabled/disabled]. By default fast re-authentication is enabled for all EAP methods that support it. This variable can be used to disable fast re-authentication. Normally, there is no need to disable this.

wpasupplicant.profile.<index>.blacklist_age – specify timeout in seconds for blacklist entries [integer]. Default 3600. Entries will be deleted from blacklist after this timeout.

wpasupplicant.profile.<index>.network.<index>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.ssid – specify the SSID in ASCII format [string].

wpasupplicant.profile.<index>.network.<index>.ssid.hex – specify the SSID in a hexadecimal format.



Either *wpasupplicant.profile.<index>.network.<index>.ssid* or *wpasupplicant.profile.<index>.network.<index>.ssid.hex* is mandatory. If both are specified *wpasupplicant.profile.<index>.network.<index>.ssid.hex* is used and the former is ignored.

wpasupplicant.profile.<index>.network.<index>.scan_ssid – specify to scan the SSID with specific Probe Request frames [enabled/disabled]. Default: disabled. Value:

disabled – do not scan this SSID with specific Probe Request frames.

enabled – scan with SSID-specific Probe Request frames (this can be used to find APs that do not accept broadcast SSID or use multiple SSIDs. This will slow down scanning, so enable this only when needed).

wpasupplicant.profile.<index>.network.<index>.bssid – specify the BSSID [MAC address]. If BSSID is set, this network block is used only when associating to the AP with configured BSSID.

wpasupplicant.profile.<index>.network.<index>.priority – specify the priority [0-65535]. Default: 0. By default, all networks will get the same priority group (0). If some of the networks are more desirable, this field can be used to change the order in which supplicant goes through the networks when selecting a BSS. The priority groups will be iterated in decreasing priority (i.e., the larger the priority value, the sooner the network is matched against the scan results). Within each priority group, networks will be selected based on security policy, signal strength, etc. Note that AP scanning with *wpasupplicant.profile.<index>.network.<index>.scan_ssid = 1* is not using this priority to select the order for scanning. Instead, it uses the order the networks are in the configuration file.

wpasupplicant.profile.<index>.network.<index>.proto.<1/2>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.proto.<1/2>.name – specify the accepted protocols [WPA/RSN]. If this key is not specified both WPA and RSN (WPA2) are accepted.

WPA = WPA/IEEE 802.11i/D3.0

RSN = WPA2/IEEE 802.11i (also WPA2 can be used as an alias for RSN)

wpasupplicant.profile.<index>.network.<index>.key_mgmt.<1-4>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.key_mgmt.<1-4>.name – specify accepted authenticated key management protocols [WPA-PSK/WPA-EAP/IEEE8021X/NONE]. If this key is not specified both WPA-PSK and WPA-EAP are accepted.

WPA-PSK – WPA pre-shared key (this requires *wpasupplicant.profile.<index>.network.<index>.psk* field)

WPA-EAP – WPA using EAP authentication

IEEE8021X – IEEE 802.1X using EAP authentication and (optionally) dynamically generated WEP keys

NONE – WPA is not used; plaintext or static WEP could be used

wpasupplicant.profile.<index>.network.<index>.auth_alg.<1-3>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.auth_alg.<1-3>.name – specify allowed IEEE 802.11 authentication algorithms [OPEN/SHARED/LEAP]. If not specified, automatic selection is used (Open System with LEAP enabled if LEAP is allowed as one of the EAP methods).

OPEN – Open System authentication (required for WPA/WPA2)

SHARED – Shared Key authentication (requires static WEP keys)

LEAP – LEAP/Network EAP (only used with LEAP)

wpasupplicant.profile.<index>.network.<index>.pairwise.<1-3>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.pairwise.<1-3>.name – specify accepted pair-wise (unicast) ciphers for WPA [CCMP/TKIP/NONE]. If not specified, both CCMP and TKIP are accepted.

CCMP – AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0]

TKIP – Temporal Key Integrity Protocol [IEEE 802.11i/D7.0]

NONE – Use only Group Keys (deprecated, should not be included if APs support pair-wise keys)

wpasupplicant.profile.<index>.network.<index>.group.<1-4>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.group.<1-4>.name – specify accepted group (broadcast/multicast) ciphers for WPA [CCMP/TKIP/WEP104/WEP40]. If not specified CCMP, TKIP, WEP104 and WEP40 are accepted.

CCMP – AES in Counter mode with CBC-MAC [RFC 3610, IEEE 802.11i/D7.0]

TKIP – Temporal Key Integrity Protocol [IEEE 802.11i/D7.0]

WEP104 – WEP (Wired Equivalent Privacy) with 104-bit key

WEP40 – WEP (Wired Equivalent Privacy) with 40-bit key [IEEE 802.11]

wpasupplicant.profile.<index>.network.<index>.psk – specify the WPA, 256-bit pre-shared key. This is the key used in WPA-PSK mode - an ASCII passphrase with double quotation (in which case, the real PSK will be generated using the passphrase and SSID). ASCII passphrase must be between 8 and 63 characters (inclusive). This field is not needed, if WPA-EAP is used.



Separate tool, `wpa_passphrase`, can be used to generate 256-bit keys from ASCII passphrase. This process uses lot of CPU and `wpa_supplicant` startup and reconfiguration time can be optimized by generating the PSK only when the passphrase or SSID has actually changed.

wpasupplicant.profile.<index>.network.<index>.psk.hex – specify the WPA pre-shared key in hex: 256-bit pre-shared key. 64 hex-digits, i.e., 32 bytes. If specified it will override `wpasupplicant.profile.<index>.network.<index>.psk`.

wpasupplicant.profile.<index>.network.<index>.eapol_flags – specify which dynamic WEP keys are required for non-WPA mode [0/1/2/3]. Default: 3. Values:

- 0** – require no keys
- 1** – require dynamically generated unicast WEP key
- 2** – require dynamically generated broadcast WEP key
- 3** – require both keys.

The following keys are only used with internal EAP implementation:

wpasupplicant.profile.<index>.network.<index>.eap.<1-12>.status – specify current entry status [enabled/disabled]. Default: enabled.

wpasupplicant.profile.<index>.network.<index>.eap.<1-12>.name – specify the EAP methods [MD5/MSCHAPV2/OTP/GTC/TLS/PEAP/TTLS/LEAP/PSK/AKA/FAST]. If not specified, all methods are allowed.

MD5 – EAP-MD5 (insecure and does not generate keying material - cannot be used with WPA. to be used as a Phase 2 method with EAP-PEAP or EAP-TTLS)

MSCHAPV2 – EAP-MSCHAPv2 (cannot be used separately with WPA; to be used as a Phase 2 method with EAP-PEAP or EAP-TTLS)

OTP – EAP-OTP (cannot be used separately with WPA; to be used as a Phase 2 method with EAP-PEAP or EAP-TTLS)

GTC – EAP-GTC (cannot be used separately with WPA; to be used as a Phase 2 method with EAP-PEAP or EAP-TTLS)

TLS – EAP-TLS (client and server certificate)

PEAP – EAP-PEAP (with tunnelled EAP authentication)

TTLS – EAP-TTLS (with tunnelled EAP or PAP/CHAP/MSCHAP/MSCHAPV2 authentication)

LEAP – EAP-LEAP

PSK – EAP-PSK

AKA – EAP-AKA

FAST – EAP-FAST

wpasupplicant.profile.<index>.network.<index>.identity – specify the identity for EAP [string].

wpasupplicant.profile.<index>.network.<index>.anonymous_identity – specify anonymous identity for EAP (to be used as the unencrypted identity with EAP types that support different tunnelled identity, e.g., EAP-TTLS) [string].

wpasupplicant.profile.<index>.network.<index>.password – specify the password for EAP [string].

wpasupplicant.profile.<index>.network.<index>.pin – specify the SIM pin code [string].

wpasupplicant.profile.<index>.network.<index>.pcsc – specify the PCSC string used for SIM authentication. Default: empty string if *wpasupplicant.profile.<index>.network.<index>.pin* is specified.

wpasupplicant.profile.<index>.network.<index>.wep_key0 – specify the WEP Key 0: 40-bit or 104-bit. The key used in static WEP mode - an ASCII passphrase.

wpasupplicant.profile.<index>.network.<index>.wep_key0.hex – specify the static WEP key 0: 40-bit or 104-bit static key. The key used in static WEP mode - hex-digits, i.e., 10 or 26 bytes. If this key is specified, it overrides

wpasupplicant.profile.<index>.network.<index>.wep_key0.

5 pairs for 40-bit key (e.g. 00:AC:01:35:FF)

13 pairs for 104-bit key (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC)

wpasupplicant.profile.<index>.network.<index>.wep_key1 – specify the static WEP key 1: 40-bit or 104-bit. The key used in static WEP mode - an ASCII passphrase.

wpasupplicant.profile.<index>.network.<index>.wep_key1.hex – specify the static WEP key 1 in hex-digits: 40-bit or 104-bit static key. The syntax is the same as *wpasupplicant.profile.<index>.network.<index>.wep_key0.hex*. If this key is specified, it overrides *wpasupplicant.profile.<index>.network.<index>.wep_key1*.

wpasupplicant.profile.<index>.network.<index>.wep_key2 – specify the static WEP key 1: 40-bit or 104-bit. The key used in static WEP mode - an ASCII passphrase.

wpasupplicant.profile.<index>.network.<index>.wep_key2.hex – specify the static WEP key 2 in hex-digits: 40-bit or 104-bit static key. The syntax is the same as *wpasupplicant.profile.<index>.network.<index>.wep_key0.hex*. If this key is specified, it overrides *wpasupplicant.profile.<index>.network.<index>.wep_key2*.

wpasupplicant.profile.<index>.network.<index>.wep_key3 – specify the static WEP key 1: 40-bit or 104-bit. The key used in static WEP mode - an ASCII passphrase.

`wpasupplicant.profile.<index>.network.<index>.wep_key3.hex` – specify the static WEP key 3 in hex-digits: 40-bit or 104-bit static key. The syntax is the same as *`wpasupplicant.profile.<index>.network.<index>.wep_key0.hex`*. If this key is specified, it overrides *`wpasupplicant.profile.<index>.network.<index>.wep_key3`*.

`wpasupplicant.profile.<index>.network.<index>.wep_tx_keyidx` – specify the default static WEP key [0/1/2/3]. Default: 0.

`wpasupplicant.profile.<index>.network.<index>.eappsk` – specify the EAP pre-shared key in hexadecimal format [32 hexadecimal digits].

`wpasupplicant.profile.<index>.network.<index>.nai` – specify the user Network Access Identifier (NAI) used to identify communicating parties [string up to 72 characters in length]. This is used for EAP-PSK protocol.

`wpasupplicant.profile.<index>.network.<index>.server_nai` – specify the authentication server's NAI [string up to 72 characters in length]. This is used for EAP-PSK protocol.

`wpasupplicant.profile.<index>.network.<index>.ca_cert` – specify the name of CA certificate file [file name with .pem or .der extension]. This file can have one or more trusted CA certificates. If `ca_cert` is not included, server certificate will not be verified. This is insecure and the CA file should always be configured. The file should be saved in `/etc/persistent/ca_cert/` directory on device.

`wpasupplicant.profile.<index>.network.<index>.client_cert` – specify the name of client certificate file [file name with .pem or .der extension]. The file should be saved in `/etc/persistent/public_cert/` directory on device.

`wpasupplicant.profile.<index>.network.<index>.private_key` – specify the name of client private key file [file name with .key or .p12 extension]. When PKCS#12 file (.p12 extension) is used, *`wpasupplicant.profile.<index>.network.<index>.client_cert`* should be commented out or removed. Both the private key and certificate will be read from the PKCS#12 file in this case. The file should be saved in `/etc/persistent/private_key/` directory on device.

`wpasupplicant.profile.<index>.network.<index>.private_key_passwd` – specify the password for private key [string].

`wpasupplicant.profile.<index>.network.<index>.dh_file` – specify the path to DH/DSA parameters file (in PEM format) [string]. This is an optional configuration file for setting parameters for an ephemeral DH key exchange. In most cases, the default RSA authentication does not use this configuration. However, it is possible setup RSA to use ephemeral DH key exchange. In addition, ciphers with DSA keys always use ephemeral DH keys. This can be used to achieve forward secrecy. If the file is in DSA parameters format, it will be automatically converted into DH parameters.

`wpasupplicant.profile.<index>.network.<index>.subject_match` – specify substring to be matched against the subject of the authentication server certificate. If this string is set, the server certificate is only accepted if it contains this string in the subject. The subject string is in following format: `/C=US/ST=CA/L=San Francisco/CN=Test AS/emailAddress=as@example.com`

Phase1 (outer authentication, i.e., TLS tunnel) parameters:

`wpasupplicant.profile.<index>.network.<index>.phase1.peapver` – specify the PEAP version which will be used [0/1]. Default: 1.

`wpasupplicant.profile.<index>.network.<index>.phase1.peaplabel` – specify the PEAP label status [enabled/disabled]. Default: disabled. When enabled, new label, "client PEAP encryption"

will be used during key derivation with PEAPv1 or newer. Most existing PEAPv1 implementations seem to be using the old label, "client EAP encryption", and supplicant is now using this as default value. Some servers may require `peaplabel` to be enabled to interoperate with PEAPv1.

`wpasupplicant.profile.<index>.network.<index>.phase1.peap_outer_success` – specify the method to terminate PEAP authentication on tunnelled EAP-Success [0/1/2]. Default: 0.

0 – PEAP terminated on Phase 2 inner EAP-Success;

1 – reply with tunnelled EAP-Success to inner EAP-Success and expect access server to send outer (unencrypted) EAP-Success after this;

2 – reply with PEAP/TLS ACK to inner EAP-Success and expect access server to send outer (unencrypted) EAP-Success after this.

This is required with some RADIUS servers that implement draft-josefsson-pppext-eap-tls-eap-05.txt.

`wpasupplicant.profile.<index>.network.<index>.phase1.sim_min_num_chal` – specify to configure the EAP-SIM to require 2 or 3 challenges [2/3]. Default 2.

Phase2 (inner authentication with TLS tunnel) parameters:

`wpasupplicant.profile.<index>.network.<index>.phase2.auth` – specify the inner authentication type for TTLS [MSCHAPV2/MSCHAP/PAP/CHAP]. It stands for TTLS/MSCHAPV2, TTLS/MSCHAP, TTLS/PAP and TTLS/CHAP. If not specified, the keys `wpasupplicant.profile.<index>.network.<index>.phase2.autheap.*` will be used instead, see below.

`wpasupplicant.profile.<index>.network.<index>.phase2.autheap.<1-5>.status` – specify current entry status [enabled/disabled]. Default: enabled.

`wpasupplicant.profile.<index>.network.<index>.phase2.autheap.<1-5>.name` – specify the inner tunnelled EAP authentication types for TTLS [MD5/TLS/MSCHAPV2/GTC/OTP]. They stand for TTLS/EAP-MD5, TTLS/EAP-TLS, TTLS/EAP-MSCHAPV2, TTLS/EAP-GTC, TTLS/EAP-OTP. If not specified all available types will be accepted. Note: If `wpasupplicant.profile.<index>.network.<index>.phase2.auth` is set - this key will have no effect.

`wpasupplicant.profile.<index>.network.<index>.phase2.authpeap.<1-5>.status` – specify current entry status [enabled/disabled]. Default: enabled.

`wpasupplicant.profile.<index>.network.<index>.phase2.authpeap.<1-5>.name` – specify the inner tunnelled EAP authentication types for PEAP [MD5/TLS/MSCHAPV2/GTC/OTP]. If not specified all available types will be accepted.

`wpasupplicant.profile.<index>.network.<index>.ca_cert2` – specify the name of CA certificate file [file name with .pem or .der extension]. This file can have one or more trusted CA certificates. If `ca_cert2` is not included, server certificate will not be verified. This is insecure and the CA file should always be configured. See also:
`wpasupplicant.profile.<index>.network.<index>.ca_cert`.

`wpasupplicant.profile.<index>.network.<index>.client_cert2` – specify the name of client certificate file [file name with .pem or .der extension]. See also:
`wpasupplicant.profile.<index>.network.<index>.client_cert`.

`wpasupplicant.profile.<index>.network.<index>.private_key2` – specify the name of client private key file [file name with .key or .p12 extension]. See also:
`wpasupplicant.profile.<index>.network.<index>.private_key`.

wpasupplicant.profile.<index>.network.<index>.private_key2_passwd – specify the password for private key [string].

wpasupplicant.profile.<index>.network.<index>.dh_file2 – specify the path to DH/DSA parameters file (in PEM format). See also:

wpasupplicant.profile.<index>.network.<index>.dh_file.

wpasupplicant.profile.<index>.network.<index>.subject_match2 – specify substring to be matched against the subject of the authentication server certificate. See also:

wpasupplicant.profile.<index>.network.<index>.subject_match.

Example:

```
wpasupplicant.profile.1.status=enabled
wpasupplicant.profile.1.ap_scan=enabled
wpasupplicant.profile.1.eapol_version=1
wpasupplicant.profile.1.fast_reauth=enabled
wpasupplicant.profile.1.name=user_1
wpasupplicant.profile.1.network.1.priority=0
wpasupplicant.profile.1.network.1.proto.1.status=enabled
wpasupplicant.profile.1.network.1.proto.2.status=enabled
wpasupplicant.profile.1.network.1.scan_ssid=disabled
wpasupplicant.profile.1.network.1.ssid=device_SSID
wpasupplicant.profile.1.network.1.status=enabled
wpasupplicant.profile.1.network.1.auth_alg.1.status=enabled
wpasupplicant.profile.1.network.1.auth_alg.1.name=OPEN
wpasupplicant.profile.1.network.1.auth_alg.2.status=disabled
wpasupplicant.profile.1.network.1.auth_alg.3.status=disabled
wpasupplicant.profile.1.network.1.ca_cert=/etc/persistent/public_cert/root.pem
wpasupplicant.profile.1.network.1.eap.1.status=enabled
wpasupplicant.profile.1.network.1.eap.1.name=PEAP
wpasupplicant.profile.1.network.1.eapol_flags=3
wpasupplicant.profile.1.network.1.group.1.status=enabled
wpasupplicant.profile.1.network.1.group.1.name=TKIP
wpasupplicant.profile.1.network.1.group.2.status=disabled
wpasupplicant.profile.1.network.1.group.3.status=disabled
wpasupplicant.profile.1.network.1.group.4.status=disabled
wpasupplicant.profile.1.network.1.identity=user_name
wpasupplicant.profile.1.network.1.key_mgmt.1.status=enabled
wpasupplicant.profile.1.network.1.key_mgmt.1.name=WPA-EAP
wpasupplicant.profile.1.network.1.pairwise.1.status=enabled
wpasupplicant.profile.1.network.1.pairwise.1.name=TKIP
wpasupplicant.profile.1.network.1.pairwise.2.status=disabled
wpasupplicant.profile.1.network.1.password=user_password
wpasupplicant.profile.1.network.1.phase1.peap_outer_success=0
wpasupplicant.profile.1.network.1.phase1.peaplabel=disabled
wpasupplicant.profile.1.network.1.phase1.peapver=0
wpasupplicant.profile.1.network.1.phase1.sim_min_num_chal=2
wpasupplicant.profile.1.network.1.phase2.authpeap.1.status=enabled
wpasupplicant.profile.1.network.1.phase2.authpeap.1.name=MSCHAPV2
wpasupplicant.profile.1.network.1.wep_tx_keyidx=0
```


6.4.3 IP Firewall

Access control and traffic accounting in a ShadowMaster is implemented through IP firewall rules. A firewall protects the resources of a private network from outside users by preventing unauthorized access and acting as a security filter which restricts specified types of network communication.

The firewall mechanism enables Port Forwarding features by creating a transparent tunnel through a firewall, allowing users on the Internet access to a service (Web server, SSH server) running on the LAN side. From the outside user's point of view, it looks like the service is running on the firewall.

The IP firewall contains three built-in tables: NAT, mangle and filter. Every table contains built-in chains. The user can create additional chains and include them into built-in chains for more flexibility. Here is the built-in chain list for those tables:

- **NAT** (network address translation including DNAT, SNAT and masquerading):
 - PREROUTING
 - POSTROUTING
 - OUTPUT
- **mangle** (general packet header modification such as setting the TOS value or marking packets for policy routing and traffic shaping):
 - PREROUTING
 - INPUT
 - FORWARD
 - OUTPUT
 - POSTROUTING
- **filter** (packet filtering: rejecting, dropping or accepting packets):
 - INPUT
 - FORWARD
 - OUTPUT

Packets coming from the network and destined for the ShadowMaster based device traverses the firewall tables, chains, and routing tables in this order:

- **mangle table, PREROUTING chain** – normally used for mangling packets, i.e., changing TOS and so on;
- **NAT table, PREROUTING chain** – mainly used for DNAT; avoid filtering in this chain since it will be bypassed in certain cases;
- **routing decision**;
- **mangle table, INPUT chain** – used to mangle packets, after they have been routed;
- **filter table, INPUT chain** – used to filter all incoming traffic destined for the ShadowMaster based device.

Packet generated by process on the ShadowMaster based device locally traverses firewall tables, chains, and routing tables in this order:

- **routing decision**;
- **mangle table, OUTPUT chain** – normally used for mangling packets; it is suggested that you do not filter in this chain since it can have side effects;
- **NAT table, OUTPUT chain** – can be used to NAT outgoing packets from the firewall itself;
- **filter table, OUTPUT chain** – used to filter all outgoing traffic from the ShadowMaster based device;
- **mangle table, POSTROUTING chain** – used when we want to do mangling on packets before they leave the ShadowMaster based device, but after the actual routing decisions (this chain will be hit by both packets just traversing the firewall, as well as packets created by the firewall itself);

- **NAT table, POSTROUTING chain** – used for SNAT; it is suggested that you don't do filtering here since it can have side effects, and certain packets might slip through even though the default policy is to drop them.

Packet passing through the ShadowMaster and destined for another host on the network traverses firewall tables, chains, and routing tables in this order:

- **mangle table, PREROUTING chain** – normally used for mangling packets;
- **NAT table, PREROUTING chain** – mainly used for DNAT; avoid filtering in this chain since it will be bypassed in certain cases;
- **routing decision;**
- **mangle table, FORWARD chain** – used for very specific needs, where we want to mangle the packets after the initial routing decision, but before the last routing decision made just before the packet is sent out;
- **filter table, FORWARD chain** – used for all the filtering; all forwarded traffic goes through this chain;
- **mangle table, POSTROUTING chain** – used for specific types of packet mangling that we wish to take place after all kinds of routing decisions has been done, but still on this machine;
- **NAT table, POSTROUTING chain** – used for SNAT; avoid doing filtering here, since certain packets might pass this chain without ever hitting it; this is also where masquerading is done.

All available keys of the Firewall configuration are listed below:

firewall.status – specify the IP firewall feature status [enabled/disabled]. Default: disabled.

firewall.<table-name>.<chain-name>.policy – specify the policy [ACCEPT/DROP/RETURN]. Default: ACCEPT. See below for descriptions.

Create a custom user chain:

firewall.chain.<index>.status – specify the chain entry status [enabled/disabled]. Default: enabled.

firewall.chain.<index>.name – specify the chain name [string without spaces].

firewall.chain.<index>.table – specify the chain table name [nat/mangle/filter, mandatory].

firewall.chain.<index>.parent – specify the parent chain name [string without spaces].



The key *firewall.chain.<index>.parent* is not recommended to use. Use rules with *Jump* target instead to arrange chains.

6.4.3.1 Rules Configuration

A firewall rule specifies criteria for a packet, and a target. If the packet does not match, the next rule in the chain is the examined; if it does match, then the next rule is specified by the value of the target, which can be the name of a user-defined chain, or one of the special values described below. Some rule keys may have an inverse sub-key. If set to enabled it inverts the test for the main key match value.

Following configuration keys are used to determine where a particular rule shall be placed:

firewall.rule.<index>.status – specify the rule entry status [enabled/disabled]. Default: enabled.

firewall.rule.<index>.table – specify the table name [nat/mangle/filter].

firewall.rule.<index>.chain – specify the chain name [string, no spaces allowed].

firewall.rule.<index>.index – specify the rule index within the chain [1-1000].

6.4.3.2 Rule Matches

firewall.rule.<index>.protocol – specify the rule protocol [TCP/UDP/ICMP/ALL/name from /etc/protocols, integer value]



The values of the /etc/protocols are listed in *Appendix D: /etc/protocols*.

firewall.rule.<index>.protocol.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled. If enabled, this will match all protocols not specified by *firewall.rule.<index>.protocol*.

firewall.rule.<index>.src – specify the source IP address. IP address can be single address, e.g. 192.168.2.1 or can be used with network mask to specify whole IP ranges - e.g. 192.168.2.0/24 or 192.168.2.0/255.255.255.0.

firewall.rule.<index>.src.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.dst – specify the destination IP address. IP address can be single address, e.g. 192.168.2.1 or can be used with network mask to specify whole IP ranges - e.g. 192.168.2.0/24 or 192.168.2.0/255.255.255.0.

firewall.rule.<index>.dst.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.in – specify the interface name where the packet came from. This option is legal only in the INPUT, FORWARD and PREROUTING chains and will not return any error message when used anywhere else. Character '+' can be used to match string of letters and numbers - e.g. value *ixp+* will match all Ethernet devices.

firewall.rule.<index>.in.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.out – specify the interface where the packet is going to. This option is legal only in the INPUT, FORWARD and PREROUTING chains and will not return any error message when used anywhere else. Character '+' can be used to match string of letters and numbers - e.g. value *ixp+* will match all Ethernet devices.

firewall.rule.<index>.out.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

6.4.3.3 Implicit Matches

firewall.rule.<index>.sport – specify the TCP or UDP source port or port range [0-65535[:0-65535]]. This match can either take a service name from /etc/services file or a port number. You can define a port range instead of one port - e.g. 22:80 will match all ports from 22 to 80.

firewall.rule.<index>.sport.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.dport – specify the TCP or UDP destination port or port range [0-65535[:0-65535]]. This match can either take a service name from /etc/services file or a port

number. You can define a port range instead of one port - e.g. 22:80 will match all ports from 22 to 80.

firewall.rule.<index>.dport.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.tcpflags – specify the TCP flags in a packet [SYN/ACK/FIN/RST/URG/PSH/ALL/NONE].

firewall.rule.<index>.tcpflags.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.tcptoption – specify the TCP option number [0-256].

firewall.rule.<index>.tcptoption.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

6.4.3.4 ICMP Matches

firewall.rule.<index>.icmp.type – specify the ICMP type [any/echo-reply/destination-unreachable/network-unreachable/host-unreachable/protocol-unreachable/port-unreachable/fragmentation-needed/source-route-failed/network-unknown/host-unknown/network-prohibited/host-prohibited/TOS-network-unreachable/TOS-host-unreachable/communication-prohibited/host-precedence-violation/precedence-cutoff/source-quench/redirect/network-redirect/host-redirect/TOS-network-redirect/TOS-host-redirect/echo-request/router-advertisement/router-solicitation/time-exceeded/ttl-zero-during-transit/ttl-zero-during-reassembly/parameter-problem/ip-header-bad/required-option-missing/timestamp-request/timestamp-reply/address-mask-request/address-mask-reply]. ICMP types can be specified either by their numeric values or by their names. Numerical values are specified in RFC 792.

firewall.rule.<index>.icmp.type.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

6.4.3.5 Explicit Matches

firewall.rule.<index>.limit – specify the maximum average number of matches to allow per time unit [0-65535/[second/minute/hour/day], e.g. 5/second].

firewall.rule.<index>.limit.burst – specify the maximum burst per time unit before the above limit kicks in [0-65535/[second/minute/hour/day], e.g. 10/second].

firewall.rule.<index>.mac – specify the source MAC address [colon separated 6 hexadecimal value pairs]. This is only useful for packets traversing the INPUT and FORWARD chains.

firewall.rule.<index>.mac.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.mark – specify the mark value which is used to match packets that have previously been marked [0-4294967296].

firewall.rule.<index>.multiport.sport – specify the multiple comma separated source ports [0-65535,...,0-65535, up to 15 ports]. This match can be used only with TCP or UDP protocols.

firewall.rule.<index>.multiport.dport – specify the multiple comma separated destination ports to [0-65535,...,0-65535, up to 15 ports]. This match can be used only with TCP or UDP protocols.

firewall.rule.<index>.multiport.port – specify the multiple ports [0-65535,...,0-65535, up to 15 ports]. This matches only if both the source and destination ports are equal to each other and are in the given port list. This match can be used only with TCP or UDP protocols.

firewall.rule.<index>.uid.owner – specify the packet creator's user id. This match works only within the OUTPUT chain.

firewall.rule.<index>.gid.owner – specify the packet creator's group id. This match works only within the OUTPUT chain.

firewall.rule.<index>.pid.owner – specify the packet creator's process id. This match works only within the OUTPUT chain.

firewall.rule.<index>.sid.owner – specify the packet creator's session id. This match works only within the OUTPUT chain.

firewall.rule.<index>.state – specify the packet's connection state [INVALID/ESTABLISHED/NEW/RELATED]. This works for almost all protocols, including ICMP and UDP.

firewall.rule.<index>.tos – specify the TOS (Type Of Service) field type [decimal or hexadecimal value]:

Minimize - Delay 16 (hexadecimal: 0X10);

Maximize - Throughput 8 (0X08);

Maximize - Reliability 4 (0X04);

Minimize - Cost 2 (0X02);

Normal - Service 0 (0X00);

firewall.rule.<index>.ttl – specify the time-to-live (TTL) value [0-256].

firewall.rule.<index>.unclean – specify the unclean match status [enabled/disabled]. Default: disabled. If enabled, this attempts to match packets which seem malformed or unusual.

firewall.rule. <index>.ipp2p.status – specify the status of IPP2P [enabled/disabled]. Default: disabled. IPP2P is a net filter extension to identify P2P file sharing traffic.

firewall.rule. <index>.ipp2p – specify status to grab all known p2p packets. [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.edk – specify to grab all known eDonkey/eMule/Overnet packets. [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.dc – specify to grab all known Direct Connect packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.kazaa – specify to grab all known KaZaA packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.gnu – specify to grab all known Gnutella packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.bit – specify to grab all known BitTorrent packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.apple – specify to grab all known AppleJuise packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.winmx – specify to grab all known WinMX packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.soul – specify to grab all known SoulSeek packets [enabled/disabled]. Default: disabled.

firewall.rule. <index>.ipp2p.ares – specify to grab all known Ares packets - use with DROP only [enabled/disabled]. Default: disabled.

Either input or output interface (not both) can be specified for the following accounting match rule. This match contains database of authenticated clients and traffic accounting for these clients is performed.

firewall.rule.<index>.acct.in – specify the input interface name.

firewall.rule.<index>.acct.in.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.acct.out – specify the output interface name.

firewall.rule.<index>.acct.out.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

Either input or output interface (not both) can be specified for the following authentication match rule.

firewall.rule.<index>.auth – specify the type of client packets: authenticated or not authenticated [auth/not-auth]. Default: auth. Based on this match, single rule for all authenticated/not authenticated clients can be applied - e.g. DROP all packets from unauthenticated clients.

firewall.rule.<index>.auth.in – specify the input interface name.

firewall.rule.<index>.auth.out – specify the output interface name.

firewall.rule.<index>.auth.in.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.auth.out.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

firewall.rule.<index>.list – specify white or black list to match packets against [white/black]. Based on this match, a single rule for all clients going to/from white (or black) listed sites can be applied. White/black list database is maintained in the separate application. If configuration value is white, all packets going to/from white-listed sites are matched. Usually such rule has target ACCEPT. Configuration value black is used for blacklisted sites together with DROP target.

6.4.3.6 IPP2P

The goal of the IPP2P is to identify peer-to-peer (P2P) data in IP traffic. IPP2P is a net filter extension to identify P2P file sharing traffic. Thereby IPP2P integrates itself easily into existing Linux firewalls and its functionality can be used by adding appropriate filter rules.

IPP2P uses suitable search patterns to identify P2P traffic thus allowing the reliable identification of traffic belonging to many P2P networks. Once identified one may handle P2P traffic in different ways - dropping such traffic, putting into low priority classes or shaping to a given bandwidth limit is possible. Reducing costs, freeing network resources and therefore improving network performance is often the result of using IPP2P.

All keys have default value: disabled.

firewall.rule.<index>.ipp2p.status -- enable/disable IPP2P match [enabled, disabled]

firewall.rule.<index>.ipp2p -- grab all known p2p packets. Equal to --edk --dc --kazaa --gnu. [enabled, disabled]

firewall.rule.<index>.ipp2p.edk -- all known eDonkey/eMule/Overnet packets [enabled, disabled].

firewall.rule.<index>.ipp2p.dc – all known direct connect packets [enabled, disabled].

firewall.rule.<index>.ipp2p.kazaa – all known KaZaA packets [enabled, disabled].

firewall.rule.<index>.ipp2p.gnu – all known Gnutella packets [enabled, disabled].

firewall.rule.<index>.ipp2p.bit – all known BitTorrent packets [enabled, disabled].

firewall.rule.<index>.ipp2p.apple – all known AppleJuice packets (beta: only few test by now) [enabled, disabled].

firewall.rule.<index>.ipp2p.winmx – all known WinMX packets (beta) [enabled, disabled].

firewall.rule.<index>.ipp2p.soul – all known SoulSeek (beta) [enabled, disabled].

firewall.rule.<index>.ipp2p.ares – all known Ares - use with DROP only (beta) [enabled, disabled].

6.4.3.7 Rule Targets

To jump to a specific chain, set the rule target to be equal to that chain's name. The chain should already exist.

firewall.rule.<index>.target – specify the rule target
[DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/T
TL/ULOG].

6.4.3.7.1 ACCEPT

As soon as the packet is matched, the rule is accepted and will not continue traversing current chain or any other ones in the same table. This target has no additional options:

firewall.rule.<index>.target=ACCEPT

6.4.3.7.2 DNAT Target

DNAT target is used to rewrite destination IP address of a packet. If a packet is matched, the packet and all subsequent packets in the same stream will be translated and then routed to the correct device, host or network. DNAT target is only available in PREROUTING and OUTPUT chains in the NAT table.

firewall.rule.<index>.target=DNAT

firewall.rule.<index>.t.dnat.dst – specify the IP or IP range. The IP range format is IP-IP (e.g. 194.236.50.155-194.236.50.160).

Example:

```
firewall.rule.1.target=DNAT
firewall.rule.1.t.dnat.dst=192.168.2.21-192.168.2.25
```

Multiple destination hosts can also be defined using the following syntax:

firewall.rule.<index>.t.dnat.<index>.dst – specify the IP address.

Example:

```
firewall.rule.1.target=DNAT
firewall.rule.1.t.dnat.1.dst=192.168.2.21
firewall.rule.1.t.dnat.2.dst=192.168.2.40
firewall.rule.1.t.dnat.3.dst=192.168.2.229
```

6.4.3.7.3 DROP

This target drops matched packets and will not carry out any further processing. If packet is dropped in a sub-chain, it will not be processed in any of the main chains in current or any other table. DROP target does not have any options.

firewall.rule.1.target=DROP

6.4.3.7.4 LOG

This target is used for logging detailed information about packets to a system's syslog. See section 6.6.4 *Syslog* for more details.

firewall.rule.<index>.target=LOG

firewall.rule.<index>.t.log.level – specify the logging level [emerg/alert/crit/err/warning/notice/info/debug].

firewall.rule.<index>.t.log.prefix – specify the log prefix [string without spaces].

firewall.rule.<index>.t.log.tcp.sequence – specify the log sequence logging status [enabled/disabled]. The sequence option will log the TCP sequence numbers in a log message.

firewall.rule.<index>.t.log.tcp.options – specify the TCP option logging status [enabled/disabled]. This logs the different options from the TCP packet headers and can be valuable when trying to debug what could go wrong, or what has actually gone wrong.

firewall.rule.<index>.t.log.ip.options – specify the IP option logging status [enabled/disabled]. The IP options will log most of the IP packet header options.

6.4.3.7.5 MARK

This target is used to set net filter mark values that are associated with specific packets. It is only valid in the mangle table.

firewall.rule.<index>.target=MARK

firewall.rule.<index>.t.mark – specify the net filter mark [0-4294967296].

6.4.3.7.6 MASQUERADE

This target modifies packet's source IP address. It is only valid in the nat table, in the POSTROUTING chain. It should only be used with dynamically assigned IP connections.

firewall.rule.<index>.target=MASQUERADE

firewall.rule.<index>.t.masq.ports – specify the port or port range [0-65535[:0-65535]]. Ports option is used to specify source port or port range to use for outgoing packets. This match can be used only with TCP or UDP protocols.

6.4.3.7.7 QUEUE

This target is used to queue packets for further processing in the userspace programs. No additional options.

firewall.rule.<index>.target=QUEUE

6.4.3.7.8 REDIRECT

REDIRECT target is used to redirect packets and streams to the machine itself. This target is valid only in PREROUTING and OUTPUT chains of the nat table. It is also valid within user-defined chains that are only called from those chains and nowhere else.

firewall.rule.<index>.target=REDIRECT

firewall.rule.<index>.t.redirect.port – specify the port or port range [0-65535[:0-65535]]. This match can be used only with TCP or UDP protocols.

6.4.3.7.9 REJECT

This target works basically the same as DROP target, but it also sends back an error message to the host sending the packet that was blocked. REJECT target is valid only in INPUT, FORWARD and OUTPUT chains.

firewall.rule.<index>.target=REJECT

firewall.rule.<index>.t.reject.with – specify the response to send to the host if sent packet was rejected [icmp-net-unreachable/icmp-host-unreachable/icmp-port-unreachable/icmp-protocol-unreachable/icmp-net-prohibited/icmp-host-prohibited/tcp-reset]. Default: port-unreachable.

6.4.3.7.10 RETURN

This target will cause current packet to stop traversing this chain and resume at the next rule in the previous (calling) chain. If the chain is the main chain, default chain policy will apply for this packet.

firewall.rule.<index>.target=RETURN

6.4.3.7.11 SNAT

This target is used to rewrite source IP address in the IP header of the packet. SNAT target is valid in POSTROUTING chain of nat table only.

firewall.rule.<index>.target=SNAT

firewall.rule.<index>.t.snat.source – specify the IP or IP range. The IP range format is IP-IP (e.g. 194.236.50.155-194.236.50.160). Source option is used to specify which source the packet should use.

6.4.3.7.12 TOS

TOS target is used to set the type of service field within IP header. It is only valid in the mangle table.

firewall.rule.<index>.target=TOS

firewall.rule.<index>.t.tos – specify the TOS field type [decimal or hexadecimal value]:

Minimize - Delay 16 (hexadecimal: 0X10);

Maximize - Throughput 8 (0X08);

Maximize - Reliability 4 (0X04);

Minimize - Cost 2 (0X02);

Normal - Service 0 (0X00);

6.4.3.7.13 TTL

TTL target is used to modify the time to live in the IP header. It is only valid in the mangle table.

firewall.rule.<index>.target=TTL

firewall.rule.<index>.t.ttl.set – specify the TTL set option [0-256]. This option tells the TTL target which TTL value to set on a packet.

firewall.rule.<index>.t.ttl.dec – specify the TTL decrement option [0-256]. This option specifies to decrement TTL by given value.

firewall.rule.<index>.t.ttl.inc – specify the TTL increment option [0-256]. This option specifies to increment TTL by given value.

6.4.3.7.14 ULOG

The ULOG target is used to provide userspace logging of matching packets. The packet information is multicasted together with the whole packet through netlink socket.

firewall.rule.<index>.target – ULOG

firewall.rule.<index>.t.ulog.nlggroup – specify the netlink group [0-32]. This option tells the ULOG target which netlink group to send the packet to.

firewall.rule.<index>.t.ulog.prefix – specify the ULOG prefix [string without spaces]. This option prefixes all log entries with a user-specified log prefix.

firewall.rule.<index>.t.ulog.cprange – specify how many bytes of packet to send [0-65535].

firewall.rule.<index>.t.ulog.qthreshold – specify how many packets to queue before sending [0-65535].

6.4.3.7.15 NAS_MARK

The NAS_MARK target is used to mark all incoming packets with their source IP address. These marks are used by traffic shaping module (used for AAA user bandwidth configuration). NAS_MARK target can be used only in PREROUTING chain (or sub-chains) of mangle table. This target has no additional parameters.

firewall.rule.<index>.target=NAS_MARK

6.4.3.7.16 Another Firewall Rule Definition Method

There is a possibility to define firewall rule with all the parameters as a regular iptables command line.

firewall.rule.<index>.cmd – specify the iptables command line [string]

Example:

```
firewall.rule.5.cmd=-t nat -A POSTROUTING -s 192.168.1.0/24 -o ixp0 -j SNAT --to-source 192.168.2.1
```

The configuration file snapshot for an example described above should be like this:

```
firewall.status=enabled
firewall.rule.1.status=enabled
firewall.rule.1.target=SNAT
firewall.rule.1.table=nat
firewall.rule.1.chain=POSTROUTING
firewall.rule.1.t.snat.source=192.168.30.1
```



```
firewall.rule.1.out=ixp1
firewall.rule.1.protocol=TCP
firewall.rule.1.dport=25

firewall.rule.2.status=enabled
firewall.rule.2.table=nat
firewall.rule.2.chain=PREROUTING
firewall.rule.2.in=ixp0
firewall.rule.2.dst=195.14.162.78
firewall.rule.2.protocol=TCP
firewall.rule.2.dport=25
firewall.rule.2.target=ACCEPT

firewall.rule.3.status=enabled
firewall.rule.3.table=nat
firewall.rule.3.chain=PREROUTING
firewall.rule.3.protocol=TCP
firewall.rule.3.in=ixp0
firewall.rule.3.dport=25
firewall.rule.3.target=DNAT
firewall.rule.3.t.dnat.dst=195.14.162.78

firewall.rule.4.status=enabled
firewall.rule.4.table=nat
firewall.rule.4.chain=POSTROUTING
firewall.rule.4.target=MASQUERADE
firewall.rule.4.out=ixp1

firewall.rule.5.table=nat
firewall.rule.5.chain=PREROUTING
firewall.rule.5.protocol=TCP
firewall.rule.5.dport=53
firewall.rule.5.target=REDIRECT

firewall.rule.6.table=nat
firewall.rule.6.chain=PREROUTING
firewall.rule.6.protocol=UDP
firewall.rule.6.dport=53
firewall.rule.6.target=REDIRECT

firewall.rule.7.table=nat
firewall.rule.7.chain=PREROUTING
firewall.rule.7.list=white
firewall.rule.7.target=ACCEPT

firewall.rule.8.table=filter
firewall.rule.8.chain=FORWARD
firewall.rule.8.list=white
firewall.rule.8.target=ACCEPT

firewall.filter.FORWARD.policy=DROP
```

6.4.4 Bridging Firewall

A bridging firewall contains three built-in tables: Filter, NAT and broute. Every table contains built-in chains. Users can create additional chains and include them into built-in chains for more flexibility. Here is the built-in chain list for those tables:

filter:

- INPUT
- FORWARD
- OUTPUT

nat:

- PREROUTING
- OUTPUT
- POSTROUTING

broute:

- BROUTING

For details about **nat** and **filter** tables and their chains check *Section 6.4.3 IP Firewall*.

The broute table is used to make a router. The targets DROP and ACCEPT have special meaning in the broute table. DROP actually means the frame has to be routed, while ACCEPT means the frame has to be bridged. The BROUTING chain is traversed very early. It is only traversed by frames entering on a bridge enslaved network interface that is in forwarding state. Normally those frames would be bridged, but you can decide otherwise here. The redirect target, described below, is very handy here.

All available keys of the Bridging Firewall feature are listed below:

ebtables.status – specify the bridging firewall feature status [enabled/disabled]. Default: disabled.

ebtables.<table-name>.<chain-name>.policy – specify the policy [ACCEPT/DROP/RETURN]. Default: ACCEPT. See below for descriptions.

ebtables.chain.<index>.status – specify the chain entry status [enabled/disabled]. Default: enabled.

ebtables.chain.<index>.name – specify the chain name [string].

ebtables.chain.<index>.table – specify the chain table name [filter/nat/broute].

6.4.4.1.1 Rules Configuration

A firewall rule specifies criteria for a packet, and a target. If the packet does not match, the next rule in the chain is the examined; if it does match, then the next rule is specified by the value of the target, which can be the name of a user-defined chain, or one of the special values described below. Some rule keys may have an inverse sub-key. If set to enabled, it inverts the test for the main key match value.

The following configuration keys are used to determine where a particular rule shall be placed:

ebtables.rule.<index>.status – specify current rule status [enabled/disabled]. Default: enabled.

ebtables.rule.<index>.table – specify the table name [string].

ebtables.rule.<index>.chain – specify the chain name [string].

A firewall rule specifies criteria for an Ethernet frame and a frame processing specification called a target. When a frame matches a rule, then the next action specified by the target is performed. The target can be one of these values: ACCEPT, DROP, CONTINUE, RETURN, an 'extension' (see below) or a user-defined chain.

ebtables.rule.<index>.target – specify the target [ACCEPT/DROP/CONTINUE/RETURN, target extension]:

ACCEPT means to let the frame through.

DROP means the frame has to be dropped.

CONTINUE means the next rule has to be checked. This can be handy to know how many frames pass a certain point in the chain or to log those frames.

RETURN means stop traversing this chain and resume at the next rule in the previous (calling) chain.

TARGET EXTENSIONS: see section 6.4.4.1.5 *Target Extensions*
arpreply

6.4.4.1.2 Rule Matches

ebtables.rule.<index>.protocol – specify the protocol that is responsible for creating the frame [hexadecimal number below 0x0600/name from /etc/ethertypes file/LENGTH]. The protocol field of the Ethernet frame can be used to denote the length of the header (802.2/802.3 networks). When the value of that field is below (or equals) 0x0600, the value equals the size of the header and should not be used as a protocol number. Instead, all frames where the protocol field is used as the length field are assumed to be of the same protocol. The protocol name for these frames is LENGTH.

Contents of /etc/ethertypes file are listed at

<http://www.cavebear.com/archive/CaveBear/Ethernet/type.html>.

ebtables.rule.<index>.protocol.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.src – specify the source MAC address [colon separated 6 hexadecimal value pairs]. Alternatively one can specify Unicast, Multicast, Broadcast or BGA (Bridge Group Address).

Unicast = 00:00:00:00:00:00/01:00:00:00:00:00, Multicast =

01:00:00:00:00:00/01:00:00:00:00:00, Broadcast = ff:ff:ff:ff:ff:ff/ff:ff:ff:ff:ff:ff or BGA =

01:80:c2:00:00:00/ff:ff:ff:ff:ff:ff. Note that a broadcast address will also match the multicast specification.

ebtables.rule.<index>.src.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.dst – specify the destination MAC address [colon separated 6 hexadecimal value pairs]. See *ebtables.rule.<index>.src* for more details.

ebtables.rule.<index>.dst.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.in – specify the interface name a frame is received from. This match is available in INPUT, FORWARD, PREROUTING and BROUTING chains.

ebtables.rule.<index>.in.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.out – specify the interface name a frame is going to be sent to. This match is available in OUTPUT, FORWARD and POSTROUTING chains.

ebtables.rule.<index>.out.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.lin – specify the (logical) bridge interface name a frame is received from. This match is available in INPUT, FORWARD, PREROUTING and BROUTING chains.

ebtables.rule.<index>.lin.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.lout – specify the (logical) bridge interface name a frame is going to be sent to. This match is available in OUTPUT, FORWARD and POSTROUTING chains.

ebtables.rule.<index>.lout.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

6.4.4.1.3 Match Extensions

802.3

Specify 802.3 DSAP/SSAP fields or SNAP type. The protocol must be specified as LENGTH (see protocol above).

ebtables.rule.<index>.802_3.sap – specify the SAP byte [hexadecimal number]. DSAP and SSAP are two one byte 802.3 fields. The bytes are always equal, so only one byte (hexadecimal) is needed as an argument.

ebtables.rule.<index>.802_3.sap.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.802_3.type – specify the SNAP value [hexadecimal number]. If the 802.3 DSAP and SSAP values are 0xaa then the SNAP type field must be consulted to determine the payload protocol. This is a two byte (hexadecimal) argument. Only 802.3 frames with DSAP/SSAP 0xaa are checked for type.

ebtables.rule.<index>.802_3.type.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ARP

Specify ARP fields. The protocol must be specified as ARP or RARP.

ebtables.rule.<index>.arp.opcode – specify the (R)ARP opcode [decimal or a string]:

- 1 = Request
- 2 = Reply
- 3 = Request_Reverse
- 4 = Reply_Reverse
- 5 = DRARP_Request
- 6 = DRARP_Reply
- 7 = DRARP_Error
- 8 = InARP_Request
- 9 = ARP_NAK

ebtables.rule.<index>.arp.opcode.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.arp.htype – specify the hardware type [number or string]. Default: Ethernet (1).

ebtables.rule.<index>.arp.htype.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.arp.ptype – specify the protocol type for which the (R)ARP is used [hexadecimal number or string]. Default: IPv4 (0x0800).

ebtables.rule.<index>.arp.ptype.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.arp.ip_src – specify the ARP IP source address specification [IP address[/netmask length in bits]].

ebtables.rule.<index>.arp.ip_src.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.arp.ip_dst – the ARP IP destination address specification [IP address[/netmask length in bits]].

ebtables.rule.<index>.arp.ip_dst.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.arp.mac_src – specify the ARP MAC source address specification [colon separated 6 hexadecimal value pairs[/netmask length in bits]].

ebtables.rule.<index>.arp.mac_src.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.arp.mac_dst – specify the ARP MAC destination address specification [colon separated 6 hexadecimal value pairs[/netmask length in bits]].

ebtables.rule.<index>.arp.mac_dst.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

IP

Specify the IP fields for IPv4 protocol.

ebtables.rule.<index>.ip.source – specify the source IP address [IP address[/netmask length in bits]].

ebtables.rule.<index>.ip.source.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.ip.destination – specify the destination IP address [IP address[/netmask length in bits]].

ebtables.rule.<index>.ip.destination.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.ip.tos – specify the IP type of service [hexadecimal number].

- Minimize - Delay (0X10);
- Maximize - Throughput (0X08);
- Maximize - Reliability (0X04);
- Minimize - Cost (0X02);
- Normal - Service (0X00);

ebtables.rule.<index>.ip.tos.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.ip.protocol – specify the IP protocol [0-255]. The standard IP protocol as specified in Appendix [D\) /etc/protocols](#).

ebtables.rule.<index>.ip.protocol.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.ip.source_port – specify the source port or port range for IP protocol [0-65535[:0-65535]].

ebtables.rule.<index>.ip.source_port.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.ip.destination_port – specify the destination port or port range for IP protocols [0-65535[:0-65535]].

ebtables.rule.<index>.ip.destination_port.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

MARK

ebtables.rule.<index>.mark – specify the mark value to check in frames [number[/mask]].

If a mark value and mask is specified, the logical AND of the mark value of the frame and the user-specified mask is taken before comparing it with the user-specified mark value. If only a mask is specified (start with '/') the logical AND of the mark value of the frame and the user-specified mark is taken and the result is compared with zero.

ebtables.rule.<index>.mark.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

Packet Type

ebtables.rule.<index>.pkttype – specify the packet type [broadcast/multicast/host/otherhost]. Matches on the Ethernet "class" of the frame, which is determined by the generic networking code. Possible values: broadcast (MAC destination is broadcast address), multicast (MAC destination is multicast address), host (MAC destination is the receiving network device) or otherhost (none of the above).

ebtables.rule.<index>.pkttype.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

STP

Specify STP BPDU (Bridge Protocol Data Unit) fields. The destination address must be specified as the bridge group address (BGA).

ebtables.rule.<index>.stp.type – specify the BPDU type [0-255].

ebtables.rule.<index>.stp.type.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.flags – specify the BPDU flag [0-255].

ebtables.rule.<index>.stp.flags.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.root_prio – specify the root priority range [0-65535[:0-65535]].

ebtables.rule.<index>.stp.root_prio.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.root_addr – specify the root MAC address [colon separated 6 hexadecimal value pairs[/netmask length in bits]]. See *ebtables.rule.<index>.src* for more details.

ebtables.rule.<index>.stp.root_addr.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.root_cost – specify the root path cost range [0-4294967295[:0-4294967295]].

ebtables.rule.<index>.stp.root_cost.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.sender_prio – specify the BPDU sender priority range [0-65535[:0-65535]].

ebtables.rule.<index>.stp.sender_prio.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.sender_addr – specify the BPDU sender MAC address [colon separated 6 hexadecimal value pairs[/netmask length in bits]]. See *ebtables.rule.<index>.src* for more details.

ebtables.rule.<index>.stp.sender_addr.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.port – specify the port identifier range [0-65535[:0-65535]].

ebtables.rule.<index>.stp.port.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.msg_age – specify the message age timer [0-65535[:0-65535]].

ebtables.rule.<index>.stp.msg_age.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.max_age – specify the max age timer [0-65535[:0-65535]].

ebtables.rule.<index>.stp.max_age.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.hello_time – specify the hello time timer [0-65535[:0-65535]].

ebtables.rule.<index>.stp.hello_time.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.stp.forward_delay – specify the forward delay timer [0-65535[:0-65535]].

ebtables.rule.<index>.stp.forward_delay.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

VLAN

Specify 802.1Q Tag Control Information fields. The protocol must be specified as 802_1Q (0x8100).

ebtables.rule.<index>.vlan.id – specify the VLAN identifier [0-4095].

ebtables.rule.<index>.vlan.id.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.vlan.prio – specify the VLAN user_priority field value [0-7]. The *ebtables.rule.<index>.vlan.id* should be set to 0 or be unspecified.

ebtables.rule.<index>.vlan.prio.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.vlan.encap – specify the encapsulated Ethernet frame type/length [0x0000-0xFFFF/symbolic name from /etc/ethertypes]. Contents of /etc/ethertypes file are listed at <http://www.cavebear.com/CaveBear/Ethernet/type.html>.

ebtables.rule.<index>.vlan.encap.inverse – specify the match value inverse status [enabled/disabled]. Default: disabled.

6.4.4.1.4 Watcher Extensions

Watchers are things that only look at frames passing by. These watchers only look the frame if the frame matches the rule.

LOG

The fact that the log module is a watcher lets us log stuff while giving a target by choice. Note that the log module therefore is not a target. Frames will be logged via system's syslog. See section 6.6.4 *Syslog* for more details.

ebtables.rule.<index>.log – specify the logging status [enabled/disabled].

ebtables.rule.<index>.log.level – specify the logging level [emerg/alert/crit/err/warning/notice/info/debug]. Default: info.

ebtables.rule.<index>.log.prefix – specify the prefix that will be printed before the logging information [string].

ebtables.rule.<index>.log.ip – specify to log the IP information when a frame made by the IP protocol matches the rule [enabled/disabled]. Default: disabled.

ebtables.rule.<index>.log.arp – specify to log the (R)ARP information when a frame made by the (R)ARP protocols matches the rule [enabled/disabled]. Default: disabled.

6.4.4.1.5 Target Extensions

arpreply

The arpreply target can be used in the PREROUTING chain of the nat table. If this target sees an ARP request it will automatically reply with an ARP reply. The used MAC address for the reply can be specified. When the ARP message is not an ARP request, it is ignored by this target.

ebtables.rule.<index>.t.arpreply.mac – specify the MAC address to reply with [colon separated 6 hexadecimal value pairs]. The Ethernet source MAC and the ARP payload source MAC will be filled in with this address.

ebtables.rule.<index>.t.arpreply.target – specify the standard target [DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/TL/ULOG].

dnat

The dnat target can only be used in the BROUTING chain of the broute table and the PREROUTING and OUTPUT chains of the nat table. It specifies that the destination MAC address has to be changed.

ebtables.rule.<index>.t.to_destination – specify the destination MAC address [colon separated 6 hexadecimal value pairs].

ebtables.rule.<index>.t.dnat_target – specify the standard target [DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/TL/ULOG].

After doing the dnat, the rule still has to give a standard target so ebtables knows what to do. The default target is ACCEPT. Making it CONTINUE could let you use multiple target extensions on the same frame. Making it DROP only makes sense in the BROUTING chain but using the redirect target is more logical there. RETURN is also allowed. Note that using RETURN in a base chain is not allowed.

mark

The mark target can be used in every chain of every table.

ebtables.rule.<index>.t.set_mark – specify the mark [number].

ebtables.rule.<index>.t.mark_target – specify the standard target [DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/TL/ULOG].

After marking the frame, the rule still has to give a standard target so ebtables knows what to do. The default target is ACCEPT. Making it CONTINUE can let you do other things with the frame in other rules of the chain.

redirect

The redirect target will change the MAC target address to that of the bridge device the frame arrived on. This target can only be used in the BROUTING chain of the broute table and the PREROUTING chain of the nat table.

ebtables.rule.<index>.t.redirect_target – specify the standard target [DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/TL/ULOG].

After doing the MAC redirect, the rule still has to give a standard target so ebtables knows what to do. The default target is ACCEPT. Making it CONTINUE could let you use multiple target extensions on the same frame. Making it DROP in the BROUTING chain will let the frames be routed. RETURN is also allowed. Note that using RETURN in a base chain is not allowed.

snat

The snat target can only be used in the POSTROUTING chain of the nat table. It specifies that the source mac address has to be changed.

ebtables.rule.<index>.t.to_source – specify the source MAC address [colon separated 6 hexadecimal value pairs].

ebtables.rule.<index>.t.snat_target – specify the standard target [DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/TL/ULOG].

After doing the snat, the rule still has to give a standard target so ebtables knows what to do. The default target is ACCEPT. Making it CONTINUE could let you use multiple target extensions on the same frame. Making it DROP does not make sense, but you could do that too. RETURN is also allowed. Note that using RETURN in a base chain is not allowed.

arpnat

The arpnat target can only be used in the POSTROUTING and PREROUTING chain of the nat table. It is used instead of absolute Wireless Station Bridge application. It must be used for both POSTROUTING and PREROUTING chain to make Wireless Station Bridge working properly.

arpnat may be configured using such options:

ebtables.arpnat.expiration – specify the expiration time in seconds [number] Default: 25200 s.

ebtables.arpnat.debug – [enabled/disabled] Default: disabled.

ebtables.arpnat.bootpnat – [enabled/disabled/relay] Default: enabled.

ebtables.arpnat.pppoenat – [enabled/disabled] Default: enabled.

ebtables.rule.<index>.t.arpnat_target – specify the standard target [DNAT/ACCEPT/DROP/LOG/MARK/MASQUARADE/QUEUE/REDIRECT/REJECT/RETURN/SNAT/TOS/TL/ULOG]. Default: ACCEPT

macvlan

The arpnat target can be used to add or remove 802.1Q VLAN tag. Example how to remove and add VLAN tag:

```
# ebtables -t nat -I PREROUTING -i ixp0 -j macvlan --untag 3
ebtables.rule.1.table=nat
ebtables.rule.1.chain=PREROUTING
ebtables.rule.1.in=ixp0 ebtables.rule.1.target=macvlan --untag 3
ebtables.rule.1.t.arpnat_target=ACCEPT
```

```
# ebtables -t nat -I POSTROUTING -o ixp1 -j macvlan --tag 3
ebtables.rule.2.table=nat
ebtables.rule.2.chain=POSTROUTING
ebtables.rule.2.out=ixp1
ebtables.rule.2.target=macvlan --tag 3
```

Example:

```
#The configuration file snapshot for an example described above:
ebtables.status=enabled
ebtables.rule.1.table=nat
```

```
ebtables.rule.1.chain=PREROUTING
ebtables.rule.1.in=ms1
ebtables.rule.1.target=redirect
ebtables.rule.1.dst=FF:FF:FF:FF:FF:FF
ebtables.rule.1.dst.inverse=enabled
ebtables.rule.2.table=nat
ebtables.rule.2.chain=POSTROUTING
ebtables.rule.2.out=ms1
ebtables.rule.2.target=snat
ebtables.rule.2.t.to_source= 00:90:4B:C8:36:37
ebtables.rule.2.t.snat_target=ACCEPT
ebtables.rule.3.table=broute
ebtables.rule.3.chain=BROUTING
ebtables.rule.3.in=ixp0
ebtables.rule.3.protocol=ARP
ebtables.rule.3.arp.mac_dst=00:90:4B:69:4A:95
ebtables.rule.3.arp.mac_dst.inverse=enabled
ebtables.rule.3.target=DROP
```

6.4.5 SMTP Redirection

SMTP redirection is useful under authenticating wireless router setups. It allows customers to connect to access points and send out emails without the need to reconfigure their email client software. If AAA is enabled, only authenticated customers should be allowed to use SMTP redirection. SMTP redirection service intercepts SMTP connections on port 25 and redirects to a preconfigured SMTP server. It can be implemented by configuring the IP firewall. See example below.

Example:

```
# redirect e-mail for clients on ixp0 interface
# 192.168.30.1 - WAN gateway
# 195.14.162.78 - SMTP server
firewall.status=enabled
firewall.rule.1.status=enabled
firewall.rule.1.target=SNAT
firewall.rule.1.table=nat
firewall.rule.1.chain=POSTROUTING
firewall.rule.1.t.snat.source=192.168.30.1
firewall.rule.1.out=ixp1
firewall.rule.1.protocol=TCP
firewall.rule.1.dport=25
```

```
firewall.rule.2.status=enabled
firewall.rule.2.table=nat
firewall.rule.2.chain=PREROUTING
firewall.rule.2.in=ixp0
firewall.rule.2.dst=195.14.162.78
firewall.rule.2.protocol=TCP
firewall.rule.2.dport=25
firewall.rule.2.target=ACCEPT
```

```
firewall.rule.3.status=enabled
firewall.rule.3.table=nat
firewall.rule.3.chain=PREROUTING
```

```
firewall.rule.3.protocol=TCP
firewall.rule.3.in=ixp0
firewall.rule.3.dport=25
firewall.rule.3.target=DNAT
firewall.rule.3.t.dnat.dst=195.14.162.78
```

6.4.6 White/Black List

The white and black access lists control user access to Web content through the Access Controller. The unauthenticated users will be allowed to access sites from white list while access to the sites from black list will be denied even for authenticated users.

There is a possibility to specify static and remote white/black list entries in the system configuration. The remote list will be retrieved from the specified remote locations. The static and remote entries will be refreshed automatically at the predefined time interval. The remote white/black is a simple text file, where each non-empty line is assumed to have one host. If the list has changed since the last update, all previously entered hosts will be overwritten by the new white/black list.

All available keys of the White/Black List are listed below:

access.<index>.status – specify the white/black list feature status [enabled/disabled]. Default: enabled.

access.verbose – specify the status whether the service daemon should be verbose or not [enabled/disabled]. Default: disabled.

access.<index>.devname – specify the interface name for which black/white policies should be applied. Instead of interface name, character '*' can be specified and it stands for all interfaces.

access.<index>.update.period – specify the list update period in seconds [0-99999999]. To disable the periodical update, use 0. The accuracy of this setting is 30 seconds. Default: 3600.

access.<index>.resolv.period – specify the DNS resolving period for black/white list entries [0-99999999]. To disable periodical resolving, use 0. The accuracy of this setting is 30 seconds. Default: 300.



The DNS resolving period should be less than update period, otherwise it will be ignored and the resolving of DNS entries will be performed on the next update.

access.<index>.whitelist.<index>.status – specify the white list status [enabled/disabled]. Default: enabled.

access.<index>.whitelist.<index>.url – specify the URL [string]. When specified, system will extract the host, port and protocol from the URL. If specified, the only key *access.<index>.whitelist.<index>.descr* is necessary, all other keys will be ignored.

access.<index>.whitelist.<index>.descr – specify the current entry description string [string]. In the case when the URL is specified it can be used as a link text for that URL.

access.<index>.whitelist.<index>.host – specify the host name or host/network IP address [IP address or hostname string].

access.<index>.whitelist.<index>.netmask – specify the netmask, used to cover network range limited by host and netmask. Default: 255.255.255.255.

access.<index>.whitelist.<index>.port.from – specify the TCP or UDP port number [0-65535]. This denotes the first port in a range or the single port when *access.<index>.whitelist.<index>.port.to* is not specified.

access.<index>.whitelist.<index>.port.to – specify the TCP or UDP port number [0-65535]. This denotes the last port in a range.

access.<index>.whitelist.<index>.proto – specify the IP protocol number [0-255] or protocol keyword. See Appendix D: /etc/protocols for details. The value 0 is used to match any protocol. Default: 0

access.<index>.whitelist.location.<index>.status – specify the status of the white list location [enabled/disabled]. Default: enabled.

access.<index>.whitelist.location.<index>.url – specify the FTP or HTTP URL, which will be used as an additional source for white list entries [string].

access.<index>.blacklist.<index>.status – specify the black list status [enabled/disabled]. Default: enabled.

access.<index>.blacklist.<index>.url – specify the URL [string]. When specified, system will extract the host, port and protocol from the URL. If specified, the only key *access.<index>.blacklist.<index>.descr* is necessary, all other keys will be ignored.

access.<index>.blacklist.<index>.descr – specify the current entry description string [string]. In case when URL is specified it can be used as a link text for that URL.

access.<index>.blacklist.<index>.host – specify the host name or host/network IP address [IP address or hostname string].

access.<index>.blacklist.<index>.netmask – specify the netmask, used to cover network range limited by host and netmask. Default: 255.255.255.255.

access.<index>.blacklist.<index>.port.from – specify the TCP or UDP port number [0-65535]. This denotes the first port in a range or the single port when *access.<index>.blacklist.<index>.port.to* is not specified.

access.<index>.blacklist.<index>.port.to – specify the TCP or UDP port number [0-65535]. This denotes the last port in a range.

access.<index>.blacklist.<index>.proto – specify the IP protocol number [0-255] or protocol keyword. See appendix D /etc/protocols for details. The value 0 is used to match any protocol. Default: 0

access.<index>.blacklist.location.<index>.status – specify the status of the black list location entry [enabled/disabled]. Default: enabled.

access.<index>.blacklist.location.<index>.url – specify the FTP or HTTP URL, which will be used as an additional source for black list entries [URL string].

Example:

```
#The 'white' entry, demonstrates specifying ip and port range.
#Range 123.123.123.0/24 with port range [1024-65535]
access.1.whitelist.1.descr=Address Range 123.123.123.0/24, port range [1024-65535]
access.1.whitelist.1.host=123.123.123.0
access.1.whitelist.1.netmask=255.255.255.0
access.1.whitelist.1.proto=TCP
access.1.whitelist.1.port.from=1024
access.1.whitelist.1.port.to=65535
```

6.4.7 Static Bandwidth Control

The **Static Bandwidth Control** is used for customers that do not use RADIUS servers to authenticate users, but want to be able to control bandwidth statically:

- upload/download bandwidth per user (IP address) based on bandwidth configuration file
- in AP client operation, ability to set max up/down speed limits overall
- in AP client operation, ability to limit packet per second, upload bandwidth, and max sessions (connection limits)

bandwidth.status – specify status of the static bandwidth control [enabled/disabled]. Default: disabled.

bandwidth.manual – enable manual editing of the configuration file /etc/persistent/bandwidth/bandwidth.cfg [enabled/disabled]. Default: disabled. This means that if there is need to add new limitation (or modify existing limitations) per IP, there is no need to reload ShadowMaster device. It is possible to modify configuration file etc/persistent/bandwidth/bandwidth.cfg manually and reload script from the shell with command: /sbin/bandwidth.sh start

Manual configuration file editing means that sysconf do not overwrites configuration file on device reload. Script reads data from /etc/persistent/bandwidth/bandwidth.cfg and generates rules.

Configuration file etc/persistent/bandwidth/bandwidth.cfg pattern for limiting per IP

Up_dev:Up_bandwidth:Down_dev:Down_bandwidth:ip:pps

Configuration file etc/persistent/bandwidth/bandwidth.cfg pattern for limiting per interface:
dev:bandwidth

Keys of the limitation per IP

bandwidth.<index>.up.dev – specify Upload interface name [string].

bandwidth.<index>.up.speed – specify the maximum upload speed in kbps [integer].

bandwidth.<index>.down.dev – specify Download interface name [string].

bandwidth.<index>.down.speed – specify the maximum download speed in kbps [integer].

bandwidth.<index>.ip – specify IP address of the client for which the traffic limitation will be set.

bandwidth.<index>.pps – specify packet per second [integer]. The packet per second value must be calculated according formula:

$$\text{down.speed} * 1024 / 8 / 1000 = \text{pps}$$

The download speed should be multiplied by 1024 to get download speed in bps (bits per second). Then this value should be divided by 8 to get value in Bps (bytes per second). Then this value should be divided by 1000 (the average of the packet size is 1000 bytes).

For example download speed is 1Mbps (1024 kbps), then we calculate PPS according formula:

$$1024 * 1024 / 8 / 1000 = 131$$

This means that minimum PPS value should be 131, otherwise the download process can be unexpected.



If device works as bridge, the name of the bridge port interface (ixp, eth, ath and etc) should be used, not bridge interface name (br0, etc).

Keys of the limitation per interface:

bandwidth.<index>.iface – specify the interface of the ShadowMaster device for which the traffic limitation will be set.



Only the egress traffic can be limited per interface.

bandwidth.<index>.speed – specify the maximum egress traffic speed in kbps [integer].



The speed limitation per interface should be the sum of all speed limitations set per IP to that interface at the least..

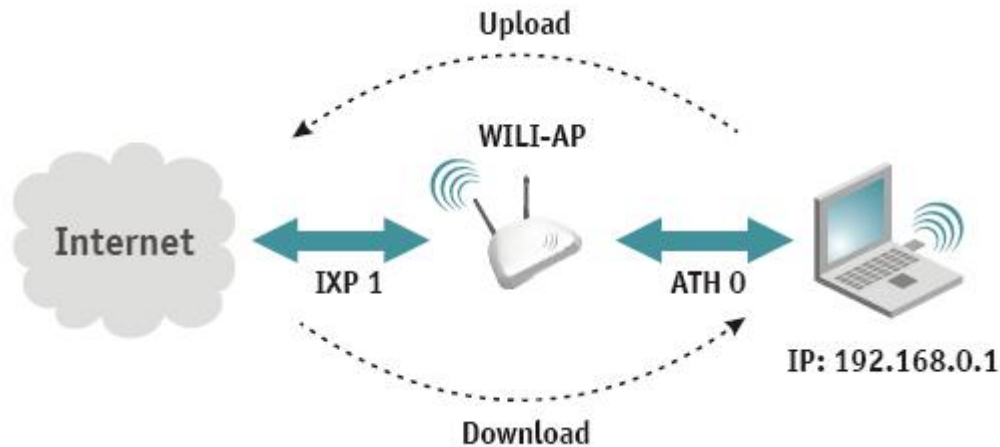


Figure 6.4.1: Traffic Limitation

According to the above Figure the configuration is:

```
bandwidth.1.up.dev=ixp1
bandwidth.1.up.speed=1024
bandwidth.1.down.dev=ath0
bandwidth.1.down.speed=1024
bandwidth.1.ip=192.168.0.1
bandwidth.1.pps=131
```

According this configuration the bandwidth configuration file /etc/persistent/bandwidth/bandwidth.cfg will be generated:

```
ixp1:1024:ath0:1024:192.168.0.1:131
```

The configuration of the limitation per interface:

```
bandwidth.2.devname=ath0 bandwidth.2.speed=10240
```

The bandwidth configuration file /etc/persistent/bandwidth/bandwidth.cfg will be generated:

```
ath0:10240
```


6.5 Management Access Configuration

This section describes user and administrative access settings, configuration of SSH, HTTP(S), SNMP servers and configuration of system users.

6.5.1 SSH Server

The SSH server is enabled by default on the ShadowMaster:

sshd.status – specify the SSH server status [enabled/disabled]. Default: enabled.

sshd.port – specify the port for incoming SSH connections [0-65535]. Default: 22.

Example:

```
# enable SSH server, these are the defaults
sshd.status=enabled
sshd.port=22
```

6.5.2 HTTP(S) Server

This section provides the description of the HTTP and HTTPS services configuration that makes ability to manage the ShadowMaster based device through a Web browser.

All available keys of the HTTP(S) configuration are listed below:

httpd.status – specify the HTTP(S) service status [enabled/disabled].

httpd.port.http – specify the TCP port for incoming HTTP requests [0-65535]. Default: 80.

httpd.port.https – specify the TCP port for incoming HTTPS requests [0-65535]. Default: 443.

httpd.port.admin – specify the TCP port for incoming HTTPS requests to Web configuration interface [0-65535]. Default: 444.

httpd.certificate.file – specify the server certificate file name required for HTTPS operation [file name with .pem extension]. It is treated as file name relative to /etc/persistent/public_cert/. Certificate file should be in PEM format.

httpd.certificate.key – specify the key file name for the server certificate required for HTTPS operation [file name with .key or .p12 extension]. It is treated as file name relative to /etc/persistent/private_key/. If certificate file is specified in PKCS#12 format (.p12 extension), it includes both the certificate and the key. In this case *httpd.certificate.file* value will be ignored.

httpd.certificate.key.password – specify the password for key decryption [string]. Only used if the certificate key is encrypted.

httpd.servername – specify the server name [string]. If this value is specified - HTTPS server will use it when generating self-referencing URL's, otherwise server will use client supplied IP address and port. Default: empty.

httpd.external.status – specify the external Web portal feature status [enabled/disabled]. Default: disabled.

httpd.external.secret – specify the external Web portal shared secret [string]. Default: empty.

The configuration keys for server performance tuning and troubleshooting:

httpd.backlog – specify the maximum pending connections HTTP server accepts [0-65535]. Default: 100.

httpd.max.request – specify the maximum size for POST requests [0-65535]. Default: 51200.

httpd.max.connections – specify the maximum requests to be served concurrently [0-65535]. Default: 50.

httpd.max.idletime – specify the maximum session idle time (in seconds) before session is considered inactive and automatically destroyed [integer]. Default: 1800 seconds.

httpd.verbose – specify for additional logging information. Default: disabled.

Example:

```
# setup HTTP(S) server
httpd.status=enabled
httpd.port.http=80
httpd.port.https=443
httpd.port.admin=444
httpd.certificate.file=/usr/etc/httpd/server.pem
httpd.certificate.key=/usr/etc/httpd/key.pem
httpd.backlog=100
httpd.external.status=disabled
httpd.max.connections=50
httpd.max.request=51200
httpd.verbose=disabled
```

6.5.3 SNMP Agent

SNMP is the standard network management protocol. The Hotspot-in-a-Box has a built-in SNMP agent. To communicate with SNMP agent you must configure SNMP communities and identifiers on both the SNMP manager and SNMP agent. The ShadowMaster supports all three SNMP protocol versions (v1, v2c and v3) in read-only mode.

All available keys of the SNMP configuration are listed below:

snmpd.status – specify the SNMP service status on AC [enabled/disabled]. With this service enabled the AC acts as the SNMP agent and can be monitored using SNMP.

snmpd.name – specify an administratively assigned name for this managed node [string]. By convention, this is the node's fully qualified domain name.

snmpd.location – specify the physical location of this node (e.g., `telephone closet, 3rd floor') [0-99 string].

snmpd.contact – specify the textual identification of the contact person for this managed node, together with information on how to contact this person [0-99 string].



SNMP community name is only used in SNMP version 1 and version 2c.

snmpd.rocommunity – specify the read-only community name [1-32 string].



SNMP user name and password are used in SNMP version 3.

snmpd.rouser – specify the user name for read-only SNMPv3 access [1-32 string].

snmpd.ropassword – specify the password for read-only SNMPv3 access [8-32 string].

Setup the Trap messages sending. The system sends a Cold Start trap when it starts up. If enabled, it also sends traps on authentication failures. Multiple *trapsink*, *trap2sink* and *informsink* hosts may be specified. Use *trap2sink* to send SNMPv2 traps and *informsink* to send inform notifications.

snmpd.traps.status – specify the trap message sending status [enabled/disabled]. Default: enabled.

snmpd.auth.traps – specify the generation of authentication failure traps status [enabled/disabled]. Default: disabled.

snmpd.trap.community – specify the community name for the SNMP trap message [string]. This community will be used in trap messages to authenticate to the SNMP manager [community string].

snmpd.trapsink. <index>.host – specify the host IP address that will receive the SNMPv1 traps [IP address].

snmpd.trapsink. <index>.community – specify the community name for SNMPv1 traps [string]. If community is not specified, the *snmpd.trap.community* will be used.

snmpd.trapsink. <index>.port – specify the port number the SNMPv1 trap messages should be send through [0-65535]. Default: 162

snmpd.trap2sink. <index>.host – specify the host IP address that will receive the SNMPv2 traps [IP address].

snmpd.trap2sink. <index>.community – specify the community name for SNMPv2 traps [string]. If community is not specified, the *snmpd.trap.community* will be used.

snmpd.trap2sink. <index>.port – specify the port number the SNMPv2 trap messages should be send through [0-65535]. Default: 162

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. However, a SNMP manager that receives an inform request acknowledges the message with an SNMP response PDU. If the manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

snmpd.informsink. <index>.host – specify the host IP address on which the inform requests will be enabled [IP address].

snmpd.informsink. <index>.community – specify the community name for inform requests [string]. If community is not specified, the *snmpd.trap.community* will be used.

snmpd.informsink. <index>.port – specify the port number the inform requests should be send through [0-65535]. Default: 162

Example:

```
# setup SNMP agent
snmpd.status=enabled
snmpd.contact=My system contact
snmpd.location=My system location
snmpd.name=My system
snmpd.rocommunity=public
snmpd.ropassword=secret
```

```
snmpd.rouser=user
snmpd.traps.status=enabled
snmpd.auth.traps=enabled
snmpd.trap.community=community_string
snmpd.trap2sink.1.host=192.168.2.21
snmpd.trap2sink.1.port=162
snmpd.trapsink.1.host=192.168.2.21
snmpd.trapsink.1.port=162
```

6.5.4 Network Usage Statistics

Configure this setting to gather and record network usage statistics if you want to see associated wireless clients on device.

Gathered network usage statistics consists of:

- MAC address of the client
- Device name
- Connection time (yyyy-mm-dd hh:mm)
- Disconnection time (for recently disassociated clients, the same format as connection time)
- RX bytes
- TX bytes
- SSID

statsd.status – enable network usage statistics gathering on device [enabled/disabled]. Default: disabled.

statsd.verbose – switch on debug messages of statistics (statsd) daemon [enabled/disabled]. Default: disabled.

6.6 System Services Configuration

This section describes system settings: device clock synchronization, NTP configuration and device message logging features.

6.6.1 Manual Clock Regulation

To set the device's internal clock, use these keys for configuration:

date.status – specify the manual clock status [enabled/disabled]. Default: disabled.

date.manual – specify the date value [MMDDhhmmYYYY.SS]. The time stamp format is:

MM - month (01-12)

DD - day of month (01-31)

hh - hour (00-23)

mm - minute (00-59)

YYYY - year (1970-2037)

SS - seconds (00-59)

date.lastknowntime.status – specify the last known time feature status [enabled/disabled].

When this feature is enabled, the system will save and restore the clock settings after reboot using

/etc/persistent/lastknowntime file. This should be used together with the NTP service (the system clock will be set to the last reboot time if no NTP servers are available). Default: disabled.

date.timezone – specify the timezone information [string]. The timezone string is one of special formats:

- std offset
- std offset dst [offset],start[/time],end[/time]

The first format is used when there is no daylight saving time in the local timezone. The std string specifies the name of the time zone and must be three or more alphabetic characters. The offset string immediately follows std and specifies the time value to be added to the local time to get Coordinated Universal Time (UTC). The offset is positive if the local time zone is west of the Prime Meridian and negative if it is east. The hour must be between 0 and 24, and the minutes and seconds 0 and 59.

The second format is used when there is daylight saving time. There are no spaces in the specification. The initial std and offset specify the standard time zone, as described above. The dst string and offset specify the name and offset for the corresponding daylight savings time zone. If the offset is omitted, it defaults to one hour ahead of standard time.

The start field specifies when daylight savings time goes into effect and the end field specifies when the change is made back to standard time. These fields may have the following formats:

- Jn** This specifies the Julian day with n between 1 and 365. February 29 is never counted even in leap years.
- n** This specifies the Julian day with n between 1 and 365. February 29 is counted in leap years.
- Mm.w.d** This specifies day d ($0 \leq d \leq 6$) of week w ($1 \leq w \leq 5$) of month m ($1 \leq m \leq 12$). Week 1 is the first week in which day d occurs and week 5 is the last week in which day d occurs. Day 0 is a Sunday.

The time fields specify when, in the local time currently in effect, the change to the other time occurs. If omitted, the default is 02:00:00.

Example 1:

```
# setup the device clock to year 2006, January 16th, 14:32:12, GMT+2
date.status=enabled
date.lastknowntime.status=disabled
date.manual=011614322006.12
date.timezone=GMT+2
```

Example 2:

```
# setup the lastknowntime function:
date.status=enabled
date.lastknowntime.status=enabled
date.timezone=GMT-2
```

6.6.2 NTP Client

The NTP (Network Time Protocol) service is used to synchronize the clock of the AC with a selected time server.



Up to 16 NTP servers can be configured on the ShadowMaster based device.

All available keys of the NTP client are listed below:

ntpd.status – specify the status for NTP service [enabled/disabled]. Default: disabled.

ntpd.<index>.status – specify the status of the particular NTP server [enabled/disabled].

ntpd.<index>.server – specify the trusted NTP server IP address or hostname for synchronizing time with [IP address or hostname string].

Example:

```
ntpd.status=enabled
ntpd.1.status=enabled
ntpd.1.server=192.53.103.103
```

6.6.3 Trace System

The trace system functionality provides debug information for system services and protocols should a malfunction occur. The trace system capability can help operators to locate mis-configurations and system errors.

The trace system functionality is controlled with the key:

sysconf.trace – specify the trace system status [enabled/disabled]. Default: disabled.

6.6.4 Syslog

You can configure the device to save log messages to a local or remote file using standard syslog facility.

All available keys of the Syslog service are listed below:

syslog.status – specify the status of syslog service [enabled/disabled].

syslog.file – specify the logged information file name with the path [string]. Default: /var/log/messages.

syslog.file.umask – specify the umask for the output file [numbers]. Default: 077

syslog.file.msg.level – specify the message level you need to trace. The level determines the importance of the message and the volume of messages generated by the AC. The levels are in order of increasing importance [emerg/alert/crit/err/warning/notice/info/debug]. Default: info.

You can configure the device to send system log messages to a remote server:

syslog.fwd.status – specify the remote syslog server status [enabled/disabled]. Default: disabled.

syslog.fwd.host.ip – specify the remote host IP address where syslog messages will be sent.

syslog.fwd.host.port – specify the port to which syslog messages will be forwarded [0-65535]. Default: 514.

syslog.fwd.msg.level – specify the message level that will be send to the remote syslog server. The levels are in order of increasing importance [emerg/alert/crit/err/warning/notice/info/debug] Default: info.



Up to 4 backup syslog hosts can be configured on the device.

syslog.fwd.backup.<index>.status - specify the status of backup syslog host [enabled/disabled]. Default: enabled.

syslog.fwd.backup.<index>.host.ip - specify the backup host IP address where syslog messages will be send to.

syslog.fwd.backup.<index>.host.port - specify the port to which syslog messages will be forwarded [0-65535]. Default: 514.

syslog.rotate.status – specify the rotation of logged message status [enabled/disabled]. Default: enabled.

syslog.rotate.at.size – specify the log size (in bytes) after which the rotation should start [1-9223372036854775807]. Default: 102400.

Example:

```
# With such configuration all messages that have level equal or higher than
# warning will be logged locally. Messages that have level equal or higher
# than critical will be logged on the remote syslog server
# 192.168.2.150:514, or to the backup server 192.168.2.152:514. The log
# message will be rotated when the syslog file will reach the 102400 bytes
# size.
```

```
syslog.status=enabled
syslog.file=/var/log/messages
syslog.file.msg.level=warning
syslog.file.umask=077
```

```
syslog.fwd.status=enabled
syslog.fwd.backup.1.status=enabled syslog.fwd.backup.1.host.ip=192.168.2.152
syslog.fwd.backup.1.host.port=514
syslog.fwd.host.ip=192.168.2.150
syslog.fwd.host.port=514
syslog.fwd.msg.level=crit
```

```
syslog.rotate.status=enabled
syslog.rotate.at.size=102400
```

6.6.5 IP Logging

IP logging function logs authenticated client station connection requests.



Be sure that syslog feature is configured properly before enabling IP logging feature.

The configuration file key of the IP Logging feature is:

ulogd.status – specify the IP logging status [enabled/disabled]. Default: disabled.

When IP logging is enabled the system continuously scans the activity of authenticated users and logs new TCP connection attempts to syslog. Each new connection is logged in the following format:

- Time stamp (time when connection was attempted).

- Source IP, source port.
- Destination IP, destination port.
- Client network card MAC address (if it can be determined).
- WAN interface IP address.
- Username

Example:

The following configuration snippet illustrates how we can setup IP logging on a router. Please be aware that ULOGD is targeted at router (NAT'ed) platform only and will not work on a simple AP.

```
firewall.rule.5.table=nat
firewall.rule.5.chain=POSTROUTING
firewall.rule.5.protocol=TCP
firewall.rule.5.tcpflags=SYN,RST,ACK SYN
firewall.rule.5.target=ULOG
firewall.rule.5.t.ulog.nlggroup=2
firewall.rule.5.t.ulog.prefix=non-nat

# Masquerade rules (customize to your needs!)
firewall.rule.6.table=nat
firewall.rule.6.chain=POSTROUTING
firewall.rule.6.out=ixpl
firewall.rule.6.target=MASQUERADE

firewall.rule.7.table=mangle
firewall.rule.7.chain=POSTROUTING
firewall.rule.7.protocol=TCP
firewall.rule.7.tcpflags=SYN,RST,ACK SYN
firewall.rule.7.target=ULOG
firewall.rule.7.t.ulog.nlggroup=2
firewall.rule.7.t.ulog.prefix=with-nat

# Enable ULOGD service
ulogd.status=enabled
```

6.6.6 Sysctl Plugin

The plugin allows to control kernel/sysctl parameters exported via /proc. Use the following keys to control sysctl plugin

sysctl.status – specify the status of the sysctl plugin [enabled/disabled].

sysctl.xxx – specify the value of the command. The symbols xxx is part of the key representing path to the file under /proc. Path symbols '/' must be replaced with '.'. Possible keys can be extracted with command:

```
find /proc/sys -type f | sed 's/\ /proc\/\./g' | sed 's/\ /\/\./g'
```

Example:

```
sysctl.status=enabled
sysctl.sys.net.ipv4.ip_forward=1
```


7.0 Appendix

7.1 Appendix A: ShadowMaster Specifications

Wireless Support	
Standard	IEEE 802.11a (OFDM) IEEE 802.11g (OFDM) IEEE 802.11b (DSSS) IEEE 802.11i IEEE 802.11d (Country element support) IEEE 802.11e (Enhancement: QoS, including WMM) IEEE 802.11h (5 GHz spectrum, DCS/DFS, TPC) IEEE 802.11j (Security and Public safety band support)
Data Rate	802.11g: 54, 48, 36, 24, 18, 12, 9, 6 Mbps 802.11b: 11, 5.5, 2, 1 Mbps (auto fall back) 802.11a: 54s, 48s, 36s, 24s, 18s, 12s, 9s, 6 Mbps
MBSSID (VSSID)	16 MBSSID (VLANs)
Encryption	WPA, WPA2, WEP64, WEP128, TKIP, IPsec with DES, 3DES, AES encryption, IKE
Network Access Control	
IP Router with NAT/NAPT, firewall filters	Hotspot access controller with 802.1x/EAP support, Smart Client support, WISPr compliant (Wi-Fi alliance)
AAA RADIUS client with EAP support	Universal access method (Web browser log-on) with XML support and walled garden (free Web sites)
Web proxy support (any client configuration is accepted)	WISPr compatible log-on via Web browser, SSL/TLS support
VPN client (GRE)	IEEE 802.1x authenticator with EAP-SIM, MD-5, TLS, TTLS, PEAP
WPA, WPA2 support (with hardware acceleration)	DHCP server, DHCP relay gateway, DHCP client
VPN pass-through	Layer 2 user isolation
E-mail redirection	Bandwidth management via RADIUS
Management	
Interfaces	HTTPS, SSH, SNMP (MIB II, Ethernet MIB, private MIB)
Software Update	Remote software update via HTTPS or FTP
Reset	Remote reset / Manufacturing reset

7.2 Appendix B: Regulatory Domain/Channels

This appendix lists the IEEE 802.11a and IEEE 802.11b channels supported by the world's regulatory domains. The ShadowMaster 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 as described below. Antenna types with similar in-band and out-of-band radiation patterns and the same or lower gain may be used with the same or lower power levels in Canada and the USA:

7.2.1 Channels for IEEE 802.11b/g

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	ShadowMaster IC / FCC Certification
1	2412	•	•	20.5 dBi panel antenna (SPAPG20) using transmit power levels up to 13 dB. 9.0 dBi Omni antenna (SPDG80) using transmit power levels up to 14 dB.
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.

7.2.2 Channels for IEEE 802.11a

Channels Identifiers	Frequency in MHz	USA, Canada (FCC)	European Union (CE/ETSI)	ShadowMaster IC / FCC Certification
34	5170	—	—	—
36	5180	•	•	16.8 dBi panel antenna (SPDN6W) using transmit power levels up to 7 dB.
38	5190	—	—	
40	5200	•	•	
42	5210	—	—	8.0 dBi Omni antenna (SPDJ6OP) using transmit power levels up to 14 dB.
44	5220	•	•	
46	5230	—	—	
48	5240	•	•	
52	5260	•	•	16.8 dBi panel antenna (SPDN6W) using transmit power levels up to 7 dB.
56	5280	•	•	8.0 dBi Omni antenna (SPDJ6OP) using transmit power levels up to 14 dB.
60	5300	•	•	<i>Full certification is still pending.</i>
64	5320	•	•	
100	5500	—	•	16.8 dBi panel antenna (SPDN6W) using transmit power levels up to 12 dB (9 dB at 5700)
104	5520	—	•	
108	5540	—	•	
112	5560	—	•	
116	5580	—	•	
120	5600	—	•	
124	5620	—	•	
128	5640	—	•	
132	5660	—	•	
136	5680	—	•	
140	5700	—	•	<i>Full certification is still pending.</i>
149	5745	•	—	
153	5765	•	—	16.8 dBi panel antenna (SPDN6W) up to 12 dB
157	5785	•	—	8.0 dBi Omni antenna (SPDJ6OP) up to 15 dB.
161	5805	•	—	—
165	5825	•	—	—



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.

7.3 Appendix C: Standard RADIUS Attributes

The following standard RADIUS attributes and messages are supported by the Hotspot-in-a-Box.

Required Attribute	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
User-Name	1	String	X		X	User enters full NAI
User-Password	2	String	X			Password of the user to be authenticated
NAS-IP-Address	4	Ipaddr	X		X	IP address of the Hotspot-in-a-Box
Service-Type	6	Integer	X			Must be set to Login (1)
Framed-IP-Address	8	Ipaddr	X		X	IP address of the user
Reply-Message	18	String		X		Text of reject reason if present
State	24	String	X	X		AC does not interpret the attribute locally
Class	25	String		X	X	Attribute provided by the authentication server, forwarded to the accounting server
Session-Timeout	27	Integer		X		Forced logout once timeout period reached (seconds)
Idle-Timeout	28	Integer		X		Implicit logout inactivity timeout period (seconds)
Called-Station-ID	30	String	X		X	This field should contain the MAC address or other information identifying the Hotspot-in-a-Box
NAS-Identifier	32	String	X		X	String identifying the NAS
Acct-Status-Type	40	Integer			X	1=Start, 2=Stop, 3=Interim Update
Acct-Delay-Time	41	Integer			X	Delay (seconds) between accounting event and when Acct-Req was sent (does not include estimated network transit time)
Acct-Input-Octets	42	Integer			X	Indicates how many octets have been received from the port over the course of this service being provided
Acct-Output-Octets	43	Integer			X	Indicates how many octets have been sent to the port in the course of delivering this service
Acct-Session-ID	44	String	X	X	X	Unique Accounting ID to make it easy to match start and stop records in a log file
Acct-Session-Time	46	Integer			X	Call duration in seconds (already compensated for idle timeout)

Required Attribute	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Acct-Input-Packets	47	Integer			X	Indicates how many packets have been received from the port over the course of this service being provided
Acct-Output-Packets	48	Integer			X	Indicates how many packets have been sent to the port in the course of delivering this service
Acct-Terminate-Cause	49	Integer			X	1=Explicit Logoff, 4=Idle Timeout, 5=Session Timeout, 6=Admin Reset, 9=NAS Error, 10=NAS Request, 11=NAS Reboot
Acct-Input-Gigawords	52	Integer			X	This attribute indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of this service being provided
Acct-Output-Gigawords	53	Integer			X	This attribute indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} in the course of delivering this service
NAS-Port-Type	61	Integer	X		X	15=Ethernet, 19=802.11
Acct-Interim-Interval	85	Integer		X		Interval (seconds) to send accounting updates

7.3.1 Vendor Specific Attributes

The Wi-Fi Alliance recommends a list of certain Vendor Specific Attributes (VSA). The VSA values are intended to provide location information to the backend processing system or to deliver service type information back to the Hotspot-in-a-Box.

The Wi-Fi Alliance has registered an IANA Private Enterprise Number (PEN) of 14122, which can be used to pass Vendor-Specific attributes to international roaming partners.

WISPr Vendor Specific Attributes	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Location-ID	1	String	X		X	Hotspot Location Identifier
Location-Name	2	String	X		X	Hotspot Location and Operator's Name
Logoff-URL	3	String	X			URL for user to perform explicit logoff
Redirection-URL	4	String		X		URL of Start Page
Bandwidth-Min-Up	5	Integer		X		Minimum Transmit Rate (bps)
Bandwidth-Min-Down	6	Integer		X		Minimum Receive Rate (bps)
Bandwidth-Max-Up	7	Integer		X		Maximum Transmit Rate (bps)
Bandwidth-Max-Down	8	Integer		X		Maximum Receive Rate (bps)
Session-Terminate-Time	9	String		X		Session termination time in ISO 8601 format: YYYY-MM-DDThh:mm:ssTZD
Session-Terminate-End-of-Day	10	Integer		X		Flag of one or zero indicating termination rule (terminate or not user's session at the end of a billing day).
Billing-Class-Of-Service	11	String		X		Text string indicating service type e.g. used for the visitor access feature



ShadowMaster vendor specific attributes are described at the client point of view (reverse accounting is disabled).

Waveteq Recommends vendors wishing to implement this portion obtain an IANA Private Enterprise Number (PEN), which can be used to pass Vendor-Specific attributes to international roaming partners.

ShadowMaster Vendor Specific Attributes	#	Type	Auth Req	Auth Reply	Acctg Req	Comment
Acct-Session-Input-Octets	21	Integer		X		Session download volume limitation in bytes. Forced logout once volume limitation is reached.
Acct-Session-Input-Gigawords	22	Integer		X		Session download volume limitation in bytes. Forced logout once volume limitation is reached
Acct-Session-Output-Octets	23	Integer		X		Session upload volume limitation in bytes. Forced logout once volume limitation is reached
Acct-Session-Output-Gigawords	24	Integer		X		Session upload volume limitation in bytes. Forced logout once volume limitation is reached
Acct-Session-Octets	25	Integer		X		Upload and download limitation
Acct-Session-Gigawords	26	Integer		X		Upload and download limitation

7.4 Appendix D: /etc/protocols

This table describes the various protocols that are available from the TCP/IP subsystem. The values will occur in the IP packet's protocol header. The latest version with references to further documentation can be found at <http://www.iana.org/assignments/protocol-numbers>.

Decimal value	Keyword	Protocol
0	HOPOPT	IPv6 Hop-by-Hop Option
1	ICMP	Internet Control Message
2	IGMP	Internet Group Management
3	GGP	Gateway-to-Gateway
4	IP	IP in IP (encapsulation)
5	ST	Stream
6	TCP	Transmission Control
7	CBT	CBT
8	EGP	Exterior Gateway Protocol
9	IGP	Any private interior gateway(used by Cisco for their IGRP)
10	BBN-RCC-MON	BBN RCC Monitoring
11	NVP-II	Network Voice Protocol
12	PUP	PUP
13	ARGUS	ARGUS
14	EMCON	EMCON
15	XNET	Cross Net Debugger
16	CHAOS	Chaos
17	UDP	User Datagram
18	MUX	Multiplexing
19	DCN-MEAS	DCN Measurement Subsystems
20	HMP	Host Monitoring
21	PRM	Packet Radio Measurement
22	XNS-IDP	XEROX NS IDP
23	TRUNK-1	Trunk-1
24	TRUNK-2	Trunk-2
25	LEAF-1	Leaf-1
26	LEAF-2	Leaf-2
27	RDP	Reliable Data Protocol
28	IRTP	Internet Reliable Transaction
29	ISO-TP4	ISO Transport Protocol Class 4
30	NETBLT	Bulk Data Transfer Protocol
31	MFE-NSP	MFE Network Services Protocol
32	MERIT-INP	MERIT Internodal Protocol
33	SEP	Sequential Exchange Protocol
34	3PC	Third Party Connect Protocol
35	IDPR	Inter-Domain Policy Routing Protocol
36	XTP	XTP
37	DDP	Datagram Delivery Protocol
38	IDPR-CMTP	IDPR Control Message Transport Protocol
39	TP++	TP++ Transport Protocol
40	IL	IL Transport Protocol
41	IPv6	Ipv6
42	SDRP	Source Demand Routing Protocol
43	IPv6-Route	Routing Header for IPv6

Decimal value	Keyword	Protocol
44	IPv6-Frag	Fragment Header for IPv6
45	IDRP	Inter-Domain Routing Protocol
46	RSVP	Reservation Protocol
47	GRE	General Routing Encapsulation
48	MHRP	Mobile Host Routing Protocol
49	BNA	BNA
50	ESP	Encap Security Payload
51	AH	Authentication Header
52	I-NLSP	Integrated Net Layer Security TUBA
53	SWIPE	IP with Encryption
54	NARP	NBMA Address Resolution Protocol
55	MOBILE	IP Mobility
56	TLSP	Transport Layer Security Protocol, Kryptonnet key mgmt
57	SKIP	SKIP
58	IPv6-ICMP	ICMP for IPv6
59	IPv6-NoNxt	No Next Header for IPv6
60	IPv6-Opts	Destination Options for IPv6
61		Any host internal protocol
62	CFTP	CFTP
63		any local network
64	SAT-EXPAK	SATNET and Backroom EXPAK
65	KRYPTOLAN	Kryptolan
66	RVD	MIT Remote Virtual Disk Protocol
67	IPPC	Internet Pluribus Packet Core
68		Any distributed file system
69	SAT-MON	SATNET Monitoring
70	VISA	VISA Protocol
71	IPCV	Internet Packet Core Utility
72	CPNX	Computer Protocol Network Executive
73	CPHB	Computer Protocol Heart Beat
74	WSN	Wang Span Network
75	PVP	Packet Video Protocol
76	BR-SAT-MON	Backroom SATNET Monitoring
77	SUN-ND	SUN ND PROTOCOL-Temporary
78	WB-MON	WIDEBAND Monitoring
79	WB-EXPAK	WIDEBAND EXPAK
80	ISO-IP	ISO Internet Protocol
81	VMTP	VMTP
82	SECURE-VMTP	SECURE-VMTP
83	VINES	VINES
84	TTP	TTP
85	NSFNET-IGP	NSFNET-IGP
86	DGP	Dissimilar Gateway Protocol
87	TCF	TCF
88	EIGRP	EIGRP
89	OSPFIGP	OSPFIGP
90	Sprite-RPC	Sprite RPC Protocol
91	LARP	Locus Address Resolution Protocol
92	MTP	Multicast Transport Protocol
93	AX.25	AX.25 Frames
94	IPIP	IP-within-IP Encapsulation Protocol

Decimal value	Keyword	Protocol
95	MICP	Mobile Internetworking Control Pro.
96	SCC-SP	Semaphore Communications Sec. Pro.
97	ETHERIP	Ethernet-within-IP Encapsulation
98	ENCAP	Encapsulation Header
99		Any private encryption scheme
100	GMTP	GMTP
101	IFMP	Ipsilon Flow Management Protocol
102	PNNI	PNNI over IP
103	PIM	Protocol Independent Multicast
104	ARIS	ARIS
105	SCPS	SCPS
106	QNX	QNX
107	A/N	Active Networks
108	IPComp	IP Payload Compression Protocol
109	SNP	Sitara Networks Protocol
110	Compaq-Peer	Compaq Peer Protocol
111	IPX-in-IP	IPX in IP
112	VRRP	Virtual Router Redundancy Protocol
113	PGM	PGM Reliable Transport Protocol
114		any 0-hop protocol
115	L2TP	Layer Two Tunneling Protocol
116	DDX	D-II Data Exchange(DDX)
117	IATP	Interactive Agent Transfer Protocol
118	STP	Schedule Transfer Protocol
119	SRP	SpectraLink Radio Protocol
120	UTI	UTI
121	SMP	Simple Message Protocol
122	SM	SM
123	PTP	Performance Transparency Protocol
124	ISIS over IPv4	
125	FIRE	
126	CRTP	Combat Radio Transport Protocol
127	CRUDP	Combat Radio User Datagram
128	SSCOMPCE	
129	IPLT	
130	SPS	Secure Packet Shield
131	PIPE	Private IP Encapsulation within IP
132	SCTP	Stream Control Transmission Protocol
133	FC	Fibre Channel
134	RSVP-E2E-IGNORE	
135	Mobility Header	
136	UDPLite	
137-252	Unassigned	
253-254	Use for experimentation and testing	
255	Reserved	

7.5 Appendix E: ISO Country Codes

This list states the country codes (a numeric code of a physical territory) and the country names (official short 2 or 3 letters names in English) in alphabetical order as given in ISO 3166-1 and the corresponding ISO 3166-1-alpha-2 code elements.

Each country or territory has three codes:

- a two letter code
- a three letter code
- a three digit code

This is a subset of the full ISO 3166 lists. The countries listed here are supported in the wireless interface drivers (**radio.countrycode** key). See <http://www.iso.org/iso/en/prods-services/iso3166ma/02iso-3166-code-lists/index.html> and <http://unstats.un.org/unsd/methods/m49/m49alpha.htm> for the complete ISO country code lists.

Country Codes			Country	Country Codes			Country
AL	ALB	008	Albania	KE	KEN	404	Kenya
DZ	DZA	012	Algeria	KP	PRK	408	Korea, democratic people's republic of
AR	ARG	032	Argentina	KR	KOR	410	Korea, republic of
AM	ARM	051	Armenia			411	South Korea
AU	AUS	036	Australia	KW	KWT	414	Kuwait
AT	AUT	040	Austria	LV	LVA	428	Latvia
AZ	AZE	031	Azerbaijan	LB	LBN	422	Lebanon
BH	BHR	048	Bahrain	LY	LBY	434	Libyan Arab Jamahiriya
BY	BLR	112	Belarus	LI	LIE	438	Liechtenstein
BE	BEL	056	Belgium	LT	LTU	440	Lithuania
BZ	BLZ	084	Belize	LU	LUX	442	Luxembourg
BO	BOL	068	Bolivia	MO	MAC	446	Macao
BR	BRA	076	Brazil	MK	MKD	807	Macedonia, the former Yugoslav republic of
BN	BRN	096	Brunei Darussalam	MY	MYS	458	Malaysia
BG	BGR	100	Bulgaria	MX	MEX	484	Mexico
CA	CAN	124	Canada	MC	MCO	492	Monaco
CL	CHL	152	Chile	MA	MAR	504	Morocco
CN	CHN	156	China	NL	NLD	528	Netherlands Antilles
CO	COL	170	Colombia	NZ	NZL	554	New Zealand
CR	CRI	188	Costa Rica	NI	NIC	558	Nicaragua
HR	HRV	191	Croatia	NO	NOR	578	Norway
CY	CYP	196	Cyprus	OM	OMN	512	Oman
CZ	CZE	203	Czech republic	PK	PAK	586	Pakistan

Country Codes			Country	Country Codes			Country
DK	DNK	208	Denmark	PA	PAN	591	Panama
DO	DOM	214	Dominican republic	PY	PRY	600	Paraguay
EC	ECU	218	Ecuador	PE	PER	604	Peru
EG	EGY	818	Egypt	PH	PHL	608	Philippines
SV	SLV	222	El Salvador	PL	POL	616	Poland
EE	EST	233	Estonia	PT	PRT	620	Portugal
FO	FRO	234	Faroe islands	PR	PRI	630	Puerto Rico
FI	FIN	246	Finland	QA	QAT	634	Qatar
FR	FRA	250	France	RO	ROU	642	Romania
		255	France2	RU	RUS	643	Russian federation
GE	GEO	268	Georgia	SA	SAU	682	Saudi Arabia
DE	DEU	276	Germany	SG	SGP	702	Singapore
GR	GRC	300	Greece	SK	SVK	703	Slovakia
GT	GTM	320	Guatemala	SI	SVN	705	Slovenia
HN	HND	340	Honduras	ZA	ZAF	710	South Africa
HK	HKG	344	Hong Kong	ES	ESP	724	Spain
HU	HUN	348	Hungary	SE	SWE	752	Sweden
IS	ISL	352	Iceland	CH	CHE	756	Switzerland
IN	IND	356	India	SY	SYR	760	Syrian Arab republic
ID	IDN	360	Indonesia	TW	TWN	158	Taiwan
IR	IRN	364	Iran, Islamic republic of	TH	THA	764	Thailand
IQ	IRQ	368	Iraq	TT	TTO	780	Trinidad and Tobago
IE	IRL	372	Ireland	TN	TUN	788	Tunisia
IL	ISR	376	Israel	TR	TUR	792	Turkey
IT	ITA	380	Italy	AE	ARE	784	United Arab Emirates
JM	JAM	388	Jamaica	UA	UKR	804	Ukraine
JP	JPN	392	Japan	GB	GBR	826	United Kingdom
		393	Japan (JP1)	US	USA	840	United States
		394	Japan (JP0)	UY	URY	858	Uruguay
		395	Japan (JP1-1)	UZ	UZB	860	Uzbekistan
		396	Japan (JE1)	VE	VEN	862	Venezuela
		397	Japan (JE2)	VN	VNM	704	Viet Nam
JO	JOR	400	Jordan	YE	YEM	887	Yemen
KZ	KAZ	398	Kazakhstan	ZW	ZWE	716	Zimbabwe

7.6 Appendix G: Weather-Proofing

Waveteq uses high quality connectors that have been specifically selected to resist the elements. Under some circumstances it can be recommended that additional weather proofing be applied to the connectors once the ShadowMaster has been mounted and connections have been completed.

Two types of products can be recommended; first, silicone rubber self-fusing tape which bonds to itself providing UV, moisture and dielectric resistance. Secondly, for hard to tape areas, most self-fusing tape companies also offer filler compounds that have similar characteristics and can also support addition of self-fusing tape.

For further properties, recommendations, or usage please contact Waveteq or your local wireless installer.

Minimum requirements to follow during preparation of any tape configuration are as follows:

- At least two (2) layers of tape should be applied over any surface onto which the tape is wrapped (i.e. bare connection, or cable/wire insulation or jacket).
- Tape must be overlapped onto the cable/wire insulation/jacket a minimum distance of 1.5" when an environmental seal is required.
- First layer of tape should be applied with maximum stretch (<75% of original width). Second layer should be applied with minimal/zero stretch.

Consult your tape manufacturer's guidelines for specific recommendations on application. Presented below are general recommendations when applying self fusing tape or fill:

- If "fill" is required, use Self-Fusion compound to fill in and around all irregular surfaces in order to cover sharp surfaces (i.e. bolts, screws, nuts, terminal lug, butt splice, electrical connector, etc.) and also to create a smooth evenly tapered surface, prior to application of self-fusing tape.
Note: When using tape for this purpose, simply stretch and push tape into cavity using finger or thumb pressure. Cutting small pieces and pushing tape into cavity is another method for filling the irregular surfaces.
- Cut an appropriate length of tape from the roll and remove the liner, taking care not to allow the tape to fold over onto itself.
- Begin wrapping the first layer of tape onto the wire or connection by holding the lead end on the surface and stretching the tape around until it touches itself. The first layer of tape should be stretched continually so that the tape reduces to <3/4 of its original width. The tape should be applied until it extends a minimum of 1 inch past any bare, un-insulated conducting surface.
Note: Tape should be wrapped in a half-lapped fashion. If an environmental seal is not required, then the tape doesn't need to be stretched on any layer.
- Wrap a second layer of tape over the entire surface of the first layer. Figure 7.6.1 below shows a properly taped Ethernet connection after the second tape layer.
Note: It is not necessary to stretch the second layer of tape, as the first layer provides the permanent environmental seal and the tape fuses to itself upon contact.



Figure 7.6.1: Properly taped Ethernet adapter

To ensure a proper weather proof seal, all external ports should be wrapped with tape . These include ports that are not used in the installation such as unused Ethernet or antenna ports (external 'N' connectors). Figure 7.6.2 below shows a properly taped external 'N' type connector.



Figure 7.6.2: Properly taped external antenna port.

7.7 Appendix H: Factory Default Configuration File

```
#####
# Configuration created by skin
# Skin: Waveteq, version: 0.5.14704
# Generated on 2008-05-01 16:04:54 UTC
#####
-notes.1=Waveteq Communications Factory Default Configuration
-notes.2=Bridged 5.18 GHz (802.11a) Access Point Using Internal Antenna
-Product=ShadowMaster
```

```
# AUTHENTICATION, AUTHORIZATION AND ACCOUNTING:
#
```

```
aaa.1.devname=ath0
aaa.1.nas.1.profile=NAS-ath0
aaa.1.nas.1.status=disabled
aaa.1.status=disabled
aaa.1.wan.1.devname=ixp0
aaa.1.wan.1.status=enabled

aaa.2.devname=ath1
aaa.2.nas.2.profile=NAS-ath1
aaa.2.nas.2.status=disabled
aaa.2.status=disabled
aaa.auth.1.status=disabled
aaa.domain.1.auth.1.status=enabled
aaa.domain.1.name=DOMAIN_PROFILE_PSK
aaa.domain.1.status=disabled
aaa.nas.1.acct.status=disabled
aaa.nas.1.auth.status=disabled
aaa.nas.1.devname=ath0
aaa.nas.1.domain.1.status=disabled
aaa.nas.1.maxclients=64
aaa.nas.1.name=NAS-ath0
aaa.nas.1.security.profile=WPA-PSK-ath0
aaa.nas.1.security.type=wpa
aaa.nas.1.status=disabled
aaa.nas.2.acct.status=disabled
aaa.nas.2.auth.status=disabled
aaa.nas.2.devname=ath1
aaa.nas.2.domain.1.status=disabled
aaa.nas.2.maxclients=64
aaa.nas.2.name=NAS-ath1
aaa.nas.2.security.profile=WPA-PSK-ath1
aaa.nas.2.security.type=wpa
aaa.nas.2.status=disabled
aaa.security.wpa.1.key.cipher=TKIP
aaa.security.wpa.1.key.method=PSK
aaa.security.wpa.1.mode=WPA2
aaa.security.wpa.1.name=WPA-PSK-ath0
aaa.security.wpa.1.passphrase=verysecretphrase
aaa.security.wpa.1.status=disabled
aaa.security.wpa.2.key.cipher=TKIP
aaa.security.wpa.2.key.method=PSK
aaa.security.wpa.2.mode=WPA2
aaa.security.wpa.2.name=WPA-PSK-ath1
aaa.security.wpa.2.passphrase=verysecretphrase
aaa.security.wpa.2.status=disabled
aaa.status=disabled
```

```
# USER ACCESS CONTROLLER:
# This section sets up white and black lists to control user access
#
access.status=disabled
access.verbose=disabled
```

```
# SETTING TO LOCK OUT THE WLAN:
# Useful to shut down the WLAN when a set number of pings is not returned
# When the pings return the network is restored
#
autolock.interval=300
autolock.retry_count=3
autolock.status=disabled

# BRIDGE:
# Transparently relays traffic between multiple interfaces
#
bridge.1.devname=br0
bridge.1.port.1.devname=ixp0
bridge.1.port.1.priority=1
bridge.1.port.1.status=enabled
bridge.1.port.2.devname=ixp1
bridge.1.port.2.priority=2
bridge.1.port.2.status=disabled
bridge.1.port.3.devname=ath0
bridge.1.port.3.priority=3
bridge.1.port.3.status=enabled
bridge.1.port.4.devname=ath1
bridge.1.port.4.priority=4
bridge.1.port.4.status=disabled
bridge.1.status=enabled
bridge.1.stp.status=disabled

bridge.2.port.1.devname=ixp0
bridge.2.port.1.priority=1
bridge.2.port.1.status=disabled
bridge.2.port.2.devname=ixp1
bridge.2.port.2.priority=2
bridge.2.port.2.status=disabled
bridge.2.port.3.devname=ath0
bridge.2.port.3.priority=3
bridge.2.port.3.status=disabled
bridge.2.port.4.devname=ath1
bridge.2.port.4.priority=4
bridge.2.port.4.status=disabled
bridge.2.status=disabled
bridge.2.stp.status=disabled
bridge.status=enabled

# DATE:
# Format is MMDDhhmmYYYY.SS
# There are setting for timezone, daylight savings, reboot time settings
#
date.status=disabled
date.timezone=GMT+8
dhcp-fwd.status=disabled

# DHCP CLIENT:
# Used to accept an IP address from a DHCP server
#
dhcpc.1.devname=ixp0
dhcpc.1.status=disabled
dhcpc.2.devname=ixp1
dhcpc.2.status=disabled
dhcpc.3.devname=ath0
dhcpc.3.status=disabled
dhcpc.4.devname=ath1
dhcpc.4.status=disabled
dhcpc.status=disabled
```



```
# DHCP SERVER:
# Each LAN interface (ixp0 & ixp1) runs a separate DHCP server to
# assign IP addresses. The DNS server, the IP address range, the
# gateway IP address and the network mask are specified
#
dhcpd.1.devname=ixp0
dhcpd.1.status=disabled
dhcpd.2.devname=ixp1
dhcpd.2.status=disabled
dhcpd.3.devname=ath0
dhcpd.3.status=disabled
dhcpd.4.devname=ath1
dhcpd.4.status=disabled
dhcpd.status=disabled

# DNS FORWARDER:
# DNS request forwarder intercepts all DNS requests
# from clients and forwards them to a DNS server
#
dnsmasq.status=disabled

# BRIDGE FIREWALL:
# Used to filter layer 2 Packets using a bridging firewall that contains
# three built in tables: Filter, NAT and Broute
#
ebtables.broute.BROUTING.policy=ACCEPT
ebtables.filter.FORWARD.policy=ACCEPT
ebtables.filter.INPUT.policy=ACCEPT
ebtables.filter.OUTPUT.policy=ACCEPT
ebtables.nat.OUTPUT.policy=ACCEPT
ebtables.nat.POSTROUTING.policy=ACCEPT
ebtables.nat.PREROUTING.policy=ACCEPT
ebtables.rule.1.chain=BROUTING
ebtables.rule.1.in=ath0
ebtables.rule.1.protocol=0x888e
ebtables.rule.1.status=disabled
ebtables.rule.1.table=broute
ebtables.rule.1.target=DROP
ebtables.rule.2.chain=BROUTING
ebtables.rule.2.in=ath1
ebtables.rule.2.protocol=0x888e
ebtables.rule.2.status=disabled
ebtables.rule.2.table=broute
ebtables.rule.2.target=DROP
ebtables.status=enabled

# IP FIREWALL:
# Used to filter layer 3 Packets using a bridging firewall that contains
# three built in tables and corresponding chain lists:
# NAT(PreRouting, PostRouting, Output),
# MANGLE(PreRouting, Input, Forward, Output, PostRouting) and
# FILTER(Input, Forward, Output)
#
firewall.filter.FORWARD.policy=ACCEPT
firewall.filter.INPUT.policy=ACCEPT
firewall.filter.OUTPUT.policy=ACCEPT
firewall.mangle.FORWARD.policy=ACCEPT
firewall.mangle.INPUT.policy=ACCEPT
firewall.mangle.OUTPUT.policy=ACCEPT
firewall.mangle.POSTROUTING.policy=ACCEPT
firewall.mangle.PREROUTING.policy=ACCEPT
firewall.nat.OUTPUT.policy=ACCEPT
firewall.nat.POSTROUTING.policy=ACCEPT
firewall.nat.PREROUTING.policy=ACCEPT
firewall.status=enabled
```

```
# FORKER:
# Do NOT change this setting
#
forker.status=enabled
forker.verbose=disabled

# HTTP WEBSERVER:
# These settings provide the ability to manage your device through
# a WEB Browser.
#
httpd.backlog=100
httpd.max.connections=50
httpd.max.idletime=1800
httpd.max.request=51200
httpd.port.admin=444
httpd.port.http=80
httpd.port.https=443
httpd.status=enabled

# IPSEC PROTOCOL CLIENT:
# IP sec is supported in both the transport and tunnel modes
# If enabled it can provide an independent secure connection between
# two remote LANs to provide a VPN solution
# a number of secure channels can be established simultaneously
#
ipsec.status=disabled

# MESH:
# Do NOT change these settings
#
mesh.status=disabled

# NETWORK INTERFACE:
# Assigns IP addresses and subnet masks
#
netconf.1.devname=ixp0
netconf.1.ip=0.0.0.0
netconf.1.netmask=255.255.255.0
netconf.1.status=enabled
netconf.1.up=enabled

netconf.2.devname=ixp1
netconf.2.ip=192.168.10.1
netconf.2.netmask=255.255.255.0
netconf.2.status=enabled
netconf.2.up=enabled

netconf.3.devname=ath0
netconf.3.ip=0.0.0.0
netconf.3.netmask=255.255.255.0
netconf.3.status=enabled
netconf.3.up=enabled

netconf.4.devname=ath1
netconf.4.ip=0.0.0.0
netconf.4.netmask=255.255.255.0
netconf.4.status=enabled
netconf.4.up=disabled

netconf.5.devname=br0
netconf.5.ip=192.168.3.1
netconf.5.netmask=255.255.255.0
netconf.5.status=enabled
netconf.5.up=enabled
```

```
netconf.6.devname=br1
netconf.6.ip=
netconf.6.netmask=
netconf.6.status=disabled
netconf.6.up=disabled
netconf.status=enabled

# NTP (NETWORK TIME PROTOCOL) CLIENT SETTINGS:
# This is used to synchronize the clock of the Access Controller to a
# selected time server. Up to 16 NTP servers can be configured.
#
ntpd.status=disabled

# IPSEC RACON:
# Uses the Internet Key Exchange (IKE) for automatically keying IPsec connections
#
racoon.status=disabled

# RADIO SETTINGS:
# This section configures the radio parameters such as channel,
# 802.11 mode (ieee mode), antenna, and acktimeout/ctstimeout/slottime
# Refer to Sections 7.3.10.1 and 7.3.10.2 in the User Manual
# and to the application note for details.
#
# Valid channels for IEEE 802.11.B/G:
# CANADA, USA AND MEXICO: Ch. 01 to 11
# EUROPE(except FRANCE): Ch. 01 to 13
# FRANCE: Ch. 10 to 13
# ISRAEL: Ch. 03 to 09
# CHINA: Ch. 01 to 13
# JAPAN: Ch. 01 to 14
#
# Mode B/G are Channels (Frequency in MHz):
# 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)
#
# Valid channels for IEEE 802.11.A:
# CANADA, USA AND MEXICO: 36,40,44,48,52,56,60,64,149,153,157,161,165
# EUROPE: 36,40,44,48,52,56,60,64,100,104,108,112,
# 116,120,124,128,132,136,140
# SINGAPORE: 36,42,44,48
# CHINA: 140,153,157,161
# JAPAN: 34,38,42,46
#
# Mode A Channels Numbers and Corresponding Frequencies (MHz)
# 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) 165(5825)
#
radio.1.acktimeout=55
radio.1.ani=disabled
radio.1.autochannel.status=disabled
radio.1.channel=153
radio.1.ctstimeout=55
radio.1.devname=ath0
radio.1.frag=off
radio.1.ieee_mode=A
radio.1.mode=master
```

```
radio.1.rate.auto=enabled
radio.1.rate.max=54M
radio.1.rts=off
radio.1.rx_antenna=2
radio.1.rx_antenna_diversity=disabled
radio.1.slottime=26
radio.1.status=enabled
radio.1.turbo=disabled
radio.1.tx_antenna=2
radio.1.tx_antenna_diversity=disabled
radio.1.txpower=12

radio.2.acktimeout=55
radio.2.ani=disabled
radio.2.autochannel.status=disabled
radio.2.channel=1
radio.2.cts timeout=55
radio.2.devname=ath1
radio.2.frag=off
radio.2.ieee_mode=G
radio.2.mode=master
radio.2.rate.auto=enabled
radio.2.rate.max=54M
radio.2.rts=off
radio.2.rx_antenna=1
radio.2.rx_antenna_diversity=disabled
radio.2.slottime=26
radio.2.status=enabled
radio.2.turbo=disabled
radio.2.tx_antenna=1
radio.2.tx_antenna_diversity=disabled
radio.2.txpower=14
radio.countrycode=CA
radio.outdoor=1
radio.status=enabled
radio.xchanmode=1

# DNS:
# Translates host names into their IP addressed based on a configuration file
# or dynamically through a DHCP lease
#
resolv.status=disabled

# STATIC ROUTING:
# This section is used to setup static routes to specific hosts
# or networks through an interface.
#
route.ip_forward=enabled
route.status=enabled

# SNMP STANDARD NETWORK MANAGEMENT PROTOCOL:
# Configures both the Manager and SNMP agent
#
snmpd.status=disabled

# STATIC SUPERVISION:
# This feature complements authentication, authorization and accounting (AAA)
# by notifying which client station should be monitored for availability.
# After a specified number of retries, users authenticated for that
# station are logged out. Static supervision should run on each
# interface that AAA is running on.
#
ssid.1.check.count=5
ssid.1.check.interval=60
ssid.1.devname=ath0
```

```
ssd.1.status=disabled

ssd.2.check.count=5
ssd.2.check.interval=60
ssd.2.devname=ath1
ssd.2.status=disabled
ssd.status=disabled

# SSH (SECURE SHELL) SERVER:
# Provides remote access capability using a secure shell (i.e. Putty).
# The SSH server is enabled on port 22 and is enabled
# by default to ensure communications capability
#
sshd.port=22
sshd.status=enabled

# NETWORK USAGE STATISTICS:
# Enable this to gather network usage statistics like the MAC address
# of the client, device name, connection & disconnection times, number
# of bytes received and transmitted, SSID
#
statsd.status=disabled
statsd.verbose=disabled

# SYSTEM TRACE:
# This feature provides debug information for system services and
# protocols should a malfunction occur. It is useful to locate
# mis-configurations and system errors.
#
sysconf.trace=disabled

# SYSTEM LOG:
# This feature allows systems log files to be set up to local
# or remote files for system devices.
#
syslog.file=/var/log/messages
syslog.file.msg.level=info
syslog.file.umask=077
syslog.fwd.msg.level=info
syslog.fwd.status=disabled
syslog.rcms.alarm.level=info
syslog.rcms.alarm.status=disabled
syslog.rotate.at.size=102400
syslog.rotate.status=enabled
syslog.status=enabled

# GENERIC ROUTING ENCAPSULATION (GRE) TUNNEL:
# This provides a solution to tunnel private address-space traffic
# over an intermediate TCP/IP network such as the Internet.
# GRE tunnels encapsulate data over the WAN without using encryption
#
tunnel.gre.status=disabled

# USER CONNECTIONS LOG:
# Allows logging of IP's, MAC addresses (if available) and other
# connection information.
#
ulogd.status=disabled

# USERS:
# User accounts and their (encrypted) passwords.
# Do NOT change this setting
#
```

```
users.status=enabled
users.1.name=admin
users.1.password=oHS13yqR.tluQ
users.1.status=enabled

# VIRTUAL LOCAL AREA NETWORK (VLAN):
# VLANs allow for logical groupings of network resources to be assigned
# and have access control policies to be applied on a per-VLAN basis.
# VLANs are identified by VLAN ID number so for a physical interface ixp0
# designated with VLAN 10 will appear as ixp0.10. Up to 4094 VLANs can be
# created on the system.
#
vlan.status=disabled

# VIRTUAL SERVICE SET IDENTIFIER (VSSID):
# This feature can be used to provide another 15 virtual
# wireless networks in addition to that defined by the primary SSID.
# They can be configured for different security settings and are active
# at the same time. If you plan on having a mixture of master and managed
# vssid's the wireless card must be setup as a MASTER and the SSID
# must be configured before adding VSSIDs.
#
vssid.status=disabled

# WIRELESS ACCESS CONTROL LIST (ACL):
# The wireless ACL controls both default access by wireless clients to the
# wireless network interfaces as well as special access rules for wireless
# clients. Wireless ACL controls can be applied to ath0, ath1 & VSSIDs.
#
wac1.status=disabled

# WIRELESS DISTRIBUTION SYSTEM (WDS) SETTINGS:
# The WDS feature allows the creation of wireless infrastructure so
# that it can be connected at Layer 2 and therefore be seamlessly
# joined to a wired network. The WDS feature also allows wireless
# Access Points to be wirelessly connected, eliminating the need
# for a wired connection between them.
#
wds.1.parent=ath0
wds.1.status=enabled
wds.2.parent=ath1
wds.2.status=disabled
wds.status=enabled

# WIRELESS INTERFACE SETTINGS:
# These setting configure the general wireless LAN interface parameters
# such as WEP, SSID, SSID broadcast suppression, Maximum number of clients,
# Country element (IEEE802.11d), power constraints and channel switch
# for IEEE802.11h, Layer 2 isolation throughput enhancements
# and Wireless Multi-Media (WMM).
#
wireless.1.authmode=1
wireless.1.chanswitch=disabled
wireless.1.compression=disabled
wireless.1.country_element=disabled
wireless.1.devname=ath0
wireless.1.fastframes=disabled
wireless.1.frameburst=disabled
wireless.1.l2_isolation=disabled
wireless.1.max_clients=64
wireless.1.power_constrain=disabled
wireless.1.security=none
wireless.1.security.1.key=
wireless.1.security.default_key=1
```

```
wireless.1.security.mode=open
wireless.1.ssid=DEFAULT1
wireless.1.ssid_broadcast=enabled
wireless.1.status=enabled
wireless.1.wmm=disabled

wireless.2.authmode=1
wireless.2.chanswitch=disabled
wireless.2.compression=disabled
wireless.2.country_element=disabled
wireless.2.devname=ath1
wireless.2.fastframes=disabled
wireless.2.frameburst=disabled
wireless.2.l2_isolation=disabled
wireless.2.max_clients=64
wireless.2.power_constrain=disabled
wireless.2.security=none
wireless.2.security.1.key=
wireless.2.security.default_key=1
wireless.2.security.mode=open
wireless.2.ssid=DEFAULT2
wireless.2.ssid_broadcast=enabled
wireless.2.status=enabled
wireless.2.wmm=disabled
wireless.status=enabled

# WPA_802.1x SUPPLICANT SETTINGS:
# In situations where a wireless interface will connect to an access point
# the supplicant allows you to configure the user authentication settings
# required to connect.
#
wpa_supplicant.device.1.devname=ath0
wpa_supplicant.device.1.driver=madwifi
wpa_supplicant.device.1.profile=WPA-sup-ath0
wpa_supplicant.device.1.status=disabled
wpa_supplicant.device.2.devname=ath1
wpa_supplicant.device.2.driver=madwifi
wpa_supplicant.device.2.profile=WPA-sup-ath1
wpa_supplicant.device.2.status=disabled
wpa_supplicant.profile.1.ap_scan=enabled
wpa_supplicant.profile.1.eapol_version=1
wpa_supplicant.profile.1.fast_reauth=enabled
wpa_supplicant.profile.1.name=WPA-sup-ath0
wpa_supplicant.profile.1.network.1.group.1.name=TKIP
wpa_supplicant.profile.1.network.1.key_mgmt.1.name=WPA-PSK
wpa_supplicant.profile.1.network.1.pairwise.1.name=TKIP
wpa_supplicant.profile.1.network.1.proto.1.name=RSN
wpa_supplicant.profile.1.network.1.psk=verysecretphrase
wpa_supplicant.profile.1.network.1.ssid=DEFAULT1
wpa_supplicant.profile.1.status=disabled
wpa_supplicant.profile.2.ap_scan=enabled
wpa_supplicant.profile.2.eapol_version=1
wpa_supplicant.profile.2.fast_reauth=enabled
wpa_supplicant.profile.2.name=WPA-sup-ath1
wpa_supplicant.profile.2.network.1.group.1.name=TKIP
wpa_supplicant.profile.2.network.1.key_mgmt.1.name=WPA-PSK
wpa_supplicant.profile.2.network.1.pairwise.1.name=TKIP
wpa_supplicant.profile.2.network.1.proto.1.name=RSN
wpa_supplicant.profile.2.network.1.psk=verysecretphrase
wpa_supplicant.profile.2.network.1.ssid=DEFAULT2
wpa_supplicant.profile.2.status=disabled
wpa_supplicant.status=disabled
wpa_supplicant.wait_for_interface=enabled
```

8.0 Glossary

Symbols

802.11: 802.11 is a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). The original specification provides for an Ethernet Media Access Controller (MAC) and several physical layer (PHY) options, the most popular of which uses GFSK modulation at 2.4GHz, enabling data rates of 1 or 2Mbps. Since its inception, two major PHY enhancements have been adopted and become "industry standards".

802.11b adds CCK modulation enabling data rates of up to 11Mbps, 802.11g supports data rates of up to 54Mbps in the same frequency band, and 802.11a specifies OFDM modulation and the same 54Mbps in the 5GHz frequency band.

A

AAA: Authentication, Authorization and Accounting. A method for transmitting roaming access requests in the form of user credentials (typically user@domain and password), service authorization, and session accounting details between devices and networks in a real-time manner.

authentication: The process of establishing the identity of another unit (client, user, device) prior to exchanging sensitive information.

B

backbone: The primary connectivity mechanism of a hierarchical distributed system. All systems, which have connectivity to an intermediate system on the backbone, are assured of connectivity to each other. This does not prevent systems from setting up private arrangements with each other to bypass the backbone for reasons of cost, performance, or security.

Bandwidth: Technically, the difference, in Hertz (Hz), between the highest and lowest frequencies of a transmission channel. However, as typically used, the amount of data that can be sent through a given communications circuit. For example, typical Ethernet has a bandwidth of 100Mbps.

bps: bits per second. A measure of the data transmission rate.

D

DHCP: Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organization's network. Using the Internet Protocol, each machine that can connect to the Internet needs a unique IP address. When an organization sets up its computer users with a connection to the Internet, IP address must be assigned to each machine. Without DHCP, the IP address must be entered manually at each computer and, if computers move to another location in another part of the network, a new IP address must be entered. DHCP lets a network administrator supervise and distribute IP addresses from a central point and automatically sends a new IP address when a computer is plugged into a different place in the network.

DNS: Domain Name Service. An Internet service that translates a domain name such as waveteq.com to an IP address, in the form xx.xx.xx.xx, where xx is an 8 bit hexadecimal number.

E

EAP: Extensible Authentication Protocol. Defined in [\[RFC2284\]](#) and used by IEEE 802.1x Port Based Authentication Protocol [8021x] that provides additional authentication methods. EAP-TLS (Transport Level Security) [\[RFC2716/RFC3546\]](#) provides for mutual authentication, integrity-protected ciphersuite negotiation and key exchange between two endpoints [\[RFC2716\]](#). EAP-TTLS (Tunnelled TLS Authentication Protocol)

provides an authentication negotiation enhancement to TLS (see Internet-Draft <draft-ietf-pppext-eap-ttls-05.txt>).

ERP: Extended Rate PHY. The 802.11g enhancement to the Physical Layer definition that introduces OFDM as a mandatory coding scheme for mandatory 6, 12 & 24Mbps bit rates and 18, 36, 48 & 54Mbps optional bit rates. The ERP retains backward compatibility with 802.11b coding and modulation mechanisms.

G

gateway: A gateway is a network point that acts as an entrance to another network. On the Internet, a node or stopping point can be either a gateway node or a host (end-point) node. Both the computers of Internet users and the computers that serve pages to users are host nodes. The computers that control traffic within your company's network or at your local Internet service provider (ISP) are gateway nodes.

H

hotspot: A hotspot is wireless public access system that allows subscribers to be connected to a wireless network in order to access the Internet or other devices, such as printers. Hot-spots are created by WLAN access points, installed in public venues. Common locations for public access are hotels, airport lounges, railway stations or coffee shops.

hotspot operator: An entity that operates a facility consisting of a Wi-Fi public access network and participates in the authentication.

HTTP: The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. Relative to the TCP/IP suite of protocols (which are the basis for information exchange on the Internet), HTTP is an application protocol.

HTTPS: HTTPS (Hypertext Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a Web protocol developed by Netscape and built into its browser that encrypts and decrypts user page requests as well as the pages that are returned by the Web server. HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sub-layer under its regular HTTP application layering.

I

ICMP: ICMP (Internet Control Message Protocol) is a message control and error-reporting protocol between a host server and a gateway to the Internet. ICMP uses Internet Protocol (IP) datagrams, but the messages are processed by the IP software and are not directly apparent to the application user.

IEEE: Institute of Electrical and Electronics Engineers. The IEEE describes itself as the world's largest professional society. The IEEE fosters the development of standards that often become national and international standards, such as 802.11.

IP: The Internet Protocol (IP) is the method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the packet directly to the computer whose address is specified.

IPsec: IPsec (Internet Protocol Security) is a developing standard for security at the network or packet processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPsec will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network routers.

IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

ISP: An ISP (Internet Service Provider) is a company that provides individuals and other companies' access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

L

LAN: A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for

example, in a home network) or many as thousands of users (for example, in an FDDI network).

M

MAC: Medium Access Control. In a WLAN network card, the MAC is the radio controller protocol. It corresponds to the ISO Network Model's level 2 Data Link layer. The IEEE 802.11 standard specifies the MAC protocol for medium sharing, packet formatting and addressing, and error detection.

N

NAT: NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses.

NAT is included as part of a router and is often part of a corporate firewall.

P

POP3: POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail. POP3 is built into the Netmanage suite of Internet products and one of the most popular e-mail products, Eudora. It's also built into the Netscape and Microsoft Internet Explorer browsers.

PPTP: Point-to-Point Tunnelling Protocol (PPTP) is a protocol (set of communication rules) that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a

single large local area network. This kind of interconnection is known as a virtual private network (VPN).

R

RADIUS: RADIUS (Remote Authentication Dial-In User Service) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics.

S

SNMP: Simple Network Management Protocol (SNMP) is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks.

SNMP is described formally in the Internet Engineering Task Force (IETF) Request for Comment (RFC) 1157 and in a number of other related RFCs.

SSL: The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

T

TCP: TCP (Transmission Control Protocol) is a set of rules (protocol) used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the individual units of data (called packets) that a message is divided into for efficient routing through the Internet.

TCP is a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end. In the Open Systems Interconnection (OSI) communication model, TCP is in layer 4, the Transport Layer.

TCP/IP: TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination.

W

WAN: A wide area network (WAN) is a geographically dispersed telecommunications

network. The term distinguishes a broader telecommunication structure from a local area network (LAN). A wide area network may be privately owned or rented, but the term usually connotes the inclusion of public (shared user) networks. An intermediate form

of network in terms of geography is a metropolitan area network (MAN).

9.0 Index

A

AAA, 72, 77
antenna diversity, 63
ath0, 5
ath1, 5
autolock WLAN, 68

B

bandwidth control, 119
bridge, 48
bridging firewall, 107
 match extensions
 802.3, 109
 ARP, 109
 IP, 110
 MARK, 111
 packet type, 111
 STP, 111
 VLAN, 113
 rule matches, 108
 rules configuration, 107
 target extensions
 arpnat, 115
 arpreply, 108, 113
 dnat, 114
 macvlan, 115
 mark, 114
 redirect, 114
 snat, 115
 watcher extensions
 LOG, 113

C

CCMP, 86, 90
channel, 62
 802.11a, 131
 802.11b/g, 130
CLI
 access, 15
 introduction, 15
CLI commands
 authcheck, 16
 passwd, 16
 quit, 18
 reboot, 18
 reset, 18

 shell, 17
 show, 17
 status, 17
configuration file, 44
configuration key
 aaa, 77
 acct, 82
 auth, 81
 domain, 83
 nas, 80
 radius.proxy, 86
 security
 wep, 84
 wpa, 85
access, 117
autolock, 68
bandwidth, 119
bridge, 48
date, 124
dhcpc, 50
dhcpcd, 50
dhcp-fwd, 51
dnsmasq, 53
ebtables, 107
firewall, 96
httpd, 121
ipsec, 56
netconf, 45
ntpd, 125
pppoe, 60
racoona, 58
radio, 61
resolv, 52
route, 73
snmpd, 122
ssid, 72
sshd, 121
statsd, 124
sysconf.trace, 126
sysctl, 128
syslog, 126
tunnel, 59
ulogd, 127
vlan, 54
vssid, 69
wacl, 71
wds, 70
wireless, 65

- wpasupplicant, 88
- connection
 - command line, 15
 - Ethernet, 10
 - wireless LAN, 12
- Conventions, xi
- country codes, 139

D

- DHCP, 50
 - client, 50
 - relay, 51
 - server, 50
- DNS, 52
- DNS forwarder, 53
- DNSMASQ, 53
- domains (WISPs), 83
- dynamic VLAN, 81

E

- EAP, 88
- Ethernet Cable
 - Assembly, 7

F

- firewall
 - bridging, 107
 - IP, 96
- Fresnel Zone, 6

G

- Graphical User Interface (GUI), 19
- GRE tunnels, 59

H

- half and quarter rates, 64
- half duplex, 47
- HTTP(S) Server, 121

I

- Installation, 6
- IP firewall, 96
 - IPP2P, 101
 - rule matches, 98
 - explicit, 99
 - ICMP, 99
 - implicit, 98

- rule targets, 102
 - accept, 102
 - DNAT target, 102
 - DROP, 103
 - LOG, 103
 - MARK, 103
 - MASQUERADE, 103
 - NAS_MARK, 105
 - QUEUE, 103
 - REDIRECT, 103
 - REJECT, 104
 - RETURN, 104
 - SNAT, 104
 - TOS, 104
 - TTL, 104
 - ULOG, 105
- rules, 97
- IP logging, 127
- IPsec, 56
- IPsec Racoon, 58
- ISO country codes, 139
- ixp0, 5
- ixp1, 5

L

- licensing, 13, 36
- Line of Sight (LoS), 6
- login, 15

M

- manual clock regulation, 124
- mounting, 6

N

- NAS (Network Access Server), 80
- netconf, 45
- network configuration, 77
- network usage statistics, 124
- NTP client, 125

P

- P2P, 101
- PPoE injector, 8
- PPPoE, 60
- product overview, 1
- protocols, 136

Q

QoS, 54, 67

R

RADIUS

- accounting servers, 82
- authentication servers, 81
- domains (WISPs), 83
- proxy, 86
- standard attributes, 132
- VSA, 134

regulatory domain, 130

RSN, 90

RX antenna, 63

S

selective source routing, 75

SMTP redirection, 116

SNMP, 42

SNMP agent, 122

source routing, 74

SSH, 121

SSH Server, 121

SSID broadcasting, 66

static bandwidth control, 119

static routing, 73

static supervision, 72

STP, 48

support, xi

sysctl plugin, 128

syslog, 126

system services, 124

T

threshold, 63

throughput enhancement

- compression, 67
- fast frame (FF), 67
- frameburst, 67

TKIP, 86

trace system, 126

tunnels

- GRE, 59
- IPsec, 56
- IPsec IKE daemon (racoon), 58

TX antenna, 64

V

VLAN, 54

- dynamic, 81

VSSID, 69

W

WDS, 70

weather-proofing, 141, 151

web interface, 19

- configuration, 25

- advanced network, 30

- basic network, 27

- basic wireless, 28

- expert, 32

- starting point, 25

- wireless security, 31

- logout, 41

- statistics, 19, 20

- ARP tables, 24

- network statistics, 22

- routes, 24

- system information, 21

- wireless details, 23

- system, 33

- license, 36

- maintenance, 33

- password, 34

- remote management, 35

- tools, 37

- antenna alignment, 38

- site survey, 37

- wireless tests, 39

WEP keys, 66

white/black list, 117

wireless ACL, 71

wireless client bridge, 71

wireless interface, 65

wireless radio, 61

wireless security

- WEP (dynamic), 84

- WEP (static), 66

- WPA/WPA2, 85

WISP domains, 83

WPA, 85, 90

WPA/802.1x supplicant, 88

WPA2, 90

10.0 Customer Support

For any problems with the ShadowMaster please contact the Waveteq main office at the contact information below.

Waveteq Communications Inc.

#222 – 3121 Hill Rd.

Lake Country, BC, Canada

V4V 1G1

Toll Free: 1-888-Waveteq(928-3837)

Phone: (250) 766-9229

Email: support@waveteq.com