Avocet 250:- PTPA Series

User Manual

Version 3.0 (17th January 2013)

Avocet 250

2x2 MIMO Point-to-Point

300Mbp/s link rate with 250Mbp/s real duplex throughput

Models: PTPA-5G-18, PTPA-5G-23 and PTPA-5G-C

Contents

1.0 General

The Avocet 250 (PTPA series) is a family of high capacity point-to-point systems for backhaul applications.

The user interface on the Avocet is designed with focus on simplicity and speed, and does not provide many selectable and advanced options, as the most favorable settings is applied automatically. This allows operators to setup high capacity systems with less effort and expertise than comparable alternatives.

All wireless links in the Avocet operate fully adaptive, and will provide link rate depending on link quality and capacity needed. This provides a more flexible application than traditional microwave PtP backhaul systems.

1.1 Terminology

Base Station are those devices configured in ***AP Mode***.

CPE Units are those devices configured in ***Station Mode***.

1.2 Default settings

IP address: *192.168.1.10/24*

Username: *admin*

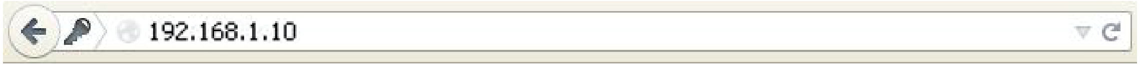
Password: *admin*

2.0 Administration

Avocet system administration is mainly done via a web browser, but may also be managed trough CLI (not shell) via SSH and Telnet.

2.1 Accessing Web Browser Interface

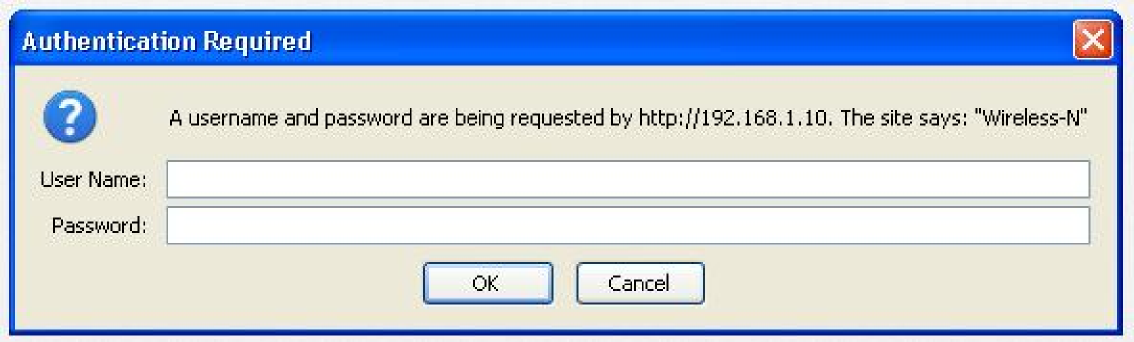
Using an up to date web browser (Chrome, Firefox or Opera recommended. Microsoft Internet Explorer is incompatible with open standard Canvas functions used in the user interface) enter the default IP Address into the browsers address bar, as shown.



192.168.1.10

You will then be prompted to enter the administrators' username and password. Unless you have updated the admin password use the default username and password.

Enter username and password:



Authentication Required

A username and password are being requested by http://192.168.1.10. The site says: "Wireless-N"

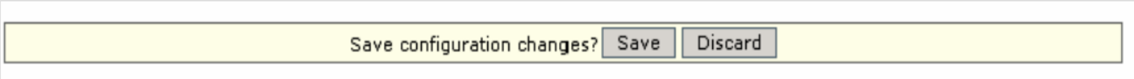
User Name:

Password:

3.0 Web Browser Administration

3.1 Saving changes

After making changes from each respective setup page or applying changes, a prompt will appear and ask you to confirm if you want to save the change permanently to device flash.



Save configuration changes?

Save will write all configuration changes to the device flash.
Discard will discard all changes made.

If you are not sure what changes were made earlier, then it is advised to discard and reconfigure again.

3.2 Menu Structure

3.2.1 Menu Structure: Base Station

The user menu consists of 8 main areas:

STATUS	read-only overview information on unit status
CLIENTS	for monitoring and management of connected stations
WLAN	for the management of the wireless interface
NETWORK	for the management of the networking configuration
ADVANCED	for advanced settings of the wireless configuration
ROUTING	for advanced networking settings in router mode
VLAN	for VLAN configuration (VLAN switching or VLAN management)
SERVICES	for specifying the management and system services
SYSTEM	for managing the radio system settings and upgrades

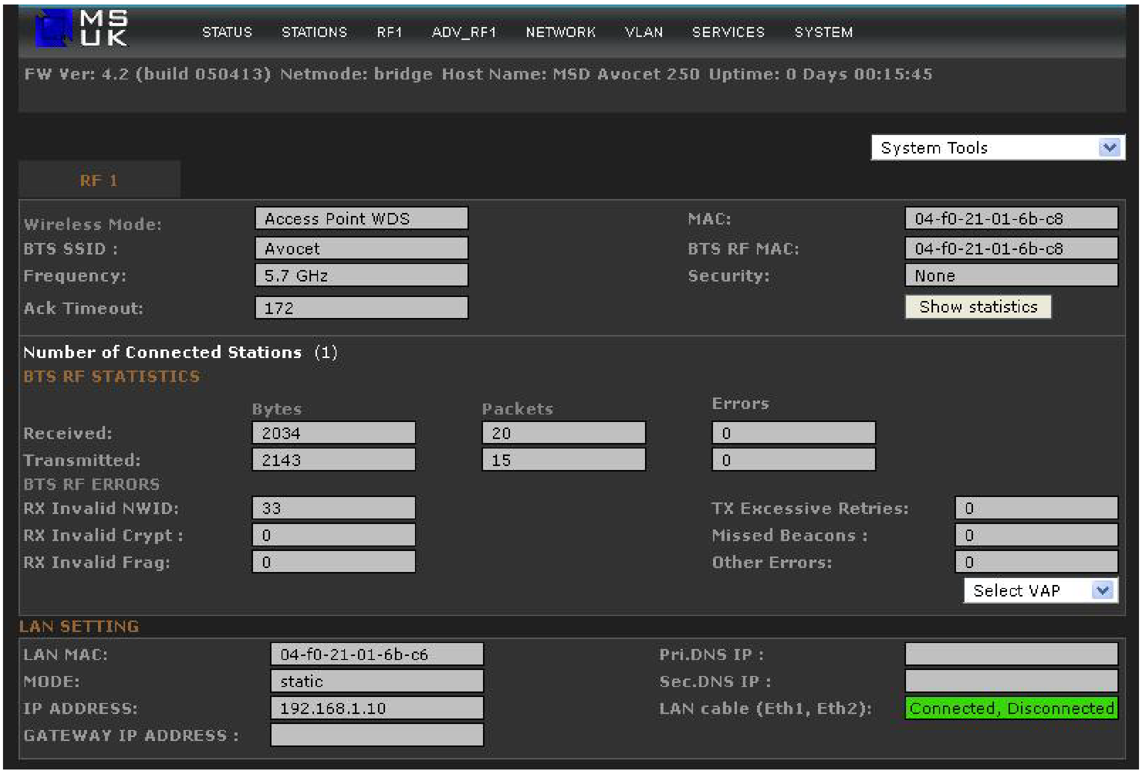
3.2.2 Menu Structure: CPE Unit

The user menu consists of 7 main areas:

STATUS	read-only overview information on unit status
WLAN	for the management of the wireless interface
NETWORK	for the management of the networking configuration
ADVANCED	for advanced settings of the wireless configuration
ROUTING	for advanced networking settings in router mode
VLAN	for VLAN configuration (VLAN switching or VLAN management)
SERVICES	for specifying the management and system services
SYSTEM	for managing the radio system settings and upgrades

3.3 STATUS Menu

3.3.1 STATUS: Base Station



FW Ver: 4.2 (build 050413) Netmode: bridge Host Name: MSD Avocet 250 Uptime: 0 Days 00:15:45

Wireless Mode:	Access Point WDS	MAC:	04-f0-21-01-6b-c8
BTS SSID :	Avocet	BTS RF MAC:	04-f0-21-01-6b-c8
Frequency:	5.7 GHz	Security:	None
Ack Timeout:	172		

Number of Connected Stations (1)

BTS RF STATISTICS

	Bytes	Packets	Errors
Received:	2034	20	0
Transmitted:	2143	15	0

BTS RF ERRORS

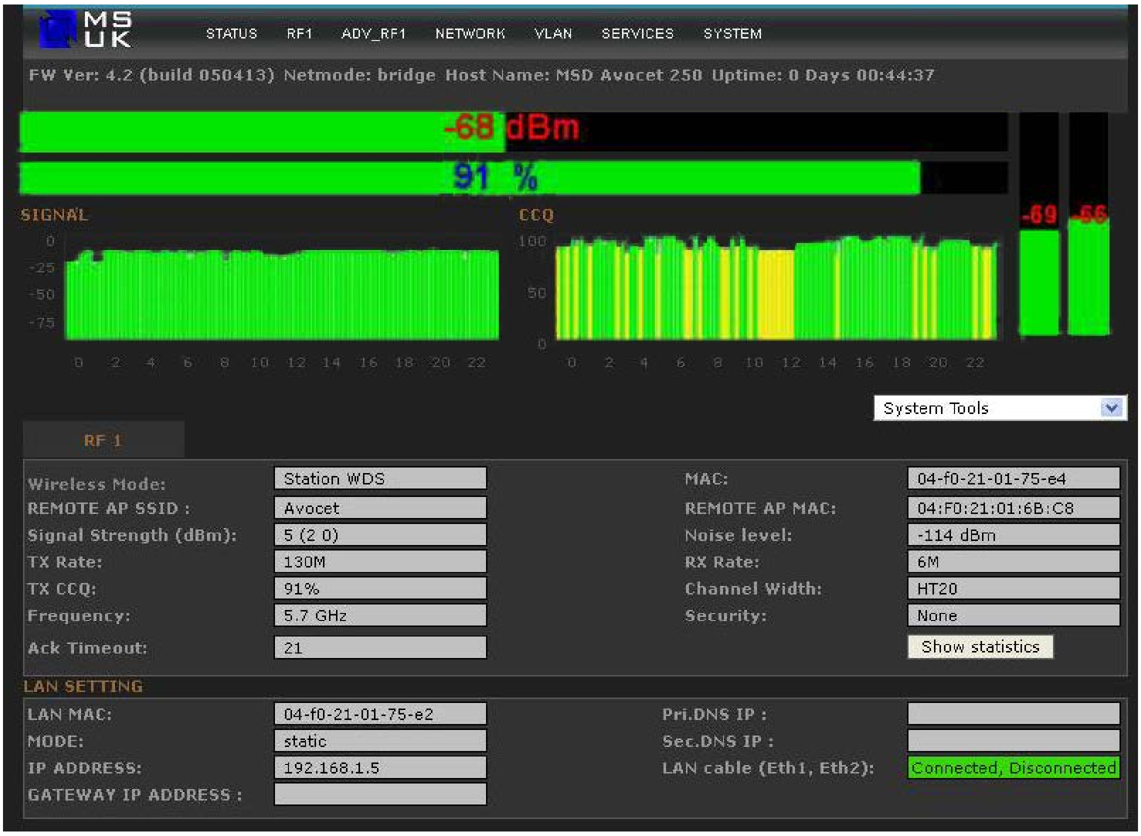
RX Invalid NWID:	33	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

LAN SETTING

LAN MAC:	04-f0-21-01-6b-c6	Pri.DNS IP :	
MODE:	static	Sec.DNS IP :	
IP ADDRESS:	192.168.1.10	LAN cable (Eth1, Eth2):	Connected, Disconnected
GATEWAY IP ADDRESS :			

The STATUS Menu for the Base Station is slightly different to that of the CPE Unit as the CPE Unit shows additional signal level information. The STATUS Menu is read-only information, and the same window that a Guest-user may be granted access to. The info-bar, just below the menu-bar, shows the running Firmware version, the Network Mode, the Host Name and Uptime.

3.3.2 STATUS: CPE Unit



FW Ver: 4.2 (build 050413) Netmode: bridge Host Name: MSD Avocet 250 Uptime: 0 Days 00:44:37

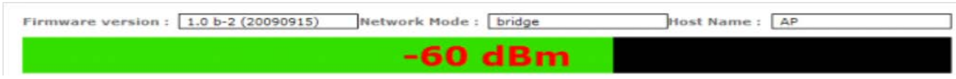
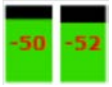
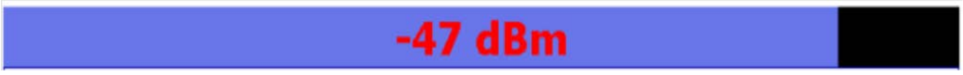
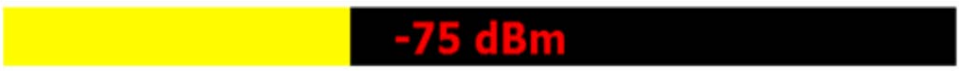
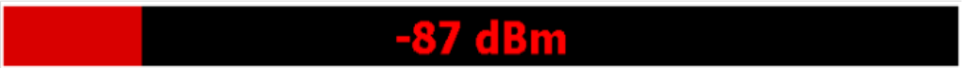
Wireless Mode:	Station WDS	MAC:	04-f0-21-01-75-e4
REMOTE AP SSID :	Avocet	REMOTE AP MAC:	04:F0:21:01:6B:C8
Signal Strength (dBm):	5 (2 0)	Noise level:	-114 dBm
TX Rate:	130M	RX Rate:	6M
TX CCQ:	91%	Channel Width:	HT20
Frequency:	5.7 GHz	Security:	None
Ack Timeout:	21		

LAN SETTING

LAN MAC:	04-f0-21-01-75-e2	Pri.DNS IP :	
MODE:	static	Sec.DNS IP :	
IP ADDRESS:	192.168.1.5	LAN cable (Eth1, Eth2):	Connected, Disconnected
GATEWAY IP ADDRESS :			

While sharing the same information as the Base Station the CPE Unit also has the received signal level in dBm, the Tx CCQ (Client Connection Quality) in % and the individual Rx levels for the two MIMO chains (Chain0 and Chain1) in dBm.

The Signal Level has quick indication by color, where **green color** indicates good signal, **yellow color** indicates low signal and **red color** indicates bad signal. **Blue color** indicates too high signal. The ideal signal level is considered to be -55 to -65 dBm for full speed.

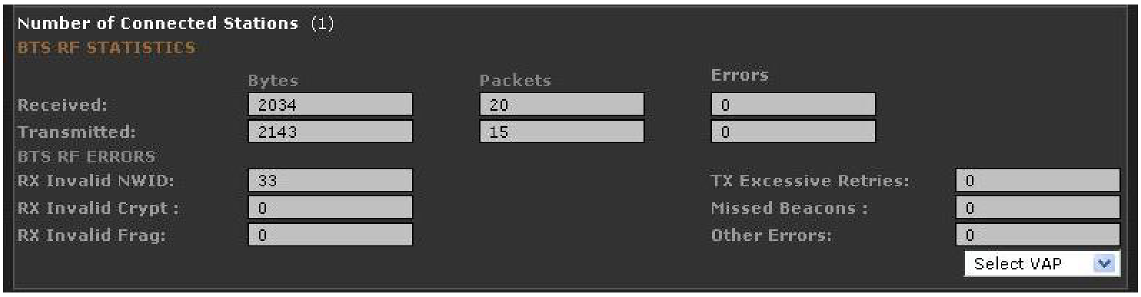
Overall received signal level	L / R Chain
 Firmware version : 1.0 b-2 (20090915) Network Mode : bridge Host Name : AP -60 dBm	 -50 -52
 -47 dBm	
 -75 dBm	
 -87 dBm	

Below the Signal Bar there is presented a Signal History and CCQ graph to easily monitor the RX signal for the last 24 hours. The color coding on the Signal History follows the same color scheme as the Signal Bar.

3.3.3 STATUS: Status Fields

Wireless Mode	The wireless mode the unit runs: AP, AP with WDS, Repeater, Station or Station WDS
Remote AP SSID	The SSID the unit is using or are connected to
Local/Remote AP MAC	MAC address on BTS WLAN or what MAC address the Client is connected to
Signal Strength	Client only (Station/Station WDS) – received signal strength and Ch0/Ch1 levels.
TX CCQ	Client Connection Quality in percentage for successful Tx frames transmitted
Noise Level	Received Noise level
TX Rate (Mbp/s)	Connected TX speed over the air – air rate
RX Rate (Mbp/s)	Connected RX speed over the air – air rate
Channel Width (MHz)	Operating Channel and mode; 5, 10, 20 or 20/40 MHz. HT indicates MIMO.
Frequency (MHz)	Operating frequency
Ack Timeout	Current setting for range calculations – in use
Security	Wireless Security Mode; WEP, WPA, WPA2, IEEE802.1X or None

All data status fields are dynamic, and further details/statistics are available by clicking on the ***Show statistics*** button:



Number of Connected Stations (1)

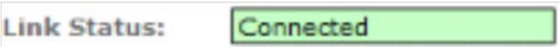
BTS RF STATISTICS

	Bytes	Packets	Errors
Received:	2034	20	0
Transmitted:	2143	15	0

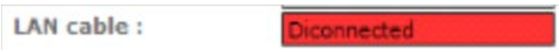
BTS RF ERRORS

RX Invalid NWID:	33	TX Excessive Retries:	0
RX Invalid Crypt :	0	Missed Beacons :	0
RX Invalid Frag:	0	Other Errors:	0

Status of the Ethernet LAN cable will show either Connected or Disconnected:



Link Status: Connected



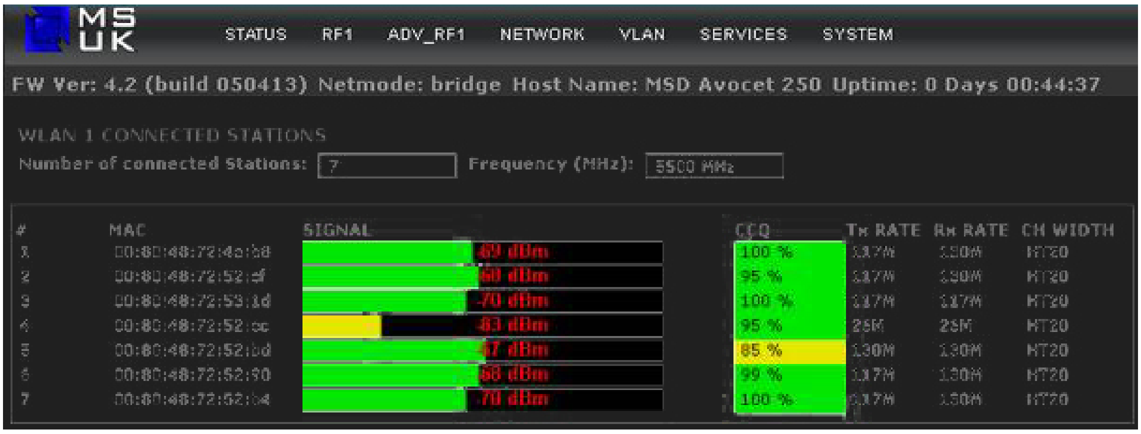
LAN cable : Diconnected

All the other menus are input menus and are only accessible through the Admin login (not by the Guest login).

The system management is based on “on the fly configuration” without need for rebooting the radio unit.

3.4 CLIENTS Menu

The CLIENT menu is only available for devices configured as a Base Station (AP Mode) only and allows the user to monitor the connected Stations for signal level and link-rates and what Station runs MIMO or legacy mode:



FW Ver: 4.2 (build 050413) Netmode: bridge Host Name: MSD Avocet 250 Uptime: 0 Days 00:44:37

WLAN 1 CONNECTED STATIONS

Number of connected Stations: 7 Frequency (MHz): 5500 MHz

#	MAC	SIGNAL	CCQ	Tx RATE	Rx RATE	CH WIDTH
1	00:80:48:72:4a:b8	-49 dBm	100 %	117M	130M	HT20
2	00:80:48:72:52:af	-60 dBm	95 %	117M	130M	HT20
3	00:80:48:72:53:1d	-70 dBm	100 %	117M	117M	HT20
4	00:80:48:72:52:cc	-83 dBm	95 %	26M	26M	HT20
5	00:80:48:72:52:bd	-67 dBm	85 %	130M	130M	HT20
6	00:80:48:72:52:90	-68 dBm	99 %	117M	130M	HT20
7	00:80:48:72:52:b4	-70 dBm	100 %	117M	130M	HT20

The color code thresholds for received signal from the Stations are set in the ADVANCED menu.

3.5 WLAN Menu

3.5.1 WLAN: Base Station

The WLAN menu provides basic wireless configuration and allows the user to set up the wireless interface:

Wireless Mode Access Point (with WDS), Station or Station WDS.

AP-ESSID Network name, where only Station units with same ESSID setting will connect to the AP unit.

Scan Scan button for performing a spectrum scan for available frequencies. Scanning frequencies are controlled by Frequency-list.

Wireless profile Informational only – the unit will operate in 802.11n mode 5GHz band

Channel Spectrum Width For selecting between 20/40MHz (Auto MIMO), 20MHz, 10MHz or 5MHz channel usage.

Guard Interval Short Guard Interval available only in 20/40 MHz and may provide higher throughput.

Channel Width The selectable frequency channels depending on regulatory domain. Channel survey button provides a spectrum scan on the selectable and available channels with RSSI parameters and also a recommended operating channel.

Spectrum Selection For selecting the regulatory frequencies. All use of SuperChannel frequencies is on user responsibilities.

Channel Frequency Manual selectable frequency – Auto must be deselected.

Frequency List Selectable set of frequencies to be used for automatic frequency (DFS) selection.

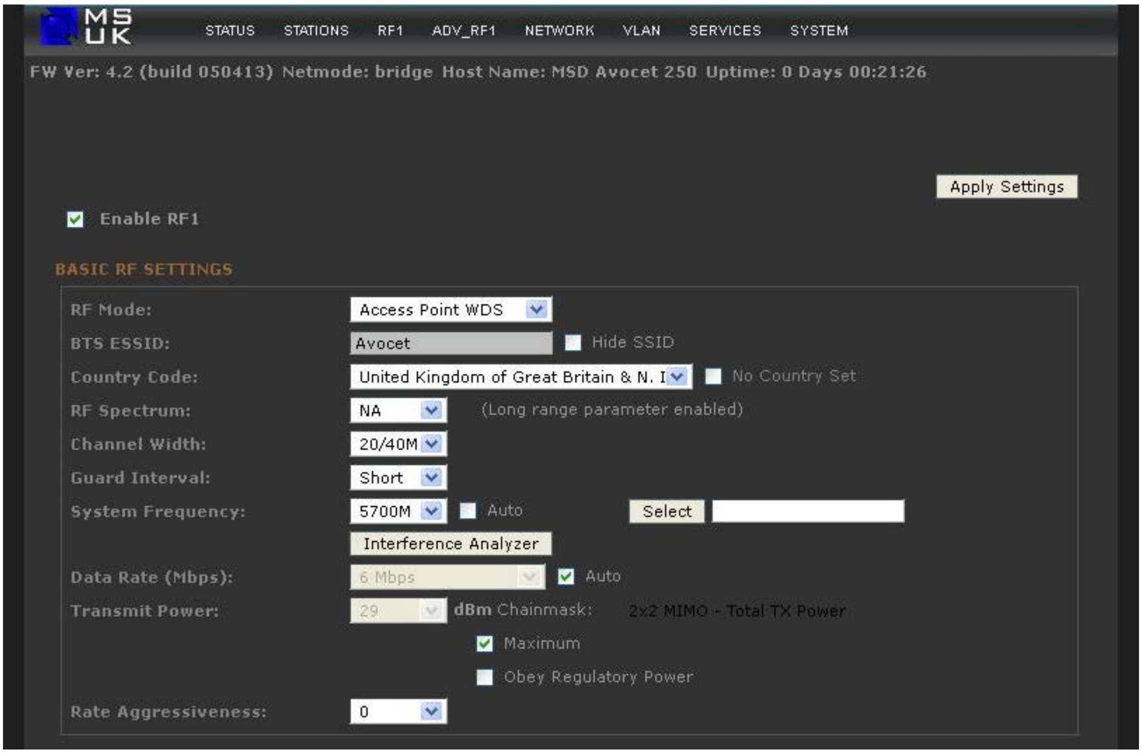
Transmit Power Allows the user to set TX power level (in dBm) or let it automatically comply with regulatory Domain settings.

Data Rate To select the modulation techniques – from 6 Mbps BPSK to 300 Mbps MCS15. Select Auto (recommended) for full link adaptation function.

Rate Aggressiveness Allows user to reduce or increase transmit rate while still remain in Fully Auto Algorithm. There are 2 scenarios that Rate Aggressiveness is useful. Environment might be noisy at times. Lower the throughput will ensure better stability. Rate Aggressiveness allows device to reduce the transmit rate, so range or power can be higher. Choose a range of value from -3,-2,-1. Environment might be free of interference. But the fully auto algorithm might give low throughput. Increase Rate Aggressiveness will increase transmit rate in this case to get higher throughput. Choose a range of value from +3, +2, +1.

Range/ACK Timeout Automatic range calculation. Deselect auto to enable manual settings.

Manual Range Manual enter the distant in meters the device is to connect with the opposite device. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.



FW Ver: 4.2 (build 050413) Netmode: bridge Host Name: MSD Avocet 250 Uptime: 0 Days 00:21:26

☑ Enable RF1

BASIC RF SETTINGS

RF Mode: Access Point WDS
BTS ESSID: Avocet ☐ Hide SSID
Country Code: United Kingdom of Great Britain & N. I ☐ No Country Set
RF Spectrum: NA (Long range parameter enabled)
Channel Width: 20/40M
Guard Interval: Short
System Frequency: 5700M ☐ Auto
Data Rate (Mbps): 6 Mbps ☑ Auto
Transmit Power: 29 dBm Chainmask: 2x2 MIMO - Total TX Power
☑ Maximum
☐ Obey Regulatory Power
Rate Aggressiveness: 0

NOTE/WARNING on regulatory compliance:
The responsibility for correct use of radio equipment i.a.w. local and national regulations lay solely on end user.

3.5.2 WLAN: CPE Unit

The WLAN menu provides basic wireless configuration and allows the user to set up the wireless interface:

Wireless Mode Station or Station WDS.

Remote AP-ESSID Network name, to specify what network the Station will connect to.

Site Survey For making a spectrum scan to see available Base Station units.

Wireless profile Selection between 802.11n modes 5GHz or 2.4GHz band.

Channel Spectrum Width For selecting between 20/40MHz (Auto MIMO), 20MHz, 10MHz or 5MHz channel usage.

Guard Interval Short Guard Interval available only in 20/40 MHz and may provide higher throughput.

Channel Width The selectable frequency channels depending on regulatory domain. Channel survey button provides a spectrum scan on the selectable and available channels with RSSI parameters and also a recommended operating channel.

Spectrum Selection For selecting the regulatory frequencies. All use of SuperChannel frequencies is on user responsibilities.

Channel Scan List Selectable set of frequencies to be used for automatic frequency selection.

Transmit Power Allows the user to set TX power level (in dBm) or let it automatically comply with regulatory Domain settings.

Data Rate To select the modulation techniques – from 6 Mbps BPSK to 300 Mbps MCS15. Select Auto (recommended) for full link adaptation function.

Rate Aggressiveness

Allows users to reduce or increase the transmit rate while still using the Auto Algorithm. There are 2 scenarios where changing Rate Aggressiveness is useful:

In locations with higher levels of background noise, lowering the throughput will ensure better stability. This is achieved by setting Rate Aggressiveness to a negative value. The more negative, the lower the throughput and the higher the chance of stability.

In situations free of interference, the Auto Algorithm may result in the unit running at lower rates. By increasing Rate Aggressiveness, this will make the algorithm select a higher transmit rate, in this case get higher throughputs. The higher the Rate Aggressiveness, the more it will tend select the highest rate.

Range / ACK Timeout

Automatic range calculation. Deselect auto to enable manual settings.

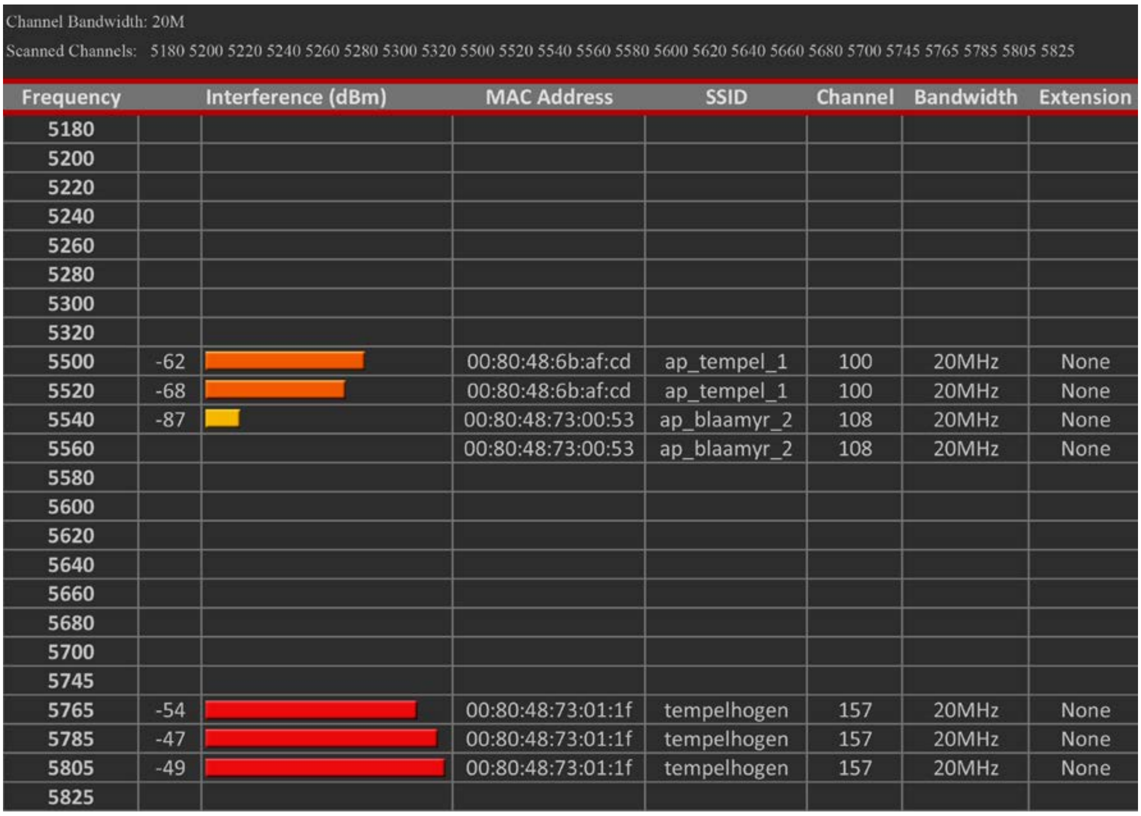
Manual Range

Manual enter the distant in meters the device is to connect with the opposite device. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.

NOTE / WARNING on regulatory compliance:
The responsibility for correct use of radio equipment in accordance with local and national regulations lay solely on end user.

3.5.3 Interference Analyzer

This feature can only be used on the Base Station unit (AP mode) and will list usage of frequencies within the selected scan-list:



Channel Bandwidth: 20M

Scanned Channels: 5180 5200 5220 5240 5260 5280 5300 5320 5500 5520 5540 5560 5580 5600 5620 5640 5660 5680 5700 5745 5765 5785 5805 5825

Frequency	Interference (dBm)	MAC Address	SSID	Channel	Bandwidth	Extension
5180						
5200						
5220						
5240						
5260						
5280						
5300						
5320						
5500	-62	00:80:48:6b:af:cd	ap_tempel_1	100	20MHz	None
5520	-68	00:80:48:6b:af:cd	ap_tempel_1	100	20MHz	None
5540	-87	00:80:48:73:00:53	ap_blaamyr_2	108	20MHz	None
5560		00:80:48:73:00:53	ap_blaamyr_2	108	20MHz	None
5580						
5600						
5620						
5640						
5660						
5680						
5700						
5745						
5765	-54	00:80:48:73:01:1f	tempelhogen	157	20MHz	None
5785	-47	00:80:48:73:01:1f	tempelhogen	157	20MHz	None
5805	-49	00:80:48:73:01:1f	tempelhogen	157	20MHz	None
5825						

Note: The Interference Analyzer will run for two minutes, and will recover your connection if it was accidently initiated on a remote site. Your selected frequency will be highlighted with grey.

3.5.4 Site Survey

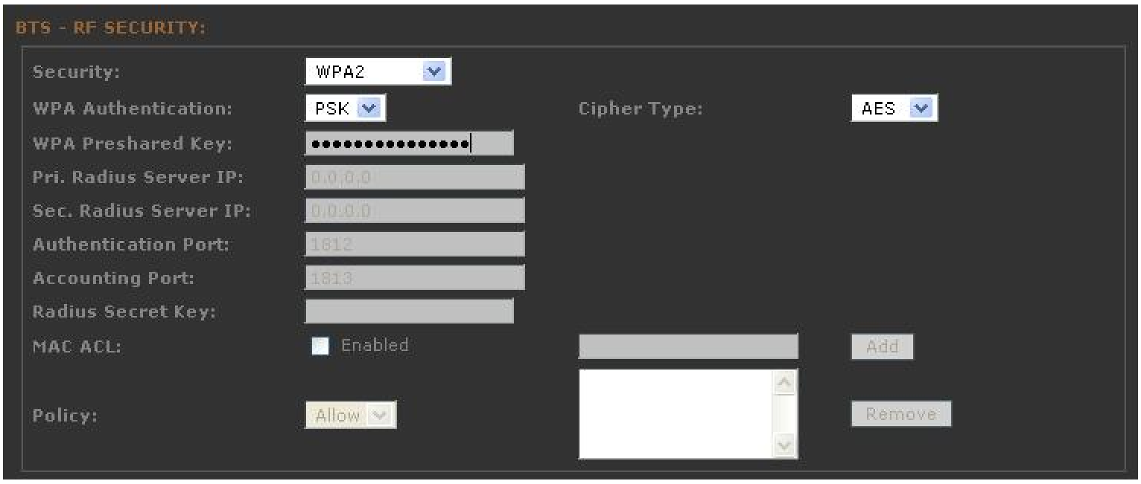
This feature can only be used on the CPE unit (Station mode) and will list all Base Stations seen within the given scan-list; connectivity to the station will not be lost during the scan.

3.5.5 Security Setup

WLAN security setup provides options to set the wireless security. The system supports both WEP and all WPA modes (with Auto WPA1/2) - including WPA2 personal/enterprise and 802.1X. It is not recommended to use WEP because of its known security issues and it is recommended to use AES over TKIP, due to legacy speed limitations of TKIP.

3.5.5.1 WPA-Personal (WPA2)

When ***WPA2*** profile is selected, you will be prompted for Key String Type of a 64 hex value or a Passphrase (between 8 to 63 characters):



BTS - RF SECURITY:

Security: WPA2

WPA Authentication: PSK

Cipher Type: AES

WPA Preshared Key: ••••••••••••••••

Pri. Radius Server IP: 0.0.0.0

Sec. Radius Server IP: 0.0.0.0

Authentication Port: 1812

Accounting Port: 1813

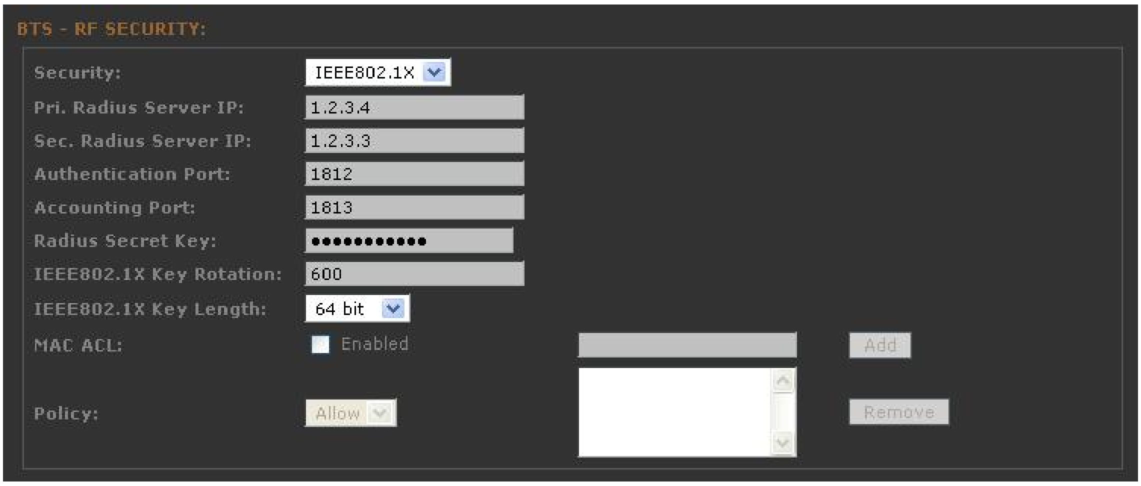
Radius Secret Key:

MAC ACL: ☑ Enabled

Policy: Allow

3.5.5.2 WPA-EAP (IEEE802.1X)

When ***IEEE802.1X*** profile is selected, you will be prompted for RADIUS Server settings (IP and Port numbers) and a Shared Secret:



BTS - RF SECURITY:

Security: IEEE802.1X

Pri. Radius Server IP: 1.2.3.4

Sec. Radius Server IP: 1.2.3.3

Authentication Port: 1812

Accounting Port: 1813

Radius Secret Key: ••••••••••••

IEEE802.1X Key Rotation: 600

IEEE802.1X Key Length: 64 bit

MAC ACL: □ Enabled

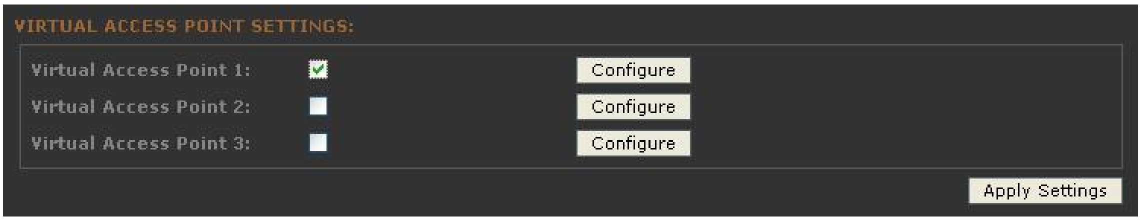
Policy: Allow

3.5.5.3 MAC ACL

This feature is for Base Station (AP Mode) configured devices only. It specifies which Policy to use ***Deny/Accept*** for any specified MAC-addresses.

3.5.5.4 Virtual Access Point

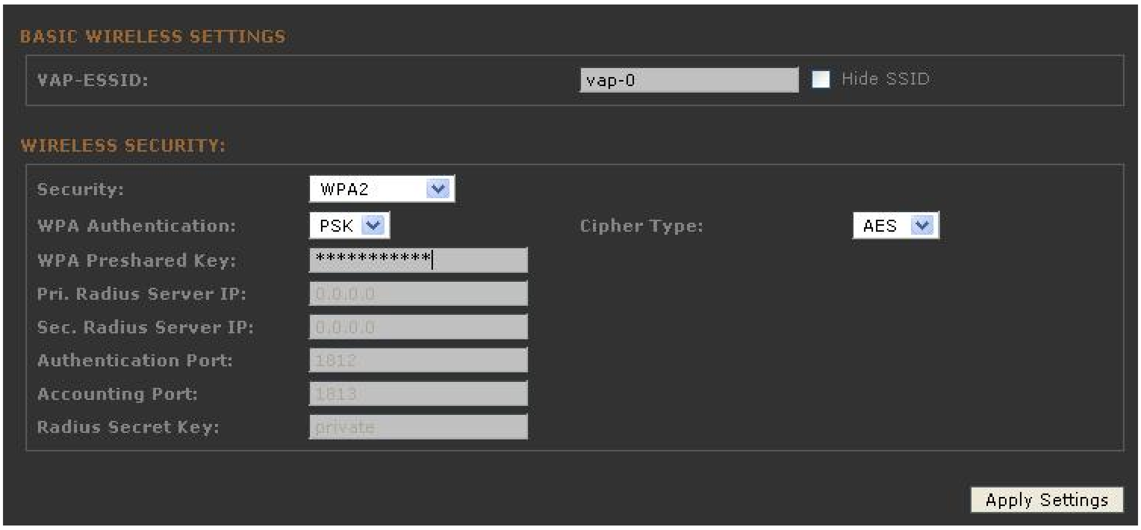
This feature is for Base Station (AP Mode) configured devices only. Up to 3 individual virtual access points may be defined:



VIRTUAL ACCESS POINT SETTINGS:

Virtual Access Point 1:	☑	Configure
Virtual Access Point 2:	□	Configure
Virtual Access Point 3:	□	Configure

With different SSIDs and Security Profiles:



BASIC WIRELESS SETTINGS

VAP-ESSID:	vap-0	□ Hide SSID

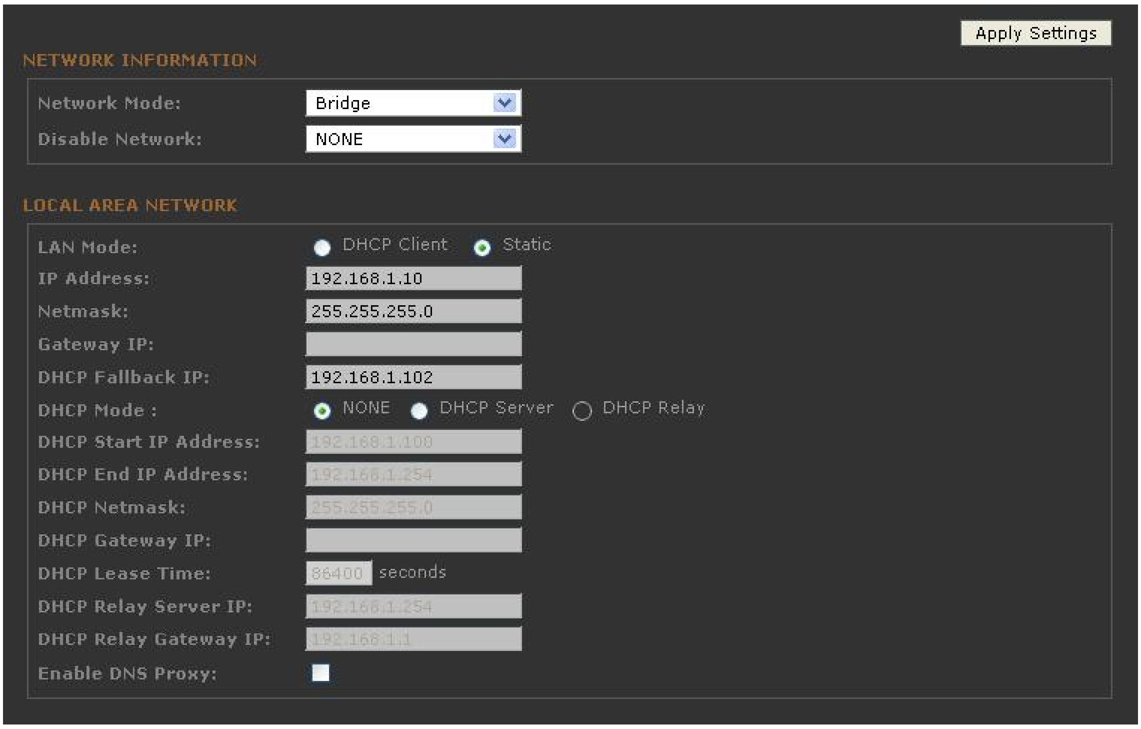
WIRELESS SECURITY:

Security:	WPA2		
WPA Authentication:	PSK	Cipher Type:	AES
WPA Preshared Key:	***********		
Pri. Radius Server IP:	0.0.0.0		
Sec. Radius Server IP:	0.0.0.0		
Authentication Port:	1812		
Accounting Port:	1813		
Radius Secret Key:	private		

3.6 NETWORK Menu

3.6.1 Basic Configuration

Network Mode for setting Bridge mode:



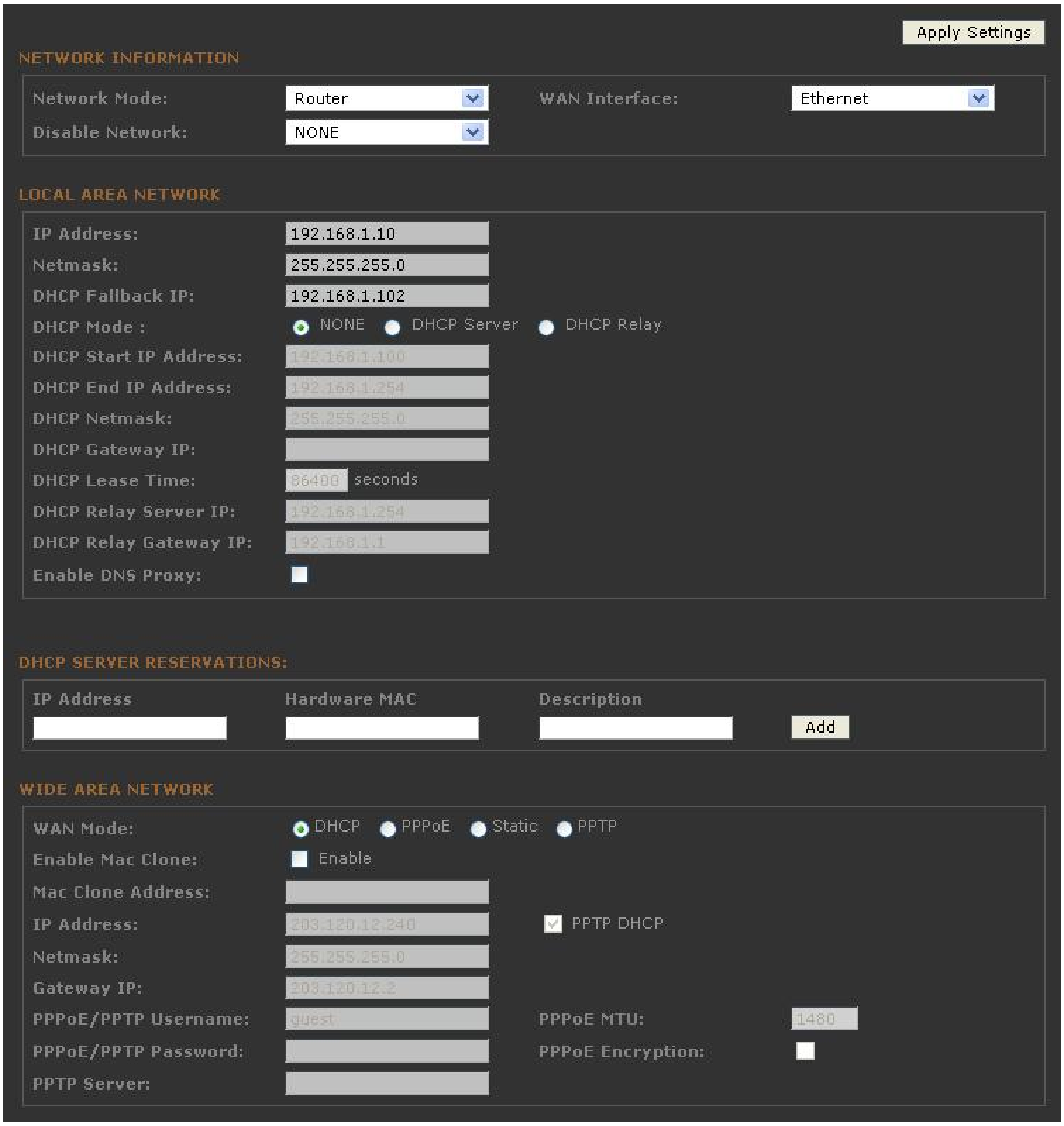
NETWORK INFORMATION

Network Mode:	Bridge
Disable Network:	NONE

LOCAL AREA NETWORK

LAN Mode:	○ DHCP Client ● Static
IP Address:	192.168.1.10
Netmask:	255.255.255.0
Gateway IP:	
DHCP Fallback IP:	192.168.1.102
DHCP Mode :	● NONE ○ DHCP Server ○ DHCP Relay
DHCP Start IP Address:	192.168.1.100
DHCP End IP Address:	192.168.1.254
DHCP Netmask:	255.255.255.0
DHCP Gateway IP:	
DHCP Lease Time:	86400 seconds
DHCP Relay Server IP:	192.168.1.254
DHCP Relay Gateway IP:	192.168.1.1
Enable DNS Proxy:	□

Or Router mode:



NETWORK INFORMATION

Network Mode: Router
WAN Interface: Ethernet
Disable Network: NONE

LOCAL AREA NETWORK

IP Address: 192.168.1.10
Netmask: 255.255.255.0
DHCP Fallback IP: 192.168.1.102
DHCP Mode : ● NONE ○ DHCP Server ○ DHCP Relay
DHCP Start IP Address: 192.168.1.100
DHCP End IP Address: 192.168.1.254
DHCP Netmask: 255.255.255.0
DHCP Gateway IP:
DHCP Lease Time: 86400 seconds
DHCP Relay Server IP: 192.168.1.254
DHCP Relay Gateway IP: 192.168.1.1
Enable DNS Proxy: □

DHCP SERVER RESERVATIONS:

IP Address	Hardware MAC	Description	
			Add

WIDE AREA NETWORK

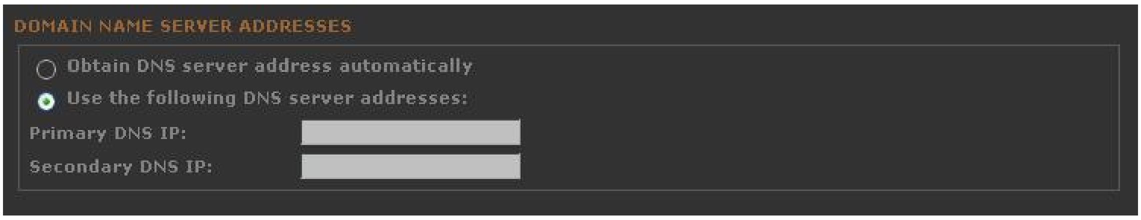
WAN Mode: ● DHCP ○ PPPoE ○ Static ○ PPTP
Enable Mac Clone: □ Enable
Mac Clone Address:
IP Address: 203.120.12.240 ☑ PPTP DHCP
Netmask: 255.255.255.0
Gateway IP: 203.120.12.2
PPPoE/PPTP Username: guest
PPPoE MTU: 1480
PPPoE/PPTP Password:
PPPoE Encryption: □
PPTP Server:

In router mode, the unit may operate as a real router – using static or dynamic (RIP) routing, or use NAT between the Wireless WAN interface and the Ethernet LAN interface – as typical for a WISP setup. The Wireless WAN interface can then use DHCP client or PPPoE to obtain an IP-address dynamically – or it can be set as a static address. Check NAT when the radio is to be used as gateway for customer network behind the CPE.

Note: When VLAN for management is enabled, the IP address is moved to the VLAN-interface, and the unit will not be accessible outside the VLAN. This is intentional, for providing system management security.

3.6.2 DNS Settings

The DNS can be obtained dynamically through DHCP or PPPoE – or be set manually. Check DNS Proxy if you want to use the radio for DNS forward look-up.



DOMAIN NAME SERVER ADDRESSES

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Primary DNS IP:

Secondary DNS IP:

3.7 ADVANCED WLAN Menu

The Advanced menu for wireless allows for more detailed and advanced system configuration on:

Long Range Parameters Allows the user to specify if long range or indoor is used in the ACK-timeout calculation. Indoor is suited for less than 150 meter range.

Long Range Parameters: Check to enable parameters.

Beacon Interval: (default is 100 ms) Define the time interval (in millisecond) the beacon to broadcast. Recommend to use default.

RTS Threshold: (Default is OFF)

Fragmentation Threshold: (Default is OFF)

Distance: Enter the distance in meters the device is to connect with the opposite device. Then click Calculate. The close approximate values for Slot Time, ACK Timeout, CTS Timeout will be calculated. Fine tuning can be further adjusted for the best environment conditions to achieve best performance and better link reliability.

Noise Immunity Adaptive Noise Immunity – a patented noise suppression algorithm implementation for dynamically fine-tuning of the Transceiver setting to conquer interference.

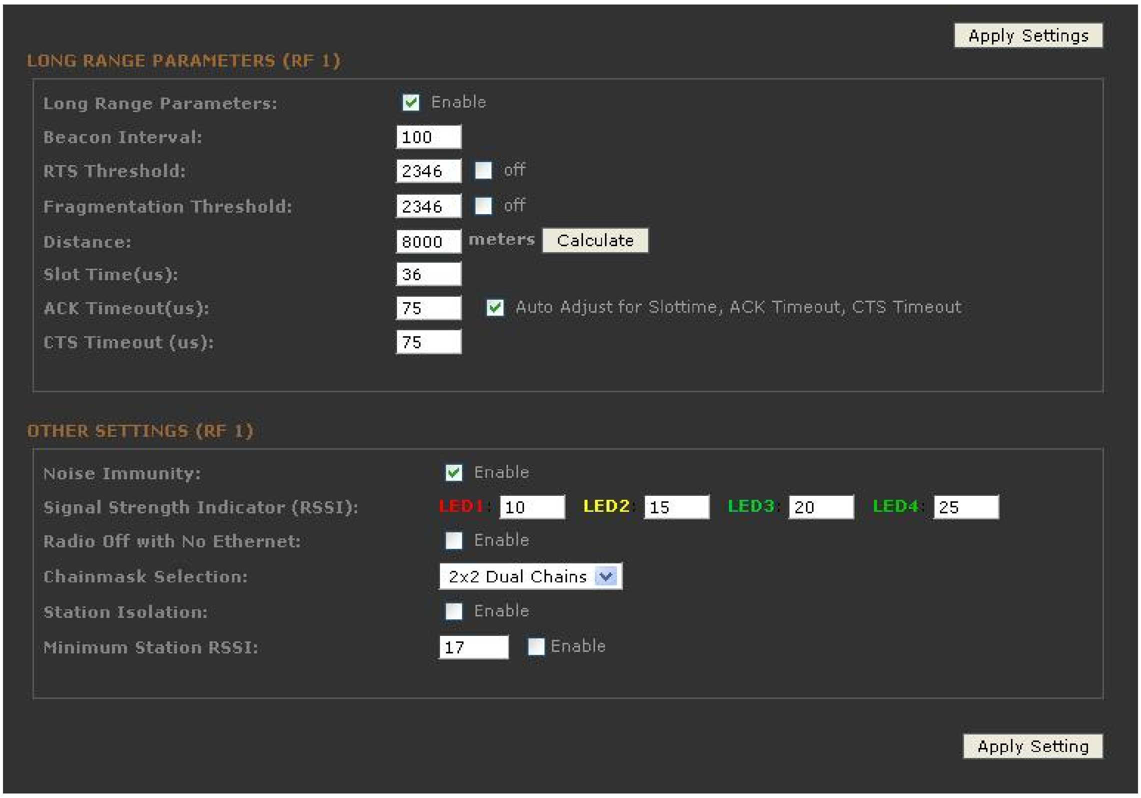
Signal Strength Indicator LED and Signal-bar control to set threshold levels.

Radio Off with no Ethernet Will disable the wireless interface if Ethernet has no link.

Chainmask Selection TX/RX MIMO chains. 2x2 Dual Chains means both polarities are selected. 1x1 Left Chain or 1x1 Right Chain selected means only one polarity is selected.

Stations Isolation Allows for stopping “Inter-client wireless traffic” if checked.

Minimum Station RSSI Set the minimum acceptable signal level from any Station. Value in RSSI may be converted to dBm by subtracting RSSI from 95 dBm.
i.e. 17 RSSI => 95dBm - 17 = 78 dBm.



Apply Settings

LONG RANGE PARAMETERS (RF 1)

Long Range Parameters:	☑ Enable
Beacon Interval:	100
RTS Threshold:	2346 □ off
Fragmentation Threshold:	2346 □ off
Distance:	8000 meters Calculate
Slot Time(us):	36
ACK Timeout(us):	75 ☑ Auto Adjust for Slottime, ACK Timeout, CTS Timeout
CTS Timeout (us):	75

OTHER SETTINGS (RF 1)

Noise Immunity:	☑ Enable
Signal Strength Indicator (RSSI):	LED1: 10 LED2: 15 LED3: 20 LED4: 25
Radio Off with No Ethernet:	□ Enable
Chainmask Selection:	2x2 Dual Chains
Station Isolation:	□ Enable
Minimum Station RSSI:	17 □ Enable

Apply Setting

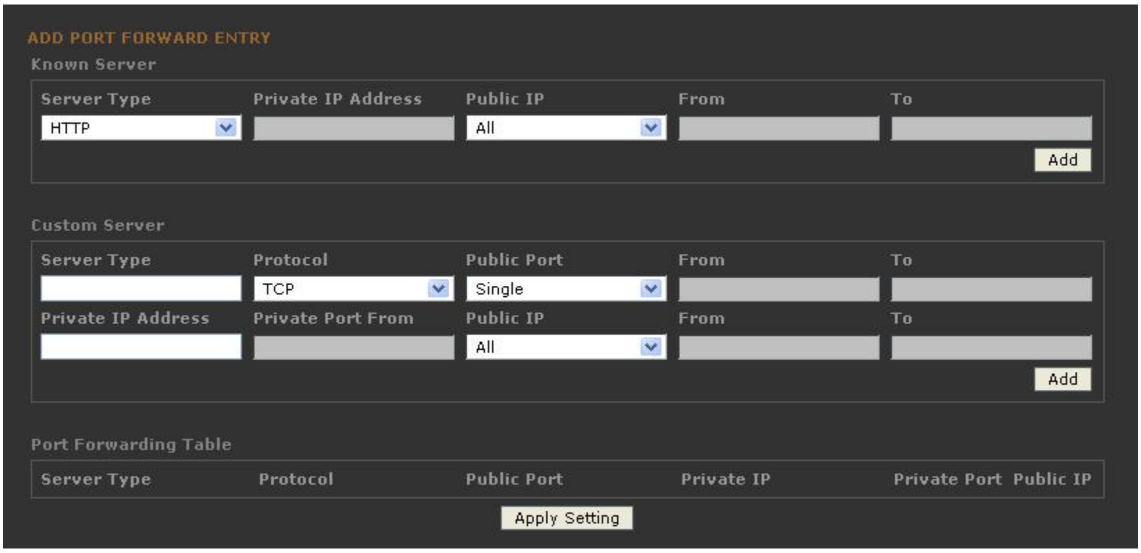
3.8 ADVANCED NETWORK Menu

This menu is only available in Router mode.

3.8.1 NAT Setup

Used to specify NAT and related port handling in Router/NAT mode.

Port forwarding can be specified for the most common services or a custom entry can be specified.



ADD PORT FORWARD ENTRY

Known Server

Server Type	Private IP Address	Public IP	From	To
HTTP		All		

Add

Custom Server

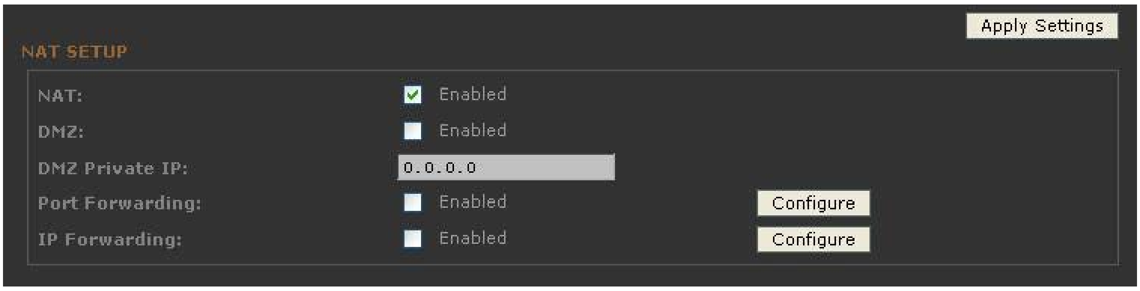
Server Type	Protocol	Public Port	From	To
	TCP	Single		
Private IP Address	Private Port From	Public IP	From	To
		All		

Add

Port Forwarding Table

Server Type	Protocol	Public Port	Private IP	Private Port	Public IP

Apply Setting



NAT SETUP

NAT: ☑ Enabled

DMZ: □ Enabled

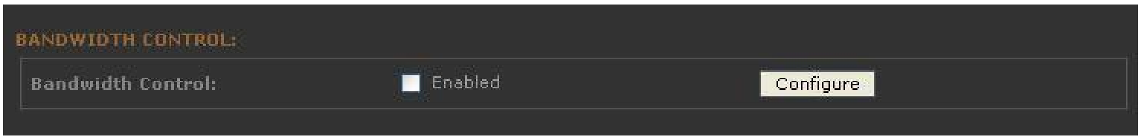
DMZ Private IP: 0.0.0.0

Port Forwarding: □ Enabled

IP Forwarding: □ Enabled

3.8.2 Bandwidth Control

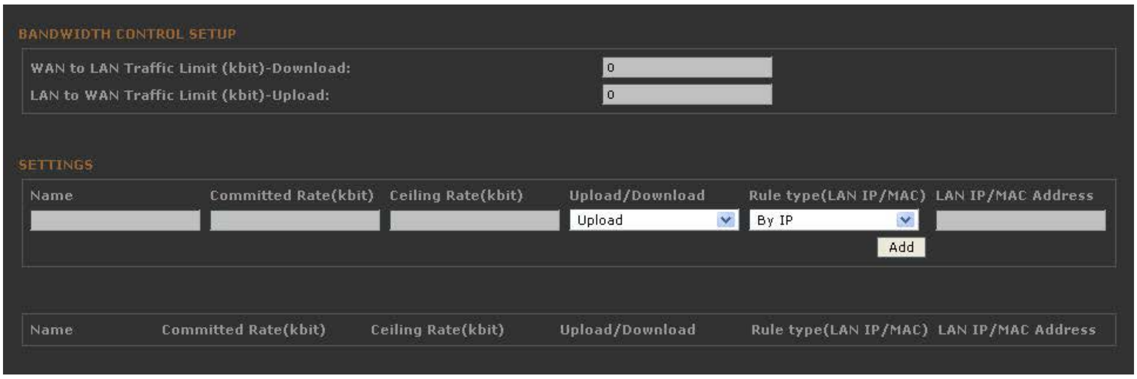
This allows a user to control maximum bandwidth or bandwidth by IP or MAC address.



BANDWIDTH CONTROL:

Bandwidth Control: □ Enabled

For Bridge mode, the bandwidth can be set by CIR/MIR and allocated by IP or MAC address:



BANDWIDTH CONTROL SETUP

WAN to LAN Traffic Limit (kbit)-Download: 0

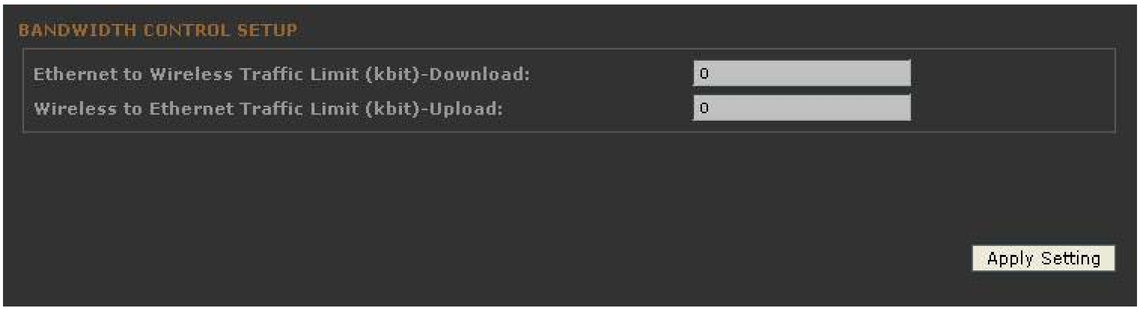
LAN to WAN Traffic Limit (kbit)-Upload: 0

SETTINGS

Name	Committed Rate(kbit)	Ceiling Rate(kbit)	Upload/Download	Rule type(LAN IP/MAC)	LAN IP/MAC Address
			Upload	By IP	

Name	Committed Rate(kbit)	Ceiling Rate(kbit)	Upload/Download	Rule type(LAN IP/MAC)	LAN IP/MAC Address

While in bridged mode, the total unit bandwidth can be specified (MIR/CIR):



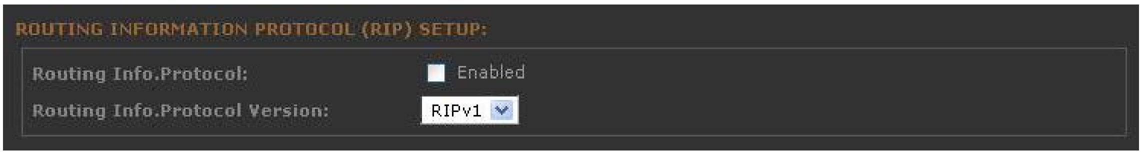
BANDWIDTH CONTROL SETUP

Ethernet to Wireless Traffic Limit (kbit)-Download: 0

Wireless to Ethernet Traffic Limit (kbit)-Upload: 0

3.8.3 RIP Routing

The unit supports RIPv1 and RIPv2 for dynamic exchange of routing information.



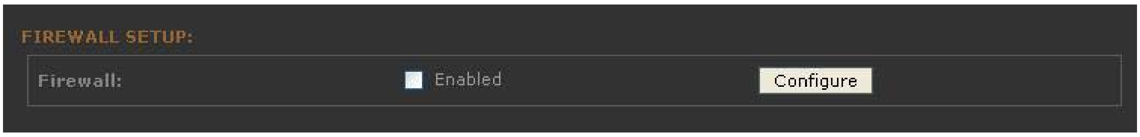
ROUTING INFORMATION PROTOCOL (RIP) SETUP:

Routing Info.Protocol: □ Enabled

Routing Info.Protocol Version: RIPv1

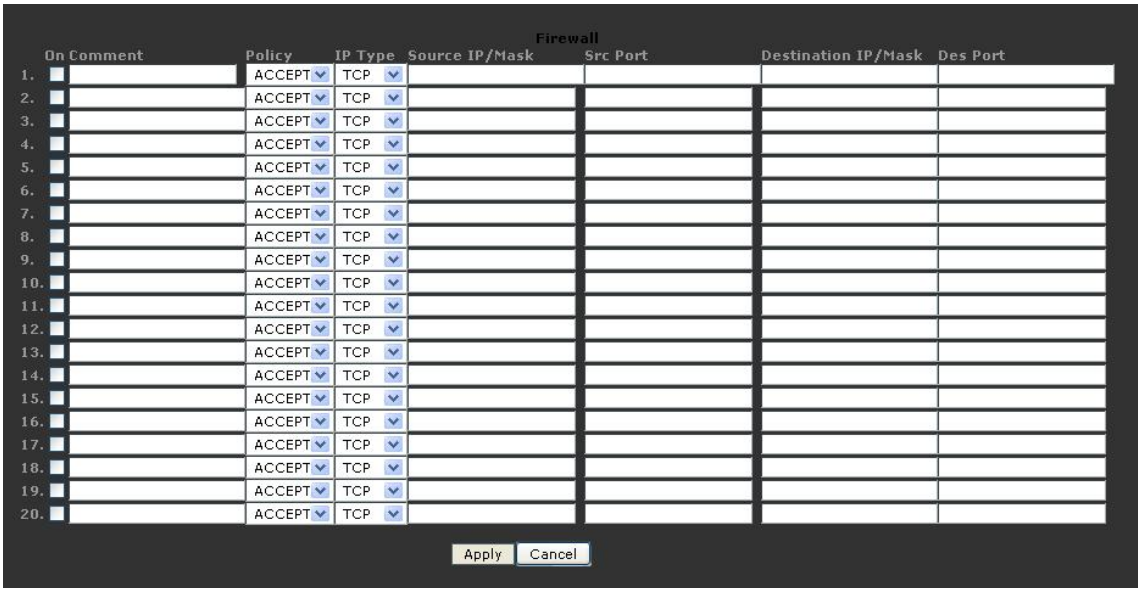
3.8.4 Firewall Setup

This allows the user to specify their required firewall rules.



FIREWALL SETUP:

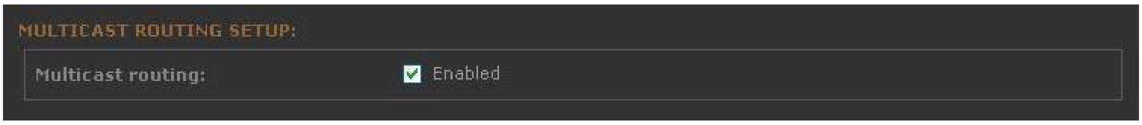
Firewall: ☐ Enabled



Firewall

	On	Comment	Policy	IP Type	Source IP/Mask	Src Port	Destination IP/Mask	Des Port
1.	☐		ACCEPT	TCP				
2.	☐		ACCEPT	TCP				
3.	☐		ACCEPT	TCP				
4.	☐		ACCEPT	TCP				
5.	☐		ACCEPT	TCP				
6.	☐		ACCEPT	TCP				
7.	☐		ACCEPT	TCP				
8.	☐		ACCEPT	TCP				
9.	☐		ACCEPT	TCP				
10.	☐		ACCEPT	TCP				
11.	☐		ACCEPT	TCP				
12.	☐		ACCEPT	TCP				
13.	☐		ACCEPT	TCP				
14.	☐		ACCEPT	TCP				
15.	☐		ACCEPT	TCP				
16.	☐		ACCEPT	TCP				
17.	☐		ACCEPT	TCP				
18.	☐		ACCEPT	TCP				
19.	☐		ACCEPT	TCP				
20.	☐		ACCEPT	TCP				

3.8.5 Multicast Routing

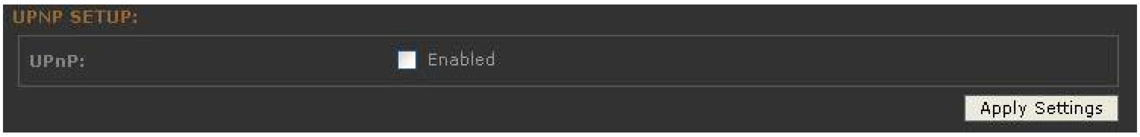


MULTICAST ROUTING SETUP:

Multicast routing: ☑ Enabled

3.8.6 Universal Plug and Play (UPNP) Setup

This allows for easy networking setup for any UPNP-aware Operating Systems.



UPNP SETUP:

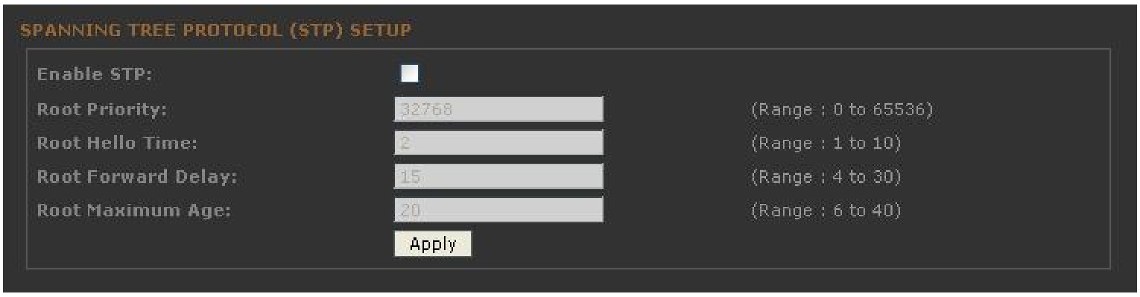
UPnP: ☐ Enabled

3.9 SERVICES Menu

The Services menu allows the user to specify various parameters for management and monitoring of the system.

3.9.1 Spanning Tree Protocol (STP) Setup

This configuration is for Bridge Mode only and implements a way to avoid looping ACK storms in the network, by controlling structured levels from root unit.



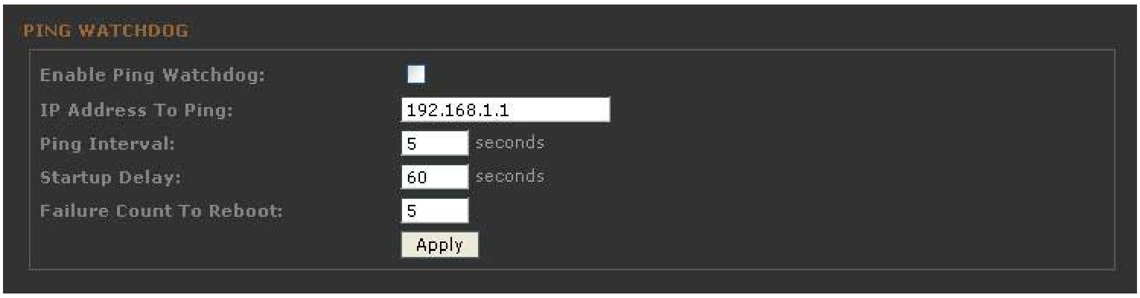
SPANNING TREE PROTOCOL (STP) SETUP

Enable STP:	□	
Root Priority:	32768	(Range : 0 to 65536)
Root Hello Time:	2	(Range : 1 to 10)
Root Forward Delay:	15	(Range : 4 to 30)
Root Maximum Age:	20	(Range : 6 to 40)

3.9.2 Ping Watchdog

This allows the user to specify an IP address to monitor and if the unit fails to reach the monitored IP address the unit will reboot automatically (based on the additional parameters).

Be careful not setting the Startup Delay to low on remote systems (CPE Unit) as it will take some time to connect to master and pass traffic (set minimum 120 sec).

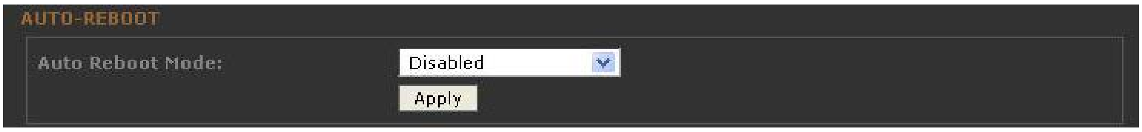


PING WATCHDOG

Enable Ping Watchdog:	□
IP Address To Ping:	192.168.1.1
Ping Interval:	5 seconds
Startup Delay:	60 seconds
Failure Count To Reboot:	5

3.9.3 Auto Reboot

This allows the user to set the device to reboot after a given amount of time. This can be specified in either hours or minutes.

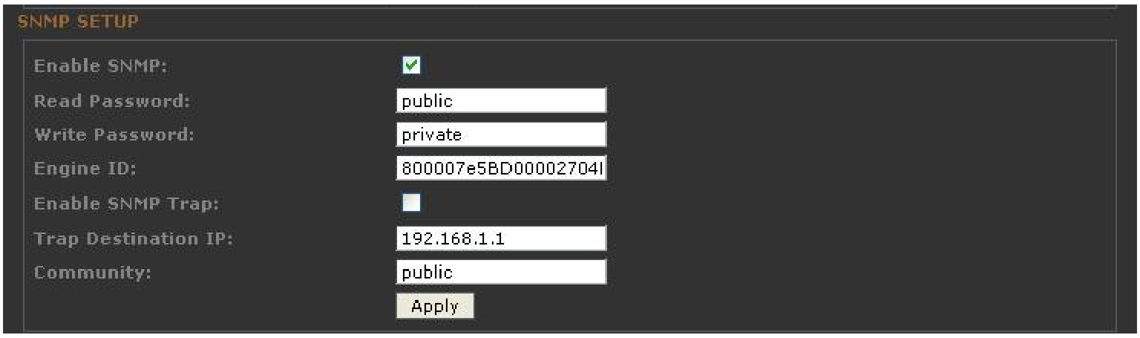


AUTO-REBOOT

Auto Reboot Mode:	Disabled

3.9.4 SNMP Setup

For setting up SNMP (Simple Network Management Protocol) with Read/Write configurations. Specify Community Read and Write password. The unit supports both SNMPv1 and v2. SNMP Trap is also supported by enabling and specifying trap host and community string.



SNMP SETUP

Enable SNMP: ☑

Read Password: public

Write Password: private

Engine ID: 800007e5BD00002704l

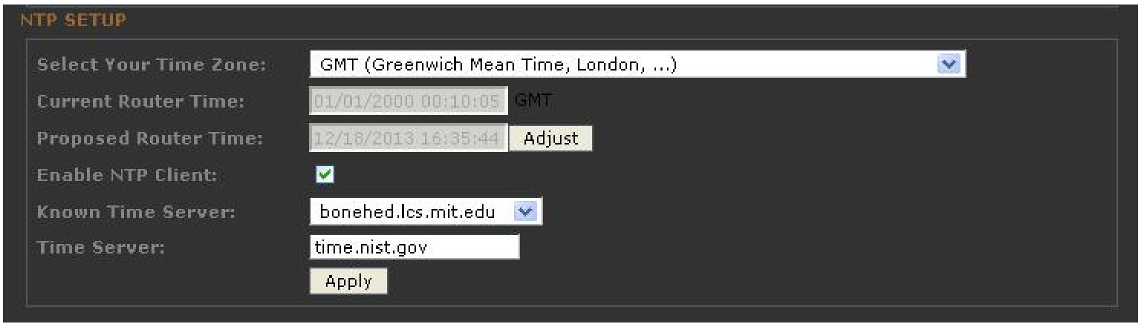
Enable SNMP Trap: □

Trap Destination IP: 192.168.1.1

Community: public

3.9.5 System Time Settings

Allows the user to set correct time on the unit manually or to use SNTP (Simple Network Time Protocol) to adjust automatically and adjust for Time Zone. Default Time Server is set to *time.nist.gov* - and works for most cases.



NTP SETUP

Select Your Time Zone: GMT (Greenwich Mean Time, London, ...)

Current Router Time: 01/01/2000 00:10:05 GMT

Proposed Router Time: 12/18/2013 16:35:44

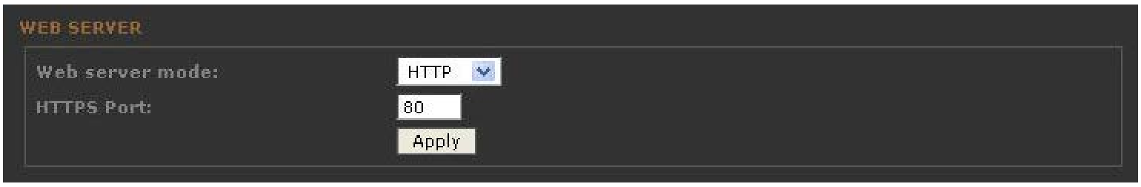
Enable NTP Client: ☑

Known Time Server: bonehed.lcs.mit.edu

Time Server: time.nist.gov

3.9.6 Web Management Setup

This is for setting the HTTP protocol to be used (HTTP or Secure HTTP/SSL) and Specifying the Login Timeout for automatic logout of inactive user.



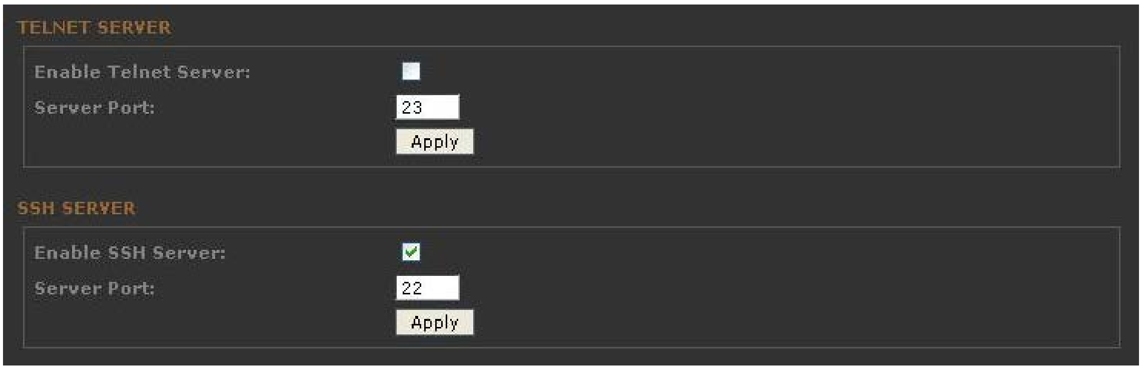
WEB SERVER

Web server mode: HTTP

HTTPS Port: 80

3.9.7 Telnet/SSH Setup

To allow/deny Telnet and/or SSH login to unit, and to specify the TCP port number to be used (default shown).



TELNET SERVER

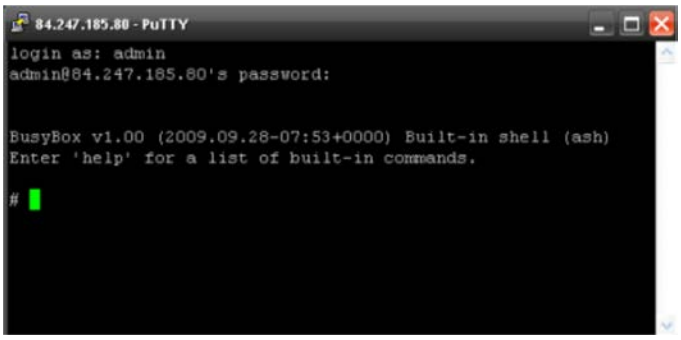
Enable Telnet Server: □

Server Port: 23

SSH SERVER

Enable SSH Server: ☑

Server Port: 22

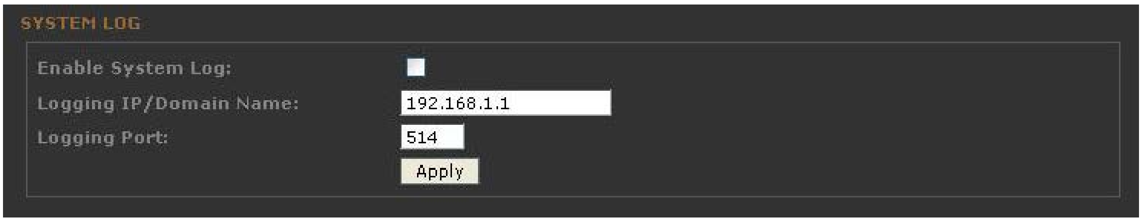


```
login as: admin
admin@84.247.185.80's password:


BusyBox v1.00 (2009.09.28-07:53+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

#
```

The Telnet/SSH gives the administrator access to BusyBox CLI shell (not Linux shell), and can enter “help” for available commands in the CLI. Log in using the default username and password (or with the password set for admin). Type "commit" to save any changes, and then "restart" to reboot and apply the new config. Note that you need to go to the wlan configuration by typing "config wlan 0" to read or change any wireless setting.

3.9.8 System log & SNMP Trap Setup

For setting the configuration for sending SNMP messages to a Trap Host. Specify the IP address to Trap Host, and the Community Password.



SYSTEM LOG

Enable System Log: □

Logging IP/Domain Name: 192.168.1.1

Logging Port: 514

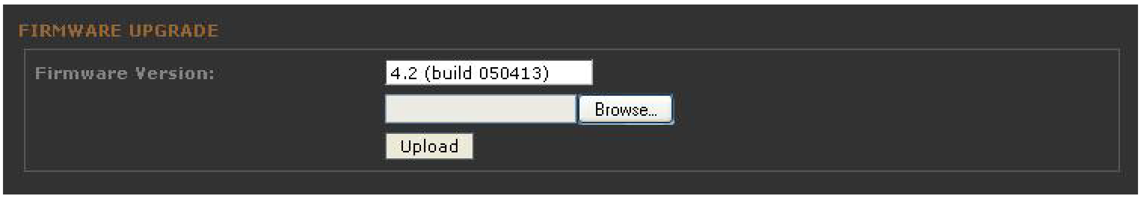
3.10 SYSTEM menu

The System menu allows the user to specify system parameters and do maintenance functions on the unit.

3.10.1 Firmware Upgrade

Allows the user to upgrade or downgrade the firmware remotely (use with caution and only when necessary). Upload firmware first, and then flash it to the units. The unit will ask you to confirm reboot after flashing is completed.

WARNING: Never interrupt the upgrade process when first started or you may damage the unit.

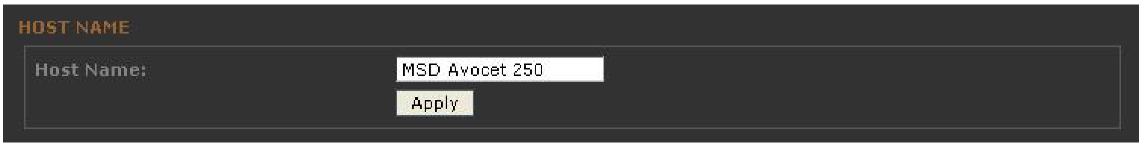


FIRMWARE UPGRADE

Firmware Version: 4.2 (build 050413)

3.10.2 Host Name

This allows a user friendly name to be set on the unit.

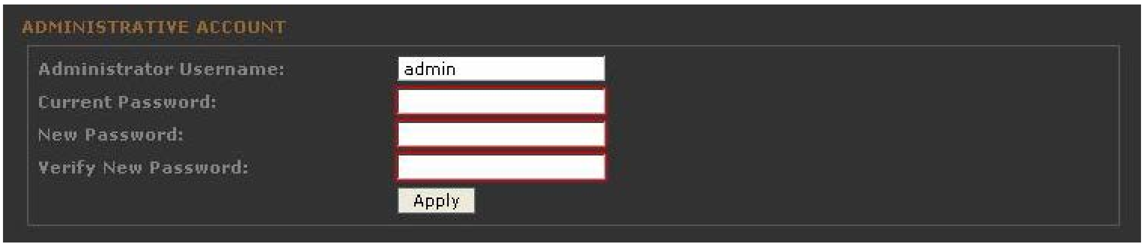


HOST NAME

Host Name: MSD Avocet 250

3.10.3 Change user Password

This allows the user to specify the Admin password for login to the unit. Current password must be specified to allow any change.



ADMINISTRATIVE ACCOUNT

Administrator Username: admin

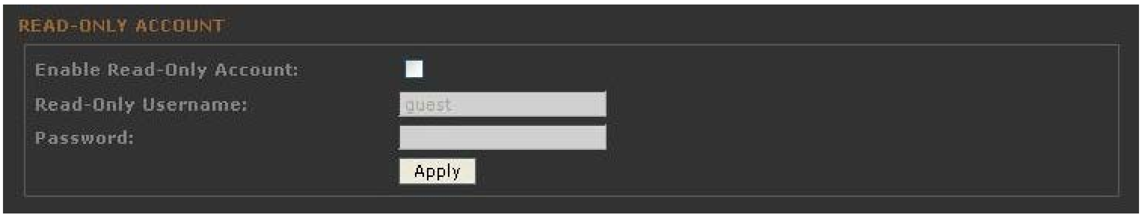
Current Password:

New Password:

Verify New Password:

3.10.4 Read-only Account

This is for specifying a read-only user and password to access the Status menu only.



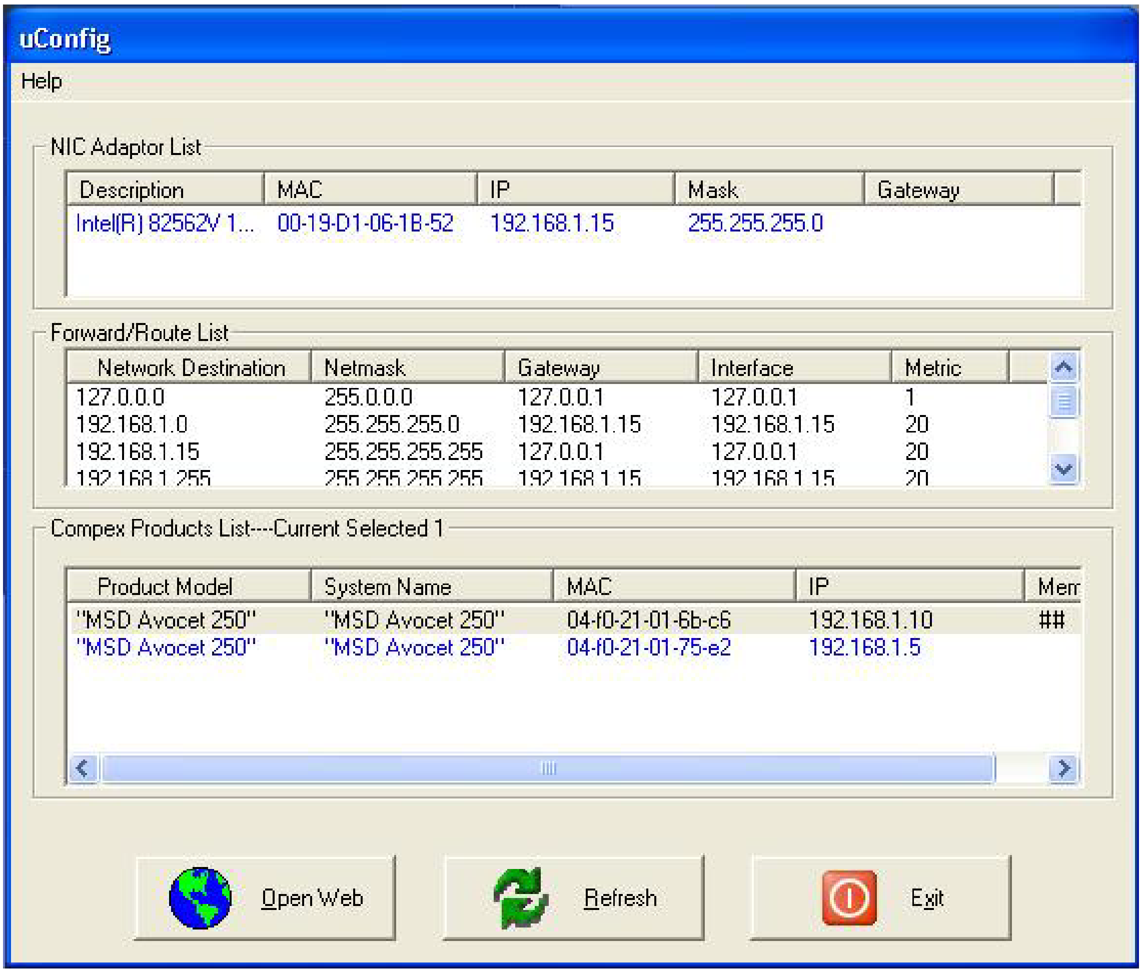
READ-ONLY ACCOUNT

Enable Read-Only Account:	□
Read-Only Username:	guest
Password:	

3.10.5 Software Tools

All Avocet unit supports a Windows program that can be used to detect any active units on Layer2 (Mac Layer) for management.

uConfig is compatible with most MS Windows versions – including Vista and Windows 7.



NIC Adaptor List

Description	MAC	IP	Mask	Gateway
Intel(R) 82562V 1...	00-19-D1-06-1B-52	192.168.1.15	255.255.255.0	

Forward/Route List

Network Destination	Netmask	Gateway	Interface	Metric
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.15	192.168.1.15	20
192.168.1.15	255.255.255.255	127.0.0.1	127.0.0.1	20
192.168.1.255	255.255.255.255	192.168.1.15	192.168.1.15	20

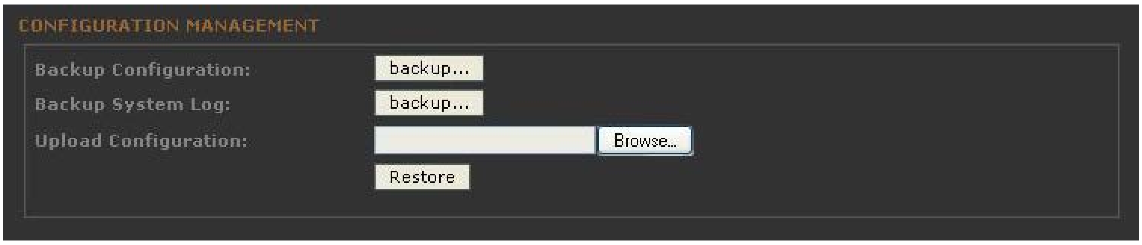
Compex Products List---Current Selected 1

Product Model	System Name	MAC	IP	Mem
"MSD Avocet 250"	"MSD Avocet 250"	04-f0-21-01-6b-c6	192.168.1.10	##
"MSD Avocet 250"	"MSD Avocet 250"	04-f0-21-01-75-e2	192.168.1.5	

Note: If Open Web is selected, the uConfig will temporarily implement an ipconfig setting compatible with unit IP-address.

3.10.6 Backup and Restore

To make backup of the running configuration or restore the configuration from a previous backed up file. Backup System Log, allows user to view startup log (dmesq file).



CONFIGURATION MANAGEMENT

Backup Configuration: backup...

Backup System Log: backup...

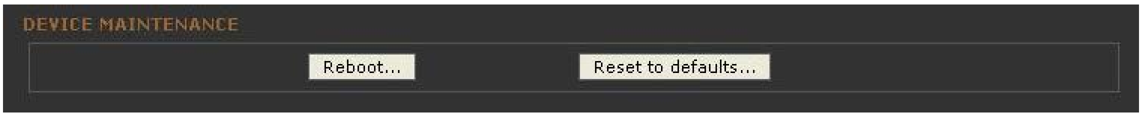
Upload Configuration: Browse...

Restore

3.10.7 Device Maintenance

Reboot System will send the unit into reboot.

Reset to default allows the user to reset the unit to “Factory Default” (RESET button forces IP address, username and password settings back to the system defaults)



4.0 SSH / Telnet Administration

4.1 CLI Command List

Note: command "commit" to activate all changed settings from "set"

System basic parameters:

Parameter	Command	Description
acl	get acl/set acl <interface> <param>:	get or set radio or vap acl state
aclpolicy	get aclpolicy/set aclpolicy <interface> <param>	get or set radio or vap aclpolicy state
acl_mac	get acl_mac/set acl_mac <interface> <mac_addr>	get or set acl mac address
brinfo	get brinfo	show bridge information
brmacinfo	get brmacinfo	show bridge mac address list
buttonpwdreset	get buttonpwdreset/set buttonpwdreset <param>	
button_all	get button/set button <param>	enable or disable all button function
ddns	get ddns/set ddns <param>	enable or disable DDNS
dhcp	get dhcp/set dhcp <param>	enable or disable dhcp server
dhcpendip	get dhcpstartip/set dhcpstartip <param>	get or set dhcpd start ip address
dnsmasq	get dnsmasq/set dnsmasq <param>	enable or disable dnsmasq
factorydefault	set factorydefault	set system configuration to default
ipaddr	get ipaddr/set ipaddr <param>	get or set lan ip address
ipmask	get ipmask/set ipmask <param>	get or set lan ip mask
macstats	get macstats	help information
nat	get nat/set nat <param>	enable or disable NAT
rip	get rip/set rip <param>	enable or disable RIP
riptype	get riptype/set riptype <param>	get or set RIP version,RIPv1 or RIPv2
routeshow	get routeshow	show routing table
satd	get satd/set satd <param>	enable or disable static address translation
snmp	get snmp/set snmp <param>	enable or disable snmp
snmpcommunity	get snmpreadcomm/set snmpreadcomm <param>	get or set snmp readonly community
snmpsetcommunity	get snmpwritecomm/set snmpwritecomm [param]	get or set snmp read/write community
ssh	get ssh/set ssh <param>	enable or disable sshd
sshport	get sshport/set sshport <param>	get or set sshd port number
sysinfo	get sysinfo	show system information
telnet	get telnet/set telnet <param>	enable or disable telnetd
telnetport	get telnetport/set telnetport <param>	set/get telnet port number
upgrade	set upgrade <tftp server ip> <remote file>	upgrade a new firmware from tftp server
upnp	get upnp/set upnp <param>	enable or disable upnp
userlist	get userlist	show user list
webserver	get webserver/set webserver <param>	get or set webs mode,http or https
wantype	get wantype/set wantype <param>	get or set wan type,e.g. static,dhcp, pppoe, pptp,l2tp
wanstaticip	get wanstaticip/set wanstaticip <param>	get or set static wan ip address
wanstaticmask	get wanstaticmask/set wanstaticmask <param>	get or set static wan mask address
restart	restart	reboot system

Parameter	Command	Description
acktimeout	get acktimeout/set acktimeout <param>	get or set long distance ACK timeout
antswitch	get antswitch/set antswitch <param>	get/set antenna state
apbridge	get apbridge/set apbridge <param>	get or set apbridge status
aplist	get aplist	list all available APs around
athstats	get athstats	list current radio statistics
autochannelselect	get autochannelselect/set autochannelselect <param>	enable or disable channel smart selection
beaconintval	get beaconintval/set beaconintval <param>	get or set radio beacon interval
bssinfo	get bssinfo	get current bss statistics
channel	get channel/set channel <param>	get or set operation channel
chanlist	get chanlist	list available channels in the currrent radio
cipher	get cipher/set cipher <param>	get or set WPA cipher type
config	get config	list all configured information
countrycode	get countrycode/set countrycode <param>	get or set country code
ctstimeout	get ctstimeout/set ctstimeout <param>	get or set CTS timeout
distance	get distance/set distance <param>	get or set long distance value
dtim	get dtim/set dtim <param>	get or set Data Beacon Rate
fragment	get fragment/set fragment <param>	get or set fragment threshold
groupkeyupdate	get groupkeyupdate/set groupkeyupdate <param>	get or set group key update interval
hidessid	get hidessid/set hidessid <param>	enable or disable beacon broadcasting
ieee80211stats	get ieee80211stats	list ieee80211 protocol statistics
interface	get interface/set interface <param>	get or set current radio interface
key	get key/set key <param>	get or set wep key
linkinfo	get linkinfo	display link information
opmode	get opmode/set opmode <param>	get or set operation mode
outdoor	get outdoor/set outdoor <param>	enable or disable outdoor
passphrase	get passphrase/set passphrase <param>	get or set wpa-psk passphrase
pvid	get pvid/set pvid <param>	get or set dot1q vlan id
radiusname	get radiusname/set radiusname <param>	get or set wpa-eap radius server
radiusport	get radiusport/set radiusport <param>	get or set wpa-eap radius port
radiussecret	get radiussecret/set radiussecret <param>	get or set shared radius secret
radio_off_eth_down	get radio_off_eth_down/set radio_off_eth_down <param>	enable or disable radio off
rootap	get rootap/set rootap <param>	enable or disable rootap role
rts	get rts/set rts <param>	get or set rts threshould
securitymode	get secmode/set secmode <param>	get or set wireless secret mode
slottimeout	get slottimeout/set slottimeout <param>	get or set slot timeout
ssid	get ssid/set ssid <param>	get or set wireless ssid
stalist	get sta	list all associated stations
txpower	get power/set power <param>	get or set transmission power
txrate	get txrate/set txrate <param>	get or set transmission rate
vlan	get vlan/set vlan <param>	get or set tag vlan id
wds	get wds/set wds <param>	enable or disable wds
wlanstate	get wlanstate/set wlanstate <param>	get or set wlan state
wirelessmode	get wirelessmode/set wirelessmode <param>	get or set wireless mode
wmm	get wmm/set wmm <param>	enable or disable WMM
wpakeytype	get wpakeytype/set wpakeytype <param>	get or set wpa keytype
keyentrymethod	get keyentrymethod /set keyentrymethod <param>	get or set wep key method