



# Table of Contents

---

<b>Chapter 1: Product Overview</b> .....	1
Package Contents .....	1
System Requirements .....	1
Top View .....	1
Rear View .....	1
<b>Chapter 2: Installation</b> .....	2
Hardware Installation.....	2
Connecting a Wireless Client to the AirRouter HP.....	4
<b>Chapter 3: Using AirOS™ on the AirRouter HP</b> .....	5
Interface Tabs .....	5
<b>Chapter 4: Main Tab</b> .....	6
Status .....	6
Monitor .....	7
<b>Chapter 5: Wireless Tab</b> .....	11
Basic Wireless Settings.....	11
Wireless Security .....	15
<b>Chapter 6: Network Tab</b> .....	18
Network Role.....	18
Bridge > Network Settings.....	19
Bridge > VLAN Network Settings.....	20
Bridge > Firewall Settings.....	20
Bridge > Static Routes .....	21
Router > WLAN Network Settings .....	21
Router > LAN Network Settings .....	23
Router > VLAN Network Settings.....	26
Router > Multicast Routing Settings.....	26
Router > Firewall Settings.....	26
Router > Static Routes .....	27
SOHO Router > WAN Network Settings.....	28
SOHO Router > LAN Network Settings .....	31
SOHO Router > VLAN Network Settings .....	32
SOHO Router > Multicast Routing Settings .....	33
SOHO Router > Firewall Settings .....	33
SOHO Router > Static Routes .....	34

<b>Chapter 7: Advanced Tab</b> .....	35
Advanced Wireless Settings .....	35
Advanced Ethernet Settings .....	37
Traffic Shaping .....	37
<b>Chapter 8: Services Tab</b> .....	38
Ping Watchdog .....	38
SNMP Agent .....	39
Web Server .....	39
SSH Server .....	39
Telnet Server .....	39
NTP Client .....	39
System Log .....	40
Device Discovery .....	40
<b>Chapter 9: System Tab</b> .....	41
Device .....	41
Date Settings .....	41
System Accounts .....	42
Miscellaneous .....	42
Location .....	42
Configuration Management .....	42
Device Maintenance .....	43
Tools .....	43
<b>Chapter 10: Ubiquiti Logo Tab</b> .....	48
AirMax Settings .....	48
AirSelect .....	49
AirView .....	50
<b>Appendix A: Specifications</b> .....	51
<b>Appendix B: Safety Notices</b> .....	52
Electrical Safety Information .....	52
<b>Appendix C: Warranty</b> .....	53
General Warranty .....	53
<b>Appendix D: Compliance Information</b> .....	54
Installer Compliance Responsibility .....	54
FCC .....	54
RF Exposure Warning .....	54
Industry Canada .....	54
CE Marking .....	54
RoHS/WEEE Compliance Statement .....	55

**Appendix E:** Declaration of Conformity ..... 56

**Appendix F:** Contact Information ..... 57

    Ubiquiti Networks Support ..... 57

# Chapter 1: Product Overview

Thank you for purchasing the Ubiquiti AirRouter HP.

## Package Contents



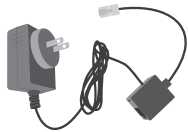
AirRouter



Antenna



Ethernet Cable



Power Adapter

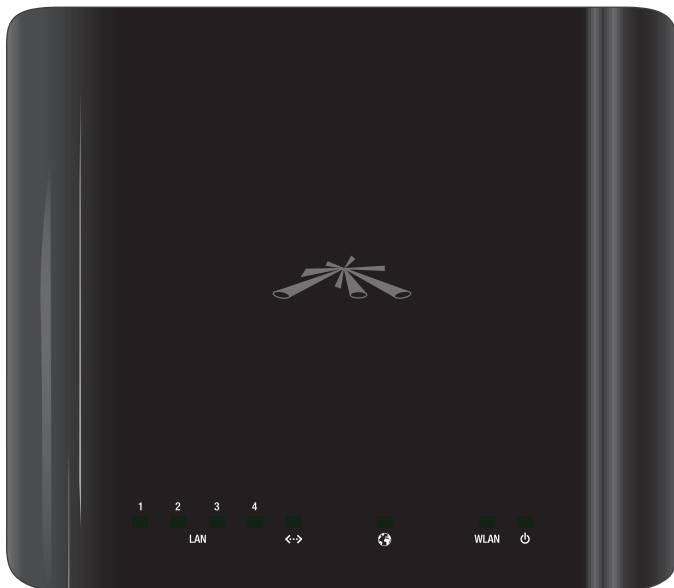


Quick Start Guide

## System Requirements

- Microsoft Windows XP, Windows Vista, Windows 7, Linux, or Mac OS X
- Java Runtime Environment 1.6 (or above) for the *AirView* utility
- Web Browser: Mozilla Firefox, Apple Safari, or Microsoft Internet Explorer

## Top View



**1-4 LAN** **LAN LEDs (1-4)** Displays the status of the wired connections to Ethernet ports 1-4. Solid green indicates a good connection. Flashing indicates activity on the specific port.

- <->** **Main Ethernet LED** Displays the status of the Main Ethernet port connection. Solid green indicates a good connection. Flashing indicates activity.
- Internet** **Internet LED** Displays solid green when the AirRouter HP is connected to the Internet. Flashes to indicate Internet activity.
- WLAN** **Wireless LAN LED** Displays solid green when the wireless LAN is enabled. It will flash to indicate wireless activity.
- Power** **Power LED** Displays solid green when the Power over Ethernet has been properly connected. An Ethernet cable should be connected to the <-> Main Ethernet port on the AirRouter HP and to the power adapter.

## Rear View



- <->** **Main Ethernet Port** Functions as the WAN port in SOHO Router mode and connects your AirRouter to your broadband modem or Internet connection using a standard Ethernet cable. Also functions as the Power over Ethernet port for the AirRouter HP.
- LAN 1-4** **LAN Ports (1-4)** Connects devices to your AirRouter using standard Ethernet cables.
- Reset** **Reset Button** Resets the AirRouter HP to the factory default settings.
 

**Note:** Resetting the AirRouter HP to factory default settings will erase custom settings you have made. You can backup your configuration from **System > Backup Configuration > Download** in the browser-based management interface.
- USB** **USB Port** Reserved for future use.
- Antenna** **Antenna Connector** The AirRouter HP antenna connects here.

## Chapter 2: Installation

### Hardware Installation

To install the AirRouter HP, perform the following steps:

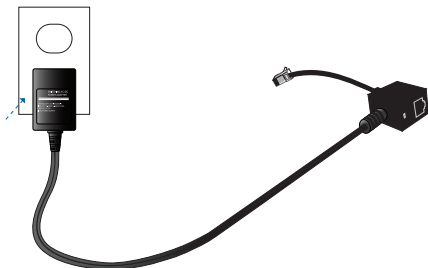
1. Connect the antenna to the antenna connector on the AirRouter HP by rotating it clockwise.



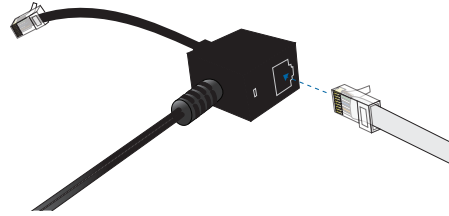
2. Raise the antenna to an upright position.



3. Connect the power adapter to a power outlet.



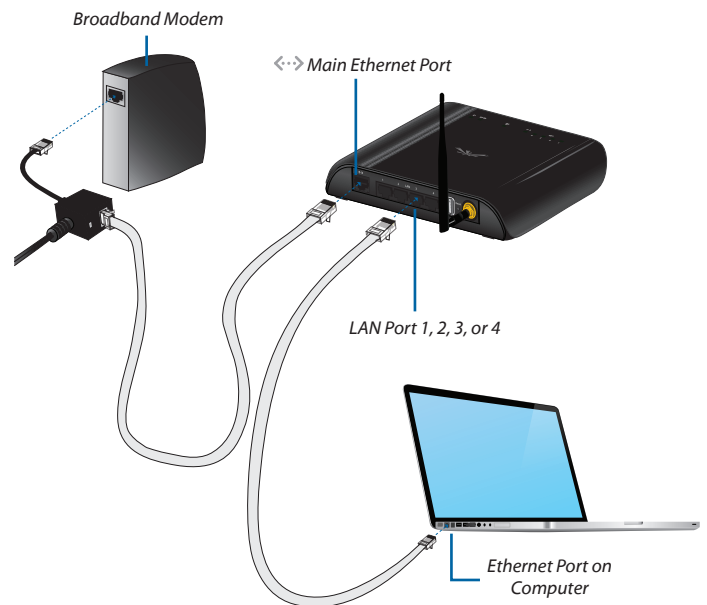
4. Connect an Ethernet cable to the <math>\leftrightarrow</math> Main Ethernet port on the power adapter.



5. Connect the other end of the Ethernet cable to the <math>\leftrightarrow</math> Main Ethernet port on the AirRouter HP. The Power LED will light up on the front of the AirRouter HP.



6. Connect the Ethernet connector on the power adapter to your broadband modem. Connect another Ethernet cable from your computer to a LAN port (1, 2, 3, or 4) on the AirRouter HP.

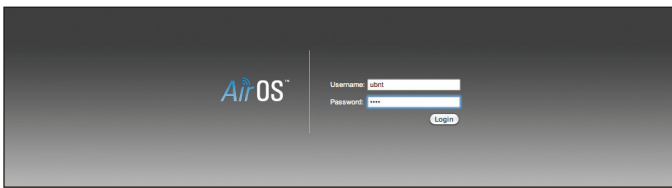


7. Launch your Web browser and type **http://192.168.1.1** in the address field and press **Enter** (PC) or **Return** (Mac).



**Note:** Your computer needs to be on the 192.168.1.x subnet. If you have DHCP enabled on your Ethernet adapter, it should receive an address automatically. If not, you will need to set a static IP address in the 192.168.1.2 - 192.168.1.254 range.

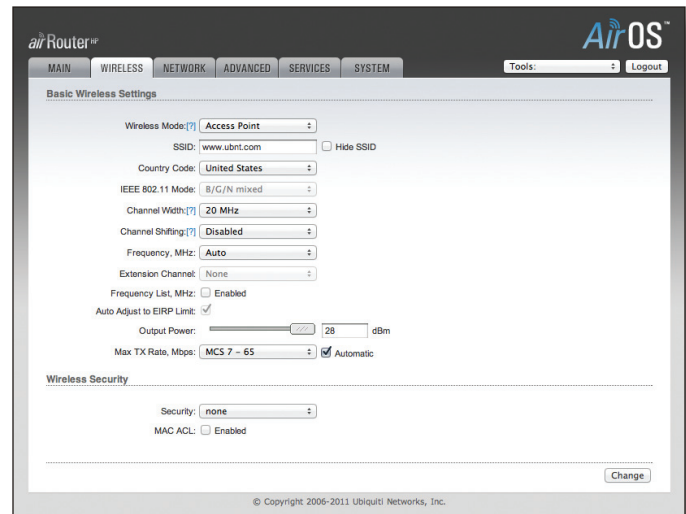
8. The login screen will appear. Enter **ubnt** in the *Username* and *Password* fields and click **Login**.



9. The AirOS interface will appear. Go to the **Wireless** tab.



10. Customize your wireless network and secure your network by entering the basic wireless network information:



- Enter a name for your wireless network in the *SSID* field.
- Select the type of security that you want to use for your wireless network from the *Security* drop-down.



**Note:** WPA2-AES security is the strongest wireless security method. If all of your devices support this option, it is recommended that you select it.


- Enter a passphrase in the **WPA Preshared Key** field. You can click the *Show* option to see the characters that you are typing.
- Click **Change**. You will be prompted to apply the changes. To proceed, click **Apply**.

Congratulations! Basic router installation is complete. The next page provides information for connecting wireless clients.


# Connecting a Wireless Client to the AirRouter HP

## Windows

1. Go to *Connect to Network*.



**Windows 7** Right-click on the *Network*  icon.

**Windows Vista** Go to **Start > Connect To**.

**Windows XP** Right-click the *Wireless Network*  icon in the *System Tray* (lower right corner of the screen) and then click **View Available Wireless Networks**.

2. Select the wireless network (SSID) that you entered in the *SSID* field in step 7a and then click **Connect**.
3. Type the passphrase that you entered in the *WPA Preshared Key* field in step 7c and click **OK** or **Connect**.
4. Launch your web browser to begin browsing the web.

## Mac

1. Click the *AirPort*  icon in the menu bar (top left side of the screen).
2. Select the wireless network (SSID) that you entered in the *SSID* field in step 7a.
3. Type the passphrase that you entered in the *WPA Preshared Key* field in step 7c and click **OK**.
4. Once connected the *AirPort*  icon will change from gray to solid black. The number of black lines indicates the signal strength. Launch your web browser to begin browsing the web.



## Chapter 3: Using AirOS™ on the AirRouter HP

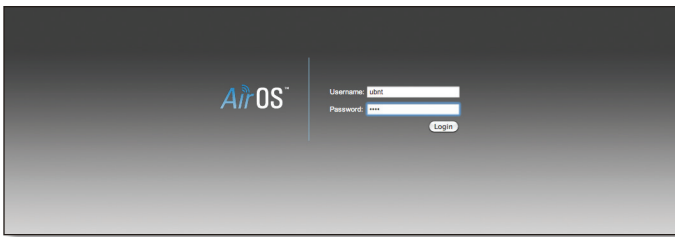
AirOS™ is an advanced operating system that is capable of powerful wireless and routing features. AirOS is built upon a simple and intuitive user interface. AirOS allows you to maximize the wireless performance of your AirRouter HP.

To access the interface, perform the following steps:

1. Launch your Web browser and type **http://192.168.1.1** in the address field and press enter (PC) or return (Mac).



2. The login screen will appear. Enter **ubnt** in the *Username* and *Password* fields and click **Login**.



### Interface Tabs

The AirRouter HP interface contains six primary tabs. This User Guide covers each tab with a chapter. For details on a specific tab, refer to the appropriate chapter.

- **Main** The *Main* tab displays AirRouter HP status information and provides network monitoring links. **"Main Tab" on page 6.**
- **Wireless** The *Wireless* tab allows you to configure the wireless mode, the basic wireless settings and the wireless security settings for the AirRouter HP. **"Wireless Tab" on page 11.**
- **Network** The *Network* tab covers the configuration of the network operating mode, IP settings, packet filtering routines and network services. **"Network Tab" on page 18.**
- **Advanced** The *Advanced* tab settings are available for additional wireless interface controls. Advanced wireless settings can be configured in this tab. The *Advanced* tab also includes advanced Ethernet and traffic shaping settings. **"Advanced Tab" on page 35.**
- **Services** The *Services* tab covers the configuration of system management services like Ping Watchdog, SNMP Agent, Web Server, SSH Server, Telnet Server, NTP Client, Dynamic DNS and System Log. **"Services Tab" on page 38.**

- **System** The *System* tab contains controls for system maintenance routines, administrator account management, device customization, firmware upgrade and configuration backup. The AirMax feature can be enabled and the interface language can also be selected here. **"System Tab" on page 41.**

Each tab also contains network administration and monitoring tools:

- **"Align Antenna" on page 43**
- **"Site Survey" on page 44**
- **"Ping" on page 44**
- **"Traceroute" on page 44**
- **"Speed Test" on page 45**
- **"AirView" on page 45**

**air Router HP** **AirOS™**

MAIN WIRELESS NETWORK ADVANCED SERVICES SYSTEM Tools: [v] Logout

**Status**

Device Name: Ubiquiti	AP MAC: 00:27:22:0E:85:7F
Network Mode: SOHO Router	Connections: 0
Wireless Mode: Access Point	Noise Floor: -96 dBm
SSID: www.ubnt.com	Transmit CCQ: -
Security: none	AirMax: Disabled
Version: v5.3.3	
Uptime: 17:46:53	
Date: 2011-07-27 05:28:50	
Channel/Frequency: 31 / 2414 MHz	
Channel Width: 40 MHz (Upper)	
ACK/Distance: 31 / 0.4 miles (0.6 km)	
TX/RX Chains: 1X1	
WLAN MAC: 00:27:22:0E:85:7F	
LAN MAC: 00:27:22:0E:85:7F	
WAN MAC: 00:27:22:0F:85:7F	
WAN/LAN: Unplugged / 100Mbps-Full	

**Monitor**

[Throughput](#) | [Stations](#) | [DHCP Client](#) | [ARP Table](#) | [Routes](#) | [Port Forward](#) | [Log](#)

LAN

WAN

## Chapter 4: Main Tab

The *Main* tab displays a summary of the link status information, current values of the basic configuration settings (depending on the operating mode), network settings and information, and traffic statistics.

### Status

**Status**

Device Name: Ubiquiti	AP MAC: 00:27:22:0E:85:7F
Network Mode: SOHO Router	Connections: 0
Wireless Mode: Access Point	Noise Floor: -96 dBm
SSID: www.ubnt.com	Transmit CCQ: -
Security: none	AirMax: Disabled
Version: v5.3.3	
Uptime: 00:04:30	
Date: 2011-07-26 11:46:27	
Channel/Frequency: 7 / 2442 MHz	
Channel Width: 20 MHz	
ACK/Distance: 31 / 0.4 miles (0.6 km)	
TX/RX Chains: 1X1	
WLAN MAC: 00:27:22:0E:85:7F	
LAN MAC: 00:27:22:0E:85:7F	
WAN MAC: 00:27:22:0F:85:7F	
WAN/LAN: Unplugged / 100Mbps-Full	

**Device Name** Displays the customizable name (ID) of the AirRouter HP. The Device Name (Host Name) is displayed in registration screens and discovery tools.

**Network Mode** Displays the network mode that the AirRouter HP is operating in. There are three modes available: *Bridge*, *Router*, and *SOHO Router*. *SOHO Router* is the default setting. This setting is configured on the *Network* tab.

**Wireless Mode** Displays the radio interface operating mode. *Access Point* (or *Access Point WDS*) and *Station* (or *Station WDS*) operating modes can be set depending on the network topology requirements.

**SSID** Displays the wireless network name (SSID). The wireless network name is dependent upon the wireless mode selected:

- While operating in Station mode, displays the SSID of the Access Point the AirRouter HP is associated with.
- While operating in Access Point mode, this displays the SSID configured on the AirRouter HP. The SSID is configured on the *Wireless* tab.

**Security** Displays the wireless security method being used on the AirRouter HP. If *None* is displayed, then wireless security has been disabled.

**Version** Displays the version of the AirOS software.

**Uptime** This is the total time the AirRouter HP has been running since last power up (reboot) or software upgrade. The time is displayed in days, hours, minutes and seconds.

**Date** Displays the current system date and time. The date and time are displayed in YEAR-MONTH-DAY HOURS:MINUTES:SECONDS format. The system date and time is retrieved from the Internet using NTP (Network Time Protocol). NTP Client is enabled by default on the *Services* tab. The AirRouter HP doesn't have an internal clock and the date and time may be inaccurate if NTP Client is disabled or the AirRouter HP isn't connected to the Internet.

**Channel/Frequency** Displays the channel number and corresponding operating frequency. The AirRouter HP uses the channel/radio frequency specified to transmit and receive data. Valid channel/frequency range will vary depending on local country regulations.

**Channel Width** This is the spectral width of the radio channel used by the AirRouter HP. 5, 10, 20 and 40 MHz channel spectrum widths are supported. In Station (or Station WDS) 20/40 MHz is the value by default.

**ACK/Distance** Displays the current timeout value for ACK frames. ACK Timeout can be set manually or self-adjusted automatically. The ACK Timeout (Acknowledgement frame Timeout) specifies how long the AirRouter HP should wait for an acknowledgement from a partner device confirming packet reception before concluding there must have been an error and resending the packet.

**TX/RX Chains** Displays the number of independent spatial data streams the AirRouter HP is transmitting/receiving simultaneously within one spectral channel of bandwidth. This ability is specific for 802.11n devices which rely on multiple-input multiple-output (MIMO) technology. Multiple chains increase data transfer performance significantly. The number of chains Ubiquiti device uses is hardware specific. Every TX/RX chain requires a separate antenna.

**WLAN MAC** Displays the MAC address of the AirRouter HP as seen on the wireless network.

**LAN MAC** Displays the MAC address of the AirRouter HP as seen on the LAN (Local Area Network).

**WAN MAC** Displays the MAC address of the AirRouter HP as seen on the WAN interface. This is the AirRouter HP's MAC address that is seen over the Internet.

**WAN/LAN** Indicates the current status of the WAN and LAN Ethernet port connections. This can indicate that a cable is not plugged into a device and there is no active Ethernet connection.

**AP MAC** Displays the MAC address of the AirRouter HP in *Access Point* or *Access Point WDS* mode. In *Station* or *Stations WDS* mode, this displays the MAC address of the Access Point the AirRouter HP is associated with.

**Connections** Displays the number of wireless devices connected to the AirRouter HP when the device is operating in *Access Point* or *Access Point WDS* mode. This value is not displayed while operating in *Station* or *Station WDS* mode.

**Noise Floor** Displays the current value of the noise level in dBm. Noise Floor is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI).

**Transmit CCQ** This is an index of which evaluates the wireless Client Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

**Airmax** Indicates the AirMax status (Ubiquiti's proprietary TDMA polling technology) when operating in *Access Point* or *Access Point WDS* mode. If AirMax is enabled, the AirRouter HP will only accept AirMax clients. (Disable AirMax for legacy 802.11bgn device compatibility). AirMax also features advanced QoS Autodetection settings.

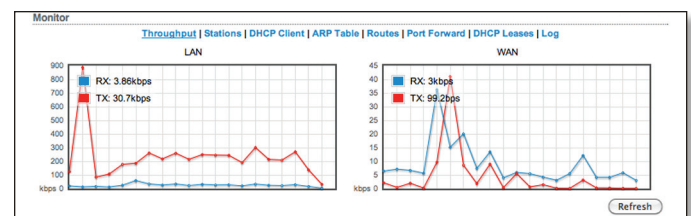
**Airmax Quality** This displays the AirMax Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

**Airmax Capacity** This is an index of maximum data rate the link is operating at. A Lower Capacity number indicates a unit that is bogging the system down.

## Monitor

There are various monitoring tools accessible via the links on the *Main* tab. The default selection is *Throughput* which is displayed as soon as you open the *Main* tab.

### Throughput



Shows a visual representation of the current data traffic on the LAN and WLAN in both graphical and numerical form. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value. The statistics are updated automatically. Throughput statistics can be updated manually using the **Refresh** button.

### Stations

This selection lists the stations which are connected to the AirRouter HP while operating in *Access Point* or *Access Point WDS* mode.

Station MAC	Device Name	Signal / Noise, dBm	TX/RX, Mbps	CCQ, %	Connection Time	Last IP	Action
10:9A:DD:BA:5A:7E		-56 / -93	52 / 58.5	95	01:08:06	192.168.25.191	kick

The following statistics for each station are displayed in the station statistics window:

**Station MAC** MAC address of the associated station. This is a clickable link that will display additional station info.

**Device Name** Displays the client's host name (if defined).

**Signal/Noise, dBm** Signal value represents the last received wireless signal level, and Noise displays the value of the noise level.

**Tx/Rx, Mbps** Tx value represents the data rates, in Mbps, of the last transmitted packets, and Rx value represents the data rates, in Mbps, of the last received packets.

**CCQ, %** This is an index that evaluates the wireless Client Connection Quality (CCQ). The level is a percentage value where 100% corresponds to a perfect link state.

**Connection Time** Displays the connection time of each station connected to the AirRouter HP. The time is expressed in days, hours, minutes and seconds.

**Last IP** Displays the station's IP address.

**Action** Shows available options for this station, e.g.: kicking a station for a few seconds to identify any problematic stations.

**Refresh** The information in the station statistics window can be updated using the *Refresh* button.

### Station Info

Detailed information is displayed when you click on a specific MAC address:

Station	10:8A:DD:BA:5A:7E	[ 1 ]
Device Name:	Negotiated Rate	Last Signal, dBm
Connection Time: 01:15:35	MCS0	N/A
Signal Strength: -61 dBm	MCS1	N/A
Noise Floor: -93 dBm	MCS2	-62
CCQ: 96%	MCS3	N/A
Last IP: 192.168.25.191	MCS4	-61
TX/RX Rate: 58.5 Mbps / 65.0 Mbps	MCS5	-62
TX/RX Packets: 146448 / 134656	MCS6	-63
TX/RX Packet Rate, pps: 7 / 11	MCS7	-62
Bytes Transmitted: 154344908 (147.19 MBytes)		
Bytes Received: 32854772 (31.33 MBytes)		

**Device Name** Displays the client's host name.

**Connection time** Displays the amount of time the station has been connected to the AirRouter HP. The time is expressed in days, hours, minutes and seconds.

**Signal Strength** Value represents, in dBm, the last received wireless signal level.

**Noise Floor** Displays the current value of the noise level in dBm. Noise Floor is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.

**CCQ** Value represents the quality of the connection to the Station.

**Last IP** Displays the last station's IP address.

**TX/RX Rate** Represents the data rates, in Mbps, of the last transmitted and received packets;

**TX/RX Packets** Value represents the total amount of packets transmitted and received from the Station during the connection uptime.

**TX/RX Packet Rate, pps** Represents the mean value of the transmitted and received packet rate.

**Bytes Transmitted** Value represents the total amount of data (in bytes) transmitted during the connection.

**Bytes Received** Value represents the total amount of data (in bytes) received during the connection.

**Negotiated Rate/Last Signal (dBm) Table** The values represent the received wireless signal level along with the all data rates of recently received packets. *N/A* value is represented as the Last Signal if no packets were received on that particular data rate.

**Kick** The connection to the station can be dropped by clicking **Kick**.

**Refresh** The list can be updated by clicking **Refresh**.

**Close** The Station Info window can be closed by clicking **Close**.

### AP Information

Available only when operating in *Station* or *Station WDS* mode.

Access Point	00:14:BF:BF:07:3F
Device Name:	Negotiated Rate Last Signal, dBm
Connection Time: 00:17:02	MCS0 N/A
Signal Strength: -60 dBm	MCS1 -60
Noise Floor: -92 dBm	MCS2 -60
CCQ: 97%	MCS3 -63
Last IP: unknown	MCS4 N/A
TX/RX Rate: 52.0 Mbps / 13.0 Mbps	MCS5 N/A
TX/RX Packets: 2349 / 2576	MCS6 N/A
TX/RX Packet Rate, pps: 2 / 2	MCS7 N/A
Bytes Transmitted: 1232791 (1.18 MBytes)	MCS8 N/A
Bytes Received: 620803 (606.25 kBytes)	MCS9 N/A
	MCS10 N/A
	MCS11 N/A
	MCS12 N/A
	MCS13 N/A
	MCS14 N/A
	MCS15 N/A

- **Access Point** Shows the MAC address of the Access Point the station is associated with.
- **Device Name** Displays the host name of the Access Point the station is associated with.
- **Connection time** Value represents the running total of time the AirRouter HP has been associated with the Access Point. The time is expressed in days, hours, minutes and seconds.
- **Signal Strength** Value represents the last received wireless signal level.
- **Noise Floor** Displays the current value of the noise level in dBm. Noise Floor is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.
- **CCQ** Value represents the quality of the connection to the Access Point.
- **Tx/Rx Rate** Represents the data rates of the last transmitted and received packets.
- **Tx/Rx Packets** Displays the total number of packets transmitted and received during the connection.
- **Tx/Rx Packet Rate (packets per second)** Represents the mean value of the transmitted and received packet rate.

- **Bytes transmitted/received** Value represents the total amount of data (in bytes) transmitted and received during the connection.
- **Negotiated Rate/Last Signal (dBm) Table** The values represent the received wireless signal level along with the all data rates of recently received packets. *N/A* value is represented as the Last Signal if no packets were received on that particular data rate.
- **Reconnect** To reconnect to the AP and reestablish the wireless link, click **Reconnect**.
- **Refresh** The list can be updated by clicking **Refresh**.

## DHCP Client

(Applicable for *Router* and *SOHO Router* in DHCP mode only.) Shows the device's WAN IP address, Netmask, DNS servers and Gateway while operating in DHCP Router mode.

DHCP Client Information	
IP Address: 72.130.85.122	DHCP Server: 76.85.238.35
Netmask: 255.255.248.0	Domain: social.rr.com
Gateway: 72.130.80.1	Total Lease Time: 00:44:42
Primary DNS IP: 209.18.47.61	Remaining Lease Time: 00:00:00
Secondary DNS IP: 209.18.47.62	

**IP Address** Displays the device's WAN IP address while operating in DHCP Client mode.

**Netmask** Displays the device's netmask when operating in DHCP Client mode. It is assigned automatically by the DHCP server (not the AirRouter HP's DHCP server), which assigns the WAN IP address to the device.

**Gateway** Displays the device's gateway when operating in DHCP Client mode, which is assigned automatically by the DHCP server (not the AirRouter HP's DHCP server).

**Primary/Secondary DNS IP** Domain Name System (DNS) is an Internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses that the AirRouter HP uses for translation.

**DHCP Server** Displays the IP address of the DHCP Server assigning the WAN IP Address to the AirRouter HP.

**Domain** Displays the domain name.

**Total Lease Time** Shows the total time (validity) of the leased IP address assigned by the external DHCP server.

**Remaining Lease Time** Displays the remaining time of the IP address leased by the external DHCP server.

**Renew** The IP address and can be renewed by clicking **Renew**.

**Release** The IP address can be released by clicking **Release**.

**Refresh** The list can be updated by clicking **Refresh**.

## ARP Table

Lists all the entries of the ARP (Address Resolution Protocol) Table currently recorded on the device.

ARP is used to associate each IP address to the unique hardware address (MAC) of each device. It is important to have unique IP addresses for each MAC or else there will be ambiguous routes in the network.

IP Address	MAC Address	Interface
192.168.26.193	00:16:CB:BA:AD:F8	LAN
192.168.26.192	00:1B:B9:5D:B9:59	LAN
192.168.26.223	90:27:E4:F6:34:43	LAN
72.130.80.1	00:30:B6:C9:02:A1	WAN

**IP Address** Displays the assigned IP address.

**MAC Address** Displays the MAC address of the device.

**Interface** Displays the interface that the device is on.

**Refresh** The list can be updated by clicking **Refresh**.

## Bridge Table

Displays the entries in the system Bridge Table when the device is operating in *Bridge* mode.

The Bridge Table shows which bridge port the particular station is associated with - in other words from which interface (*LAN* or *Wireless LAN*, as *WLAN*) the network device (defined by MAC Address) is reachable from. The AirRouter HP will forward the packets to that port only (thus saving a lot of redundant copies and transmits).

MAC Address	Interface	Ageing Timer
00:23:EE:E3:57:E5	LAN	2.77
10:9A:DD:65:8C:A2	WLAN	0.19
10:9A:DD:BA:5A:7E	LAN	0.02
30:48:9A:26:18:5D	LAN	0.02
3C:EA:4F:8A:81:29	LAN	0.29
C0:3F:0E:3F:BC:1D	LAN	4.36

**MAC Address** Displays the MAC Address entry of each network device that is associated to the station.

**Interface** Displays the interface the network device (defined by MAC Address) is reachable from. Displayed as *LAN* or *WLAN*.

**Ageing Timer** Displays how long it has been since a packet has been detected from each MAC Address entry (in seconds). After a particular time-out without detecting any packet activity, the bridge will delete that address from the Bridge Table.

• **Refresh** The list can be updated by clicking **Refresh**.

## Routes

Lists all the entries in the system routing table, while the device is operating in *Router* mode.

Destination	Gateway	Netmask	Interface
192.168.26.0	0.0.0.0	255.255.255.0	LAN
72.130.80.0	0.0.0.0	255.255.248.0	WAN
169.254.0.0	0.0.0.0	255.255.0.0	LAN
0.0.0.0	72.130.80.1	0.0.0.0	WAN

AirOS examines the destination IP address of each data packet traveling through the system (**Destination** column) and chooses the appropriate interface to forward the packet to. The system choice depends on static routing rules – entries, which are registered in the system routing table. Static routes to specific hosts, networks or default gateway (**Gateway**, **Netmask** and **Interface** columns) are set up automatically according to the IP configuration of all the AirOS interfaces.

- **Refresh** The list can be updated by clicking **Refresh**.

## Port Forward

Chain	bytes	target	prot	opt	in	out	source	destination	top
PORTFORWARD	0	DNAT	tcp	--	*	+	0.0.0.0/0	0.0.0.0/0	top dpt:21 to:1

Lists active port forward entries in the PORTFORWARD chain of the standard iptables nat table, while the device is operating in *Router* mode.

Port forwarding is enabled and configured on the *Network* tab.

Port Forwarding creates a transparent tunnel through a firewall/NAT, granting an access from the WAN side to the particular network service running on the LAN side.

- **Refresh** The list can be updated by clicking **Refresh**.

## DHCP Leases

Shows the current status of the leased IP addresses by the device's DHCP server. This option is available if DHCP Server is enabled while the device is operating in *Router* mode.

MAC Address	IP Address	Remaining Lease	Hostname	Interface
00:16:CB:BA:AD:F8	192.168.26.193	00:07:12		LAN
00:1B:B9:5D:09:59	192.168.26.192	00:06:01	raquel-rm	LAN
90:27:E4:F8:34:43	192.168.26.223	00:06:32		LAN

**MAC Address** Displays the client's MAC address, which is connected to the Access Point.

**IP Address** Displays the client's IP address leased by the device's DHCP server.

**Remaining Lease Time** Shows how long the leased IP address will be valid and reserved for particular DHCP client.

**Hostname** Displays the device name (hostname) of the client receiving an IP lease.

**Interface Name** Displays the interface to which the specific MAC address is connected.

**Refresh** The list can be updated by clicking **Refresh**.

More information is provided in the *Wireless* section.

## Log

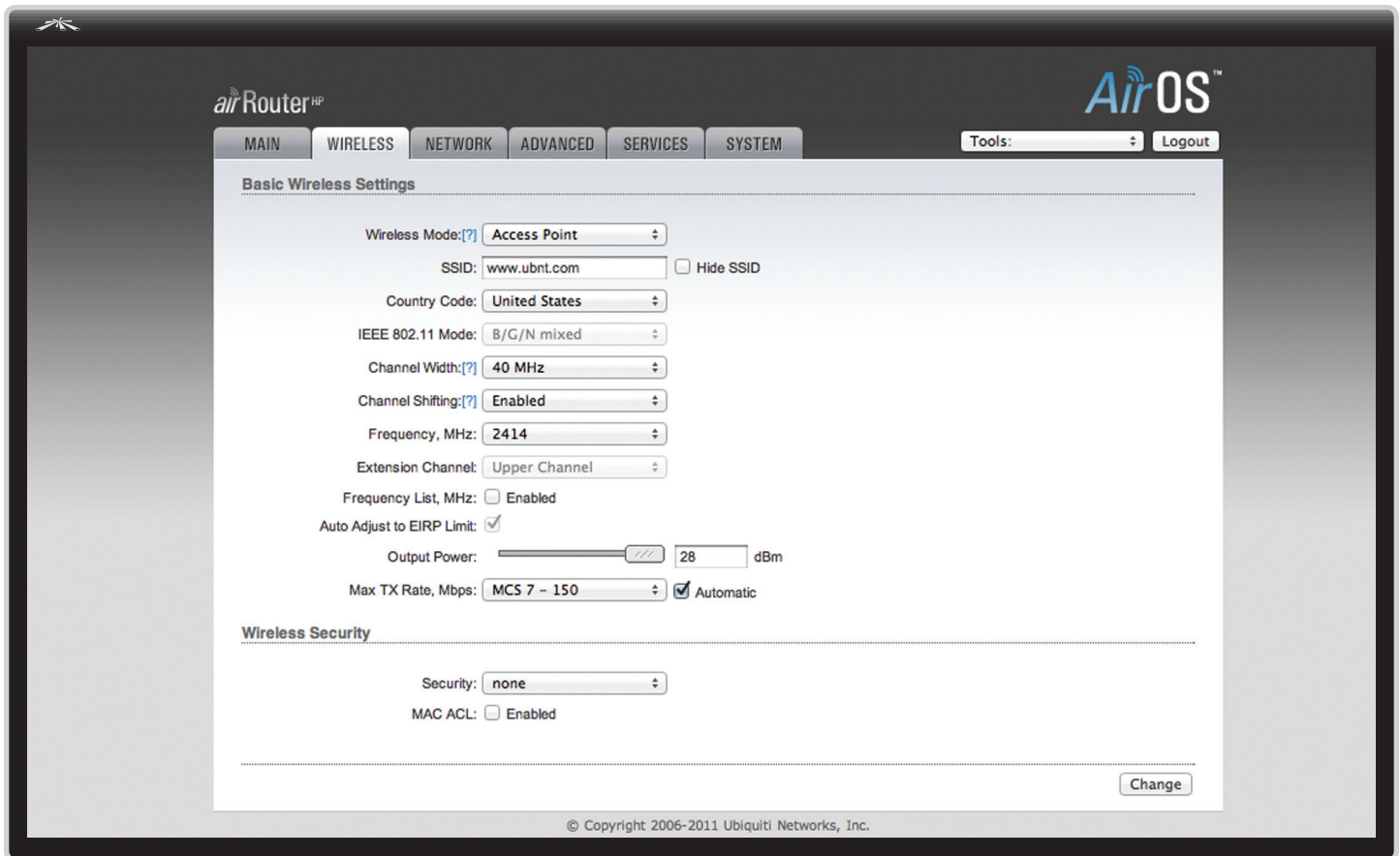
When logging is enabled (*Services > System Log > Enable Log*) this option lists all registered system events. By default, logging isn't enabled.

```

System Log
May 19 12:38:05 syslogd started: BusyBox v1.11.2
May 19 12:38:05 init: starting pid 15715, tty '/dev/null': '/usr/bin/ivewent -s'
May 19 12:38:05 init: starting pid 15711, tty '/dev/null': '/bin/dropbear -F -d /etc/persistent/dropbea
May 19 12:38:05 init: starting pid 15712, tty '/dev/null': '/sbin/npcclient -n -s -o 0 -l -h pool.ntp.o
May 19 12:38:05 init: starting pid 15713, tty '/dev/null': '/bin/hostapd /etc/aal.cfg'
May 19 12:38:05 dnsmasq[15709]: started, version 2.47 cachesize 150
May 19 12:38:05 dnsmasq[15709]: compile time options: IPV6 GNU-getopt no-DBus no-118N TFTP
May 19 12:38:05 dnsmasq[15709]: DHCP, IP range 192.168.26.2 -- 192.168.26.254, lease time 10m
May 19 12:38:05 dnsmasq[15709]: no servers found in /etc/resolv.conf, will retry
May 19 12:38:05 wireless: ath0 Set Mode:Master
May 19 12:38:06 dnsmasq[15709]: read /etc/hosts - 1 addresses
May 19 12:38:06 dropbear[15711]: Not backgrounding
May 19 12:38:11 hostapd: ath0: STA 00:16:cb:ba:ad:f8 IEEE 802.11: associated
May 19 12:38:11 wireless: ath0 Registered node:00:16:CB:BA:AD:F8
May 19 12:38:13 dnsmasq[15709]: reading /etc/resolv.conf
May 19 12:38:13 dnsmasq[15709]: using nameserver 209.18.47.62#53
May 19 12:38:13 dnsmasq[15709]: using nameserver 209.18.47.61#53
May 19 12:38:13 dnsmasq[15709]: DHCPREQUEST(eth0) 192.168.26.192 00:1b:b9:5d:b9:59
May 19 12:38:13 dnsmasq[15709]: DHCPACK(eth0) 192.168.26.192 00:1b:b9:5d:b9:59 raquel-rm
May 19 12:38:13 hostapd: ath0: STA 00:16:cb:ba:ad:f8 WPA: pairwise key handshake completed (RSN)
May 19 12:38:15 dnsmasq[15709]: DHCPREQUEST(eth0) 192.168.26.193 00:16:cb:ba:ad:f8
May 19 12:38:15 dnsmasq[15709]: DHCPACK(eth0) 192.168.26.193 00:16:cb:ba:ad:f8
May 19 12:38:18 hostapd: ath0: STA 90:27:e4:f6:34:43 IEEE 802.11: associated
May 19 12:38:18 wireless: ath0 Registered node:90:27:E4:F6:34:43
May 19 12:38:18 hostapd: ath0: STA 90:27:e4:f6:34:43 WPA: pairwise key handshake completed (RSN)
May 19 12:38:20 dnsmasq[15709]: DHCPREQUEST(eth0) 192.168.26.223 90:27:e4:f6:34:43
May 19 12:38:20 dnsmasq[15709]: DHCPACK(eth0) 192.168.26.223 90:27:e4:f6:34:43
  
```

**Clear** Deletes all entries in the system log.

**Refresh** Updates System Log content.



## Chapter 5: Wireless Tab

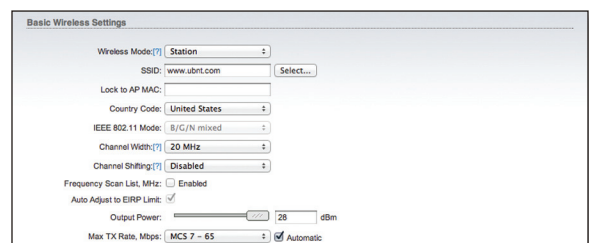
The *Wireless* tab contains everything needed by the operator to set up the wireless part of the link. This includes device wireless mode, SSID, country settings, channel and frequency settings, data rates, and wireless security.

### Basic Wireless Settings

The general wireless settings, such as wireless mode, wireless network name (SSID), country code, 802.11 mode, output power and data rates can be configured in this section.

**Wireless Mode** Allows you to specify the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported on the AirRouter HP: *Station*, *Station WDS*, *Access Point*, *Access Point WDS*.

- **Station** This is a client mode, which connects the AirRouter HP to an Access Point. In *Station* mode, the AirRouter HP acts as the subscriber Station while connecting to the Access Point. The SSID of the Access Point is used and all the traffic to/from the network devices connected to the Ethernet interface is forwarded.



Subscriber Station uses the arpnat technique which may result in a lack of transparency while passing-through broadcast packets in bridge mode.

- **Station WDS** WDS stands for Wireless Distribution System. Station WDS should be used while connecting to an Access Point that is operating in WDS mode. This mode is compatible with WPA/WPA2 encryption.

Station WDS mode enables packet forwarding at the Layer 2 level.

The benefit of Station WDS is improved performance and faster throughput. Station WDS - Bridge mode is fully transparent for all Layer 2 protocols.

The screenshot shows the 'Basic Wireless Settings' interface with 'Wireless Mode' set to 'Station WDS'. Other settings include SSID: www.ubnt.com, Country Code: United States, IEEE 802.11 Mode: B/G/N mixed, Channel Width: 20 MHz, Channel Shifting: Disabled, Frequency Scan List: Enabled, Auto Adjust to EIRP Limit: checked, Output Power: 28 dBm, and Max TX Rate: MCS 7 - 65 Automatic.

- **Access Point** This is 802.11 *Access Point* mode.

The screenshot shows the 'Basic Wireless Settings' interface with 'Wireless Mode' set to 'Access Point'. Other settings include SSID: www.ubnt.com, Country Code: United States, IEEE 802.11 Mode: B/G/N mixed, Channel Width: 20 MHz, Channel Shifting: Disabled, Frequency: Auto, Extension Channel: None, Frequency List: Enabled, Auto Adjust to EIRP Limit: checked, Output Power: 28 dBm, and Max TX Rate: MCS 7 - 65 Automatic.

- **Access Point WDS** This is an 802.11 Access Point which allows for Layer 2 bridging with Station WDS devices using the WDS protocol. Access Point WDS is not fully compatible with WPA/WPA2 encryption.

WDS allows you to bridge wireless traffic between devices which are operating in Access Point mode. Access Point is usually connected to a wired network (Ethernet LAN) allowing wireless connection to the wired network. By connecting Access Points to one another in an extended service set using the WDS, distant Ethernet connections can be bridged into a single LAN.

It is very important that network loops should not be created with either WDS bridges or combinations of wired (Ethernet) connections and WDS bridges. Tree or Star shape network topology should be used in all WDS use-cases (i.e. If Access Point 2 and Access Point 3 are specified as the WDS peers of Access Point 1, Access Point 2 should not be specified as the WDS peer of Access Point 3 and Access Point 3 should not be specified as the WDS peer of Access Point 2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all use cases.

The screenshot shows the 'Basic Wireless Settings' interface with 'Wireless Mode' set to 'Access Point WDS'. It includes a 'WDS Peers' section with three empty input fields. Other settings include SSID: www.ubnt.com, Country Code: United States, IEEE 802.11 Mode: B/G/N mixed, Channel Width: 20 MHz, Channel Shifting: Disabled, Frequency: Auto, Extension Channel: None, Frequency List: Enabled, Auto Adjust to EIRP Limit: checked, Output Power: 28 dBm, and Max TX Rate: MCS 7 - 65 Automatic.



**Note:** *Station WDS* and *Access Point WDS* mode use the WDS protocol which is not defined as the standard thus compatibility issues between equipment from different vendors may arise.



**Note:** When connecting devices in *Access Point WDS* to *Access Point WDS* mode, the WPA/WPA2 security methods will not function. When connecting *Access Point WDS* devices to other *Access Point WDS* device use none or the WEP security method. However, this may compromise the security of your network. When connecting *Station WDS* clients to an *Access Point WDS* device, all security methods are available and work properly.



- **WDS Peers** (Only applicable in *Access Point WDS* mode.) WDS Stations and/or WDS Access Points connected to the AirRouter HP should be specified in this list to create a wireless network infrastructure - Wireless Distribution System. Enter the MAC address of the paired WDS device in the WDS Peer entry field. One MAC address should be specified for a Point-to-Point connection use case. Up to six WDS Peers can be specified for a Point-to-Multi-Point connection use case.

MAC Address	SSID	Device Name

- **Auto** (Only applicable in *Access Point WDS* mode.) Option should be enabled in order to establish WDS connections between Access Points if WDS Peers are not specified. If the *Auto* option is enabled, the AirRouter HP will choose WDS Peers (Access Points) according to the SSID setting. Access Point operating in WDS mode should have the same SSID as the WDS Peer in order to establish the connection automatically while the *Auto* option is enabled. This configuration is also known as repeater mode. AP WDS Auto option can not be selected if any type of WPA or WPA2 security is used as WPA requires different roles on AP configuration (authenticator or supplicant).

Wireless Mode:  Access Point WDS  Auto



**Note:** Access Point operating in WDS mode and all the WDS Peers must operate on the same frequency channel, use the same channel spectrum width and the same security settings.

**SSID** The wireless network name or SSID (Service Set Identifier) used to identify your 802.11 wireless LAN should be specified while operating in Access Point or Access Point WDS mode. All the client devices within range will receive broadcast messages from the access point advertising this SSID.

SSID: www.ubnt.com

While operating in Station or Station WDS mode, you should specify the SSID of the Access Point the AirRouter HP is associated with. There can be several Access Points with an identical SSID. If the SSID is set to "Any" the station will connect to any available Access Point.

- **Select** (Only applicable in *Station* and *Station WDS* mode.) The list of the available Access Points can be retrieved using the **Select** button.

SSID: www.ubnt.com

This control activates *Site Survey* tool which is used for the AP selection. Site Survey will search for the available wireless networks in range on all supported channels and allows you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in the *Wireless Security* section.

Scanned Frequencies: 2.412GHz 2.417GHz 2.422GHz 2.427GHz 2.432GHz 2.437GHz 2.442GHz 2.447GHz 2.452GHz 2.457GHz 2.462GHz

MAC Address	SSID	Device Name	Encryption	Signal / Noise, dBm	Frequency, GHz	Channel
00:0A:95:F1:73:90	Necronomicon	WEP	-50 / -88	2.482	11	
00:22:A4:66:06:D9	ZWIRE831	WEP	-90 / -96	2.412	1	
00:0C:EA:4F:8A:81:29	Evilinkaya	WPA	-43 / -96	2.412	1	
00:25:9C:D2:CE:09	Evilinkaya N	WPA	-28 / -96	2.437	6	
00:1F:F3:C3:B6:66	1st born's Network	WPA2	-79 / -96	2.437	6	

Selectable SSID's must be visible and have compatible channel bandwidth and security settings

Select the Access Point from the list and click the **Select** button for association. This will automatically enter the name of the Access Point into the SSID field and display the appropriate security options in the *Wireless Security* section at the bottom of the page.

Or, to lock the station to a particular Access Point, select the Access Point from the list and click the **Lock to AP** button for association. This will automatically enter the name of the Access Point into the *Lock to AP MAC* field and display the appropriate security options in the *Wireless Security* section at the bottom of the page.

Click **Scan** to refresh the list of available wireless networks. The Site Survey channel scan list can be modified using the Channel Scan List control.

**Hide SSID** (Only applicable in *Access Point* and *Access Point WDS* mode.) When this option is enabled, the SSID (wireless network name) will not be broadcast to wireless stations.

SSID: www.ubnt.com  Hide SSID

**Lock to AP MAC** (Only applicable in *Station* and *Station WDS* mode.) This allows the station to always maintain a connection to a particular Access Point with a specific MAC address. This is useful as sometimes there can be multiple Access Points using the same SSID. With Access Point lock on, the station will lock to a specific MAC Address and not roam between several Access Points with the same SSID.

**Country Code** Each country has their own power level and frequency regulations. To ensure the AirRouter HP operates under the necessary regulatory compliance rules, be sure to select the country where your device will be used. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country.

**IEEE 802.11 Mode** Displays the radio standards used for the AirRouter HP.

**Channel Width** Displays the spectral width of the radio channel. Supported wireless channel spectrum widths:

- **5 MHz** is the channel spectrum with the width of 5 MHz (known as Quarter-Rate mode).
- **10 MHz** is the channel spectrum with the width of 10 MHz (known as Half-Rate mode).
- **20 MHz** is the standard channel spectrum width (selected by default).
- **40 MHz** is the channel spectrum with the width of 40 MHz.
- **Auto 20/40MHz** (Only applicable in *Station* or *Station WDS* mode.) It offers better compatibility.



**Note:** Laptops cannot connect to the AirRouter HP when the channel width is set to 5/10 MHz. Some devices may not be able to connect using the 40 MHz setting.

**Channel Shifting** Enables special channels which have the frequency offset from the standard 802.11b/g/n channels. This is a proprietary Ubiquiti Networks- developed feature. While 802.11 networks have standard channels spaced every 5 MHz apart, channel shifting uses non-standard channels offset from the standard channels. All the channels can be shifted by 5 MHz (in 802.11n) or 2 MHz (in 802.11bgn) from the default central channel frequency. Options include *Enabled* and *Disabled*.



**Note:** Channel shifting is not compatible with legacy products.

The benefits of this are private networking and inherent security. Using channel-shifting, networks instantly become invisible to the millions of Wi-Fi devices in the world.

**Frequency, MHz** (Only applicable in *Access Point* or *Access Point WDS* mode.) Select the wireless channel while operating in *Access Point* mode. Multiple frequency channels are available to avoid interference between nearby access points. The channel list varies depending on the selected country code, IEEE 802.11 mode and Channel Spectrum Width and Channel Shifting option.

**Extension Channel** (Only applicable in *Access Point* or *Access Point WDS* mode with 40 MHz channel width.) Indicates the use of channel bonding that allows the AirMax network to use two channels at once. Using two channels improves the performance of the Wi-Fi connection. It is automatically selected by the system. Options include *Upper Channel* and *Lower Channel*.

**Channel Scan List, MHz** (Only applicable in *Station* or *Station WDS* mode.) This will confine scanning only to the selected channels. The benefits of this are faster scanning as well as filtering out unwanted AP's in the results. Site Survey tool will look for the Access Points in selected channels only. Once enabled, click **Edit** to open the *Channel Scan List* window.

Select the channels that you want to scan and click **OK** or click **Close** to close the window without any selections.

**Output Power** This defines the maximum average transmit output power (in dBm) of the AirRouter HP. The output power can be specified using the slider. When entering the output power value manually, the slider position will change according to the entered value. The transmit power level maximum is limited according to the country regulations. Output power is the output power delivered to the internal antenna.

**Max Data Rate, Mbps** This defines the data rate (in Mbps) at which the device should transmit wireless packets.

You can fix a specific data rate between MCS 0 and MCS 7. It is recommended that you use the *Automatic* option, especially if you are having trouble getting connected or losing data at a higher rate. In this case, the lower data rates will be used automatically. If you select 20 MHz Channel Spectrum width, the maximum data rate is MCS 7 (65Mbps). If you select 40 MHz Channel Spectrum width the maximum data rate is MCS7 (150 Mbps).

**Automatic** When selected, the rate algorithm will select the best data rate, depending on link quality conditions. It is recommended that you use this option, especially if you are having trouble getting connected or losing data at a higher rate. Refer to the *Advanced* section for detailed information about rate algorithms.

## Wireless Security

In *Access Point* and *Access Point WDS* mode, this is where you configure the wireless security settings that will be used by the devices on your wireless network.

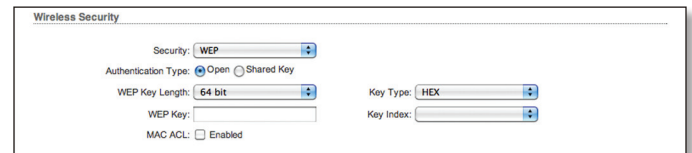
In *Station* or *Station WDS* mode, you will need to match the security settings of the Access Point that the AirRouter HP is associated with.



**Security** The AirRouter HP supports the following wireless security methods:

- **None** Creates an open network without any security.
- **WEP** WEP (Wired Equivalent Privacy) is the oldest and least secure security algorithm. WPA™/WPA2™ security methods should be used when possible.
- **WPA** WPA™ or Wi-Fi Protected Access was developed as a stronger encryption method over WEP.
- **WPA-TKIP** WPA™ (Wi-Fi Protected Access) security mode with TKIP support only. TKIP (Temporal Key Integrity Protocol) uses the RC4 encryption algorithm.
- **WPA-AES** WPA™ (Wi-Fi Protected Access) security mode with AES support only. AES (also known as CCMP) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm.
- **WPA2** WPA2™ was developed to strengthen wireless encryption security and is stronger than WEP and WPA™.
- **WPA2-TKIP** WPA2™ (Wi-Fi Protected Access) security mode with TKIP support only. Temporal Key Integrity Protocol which uses RC4 encryption algorithm.
- **WPA2-AES** WPA2™ (Wi-Fi Protected Access) security mode with AES support only. AES (also known as CCMP) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm. This is the strongest security option available. If all of the wireless devices on your network support this option, it is recommended that you select it.

## WEP



**Authentication Type** One of the following authentication methods should be selected if WEP security is used:

- **Open** The station is authenticated automatically by the AP (selected by default).
- **Shared Key** Station is authenticated after the challenge, generated by the AP.

**WEP Key Length** This determines the length of the WEP security key. Select one of the two key length options:

- **64-bit** This option is selected by default. A 64-bit key is 10 HEX or 5 ASCII characters in length.
- **128-bit** The 128-bit option provides a little more security and is 26 HEX or 13 ASCII characters in length.

**Key Type** Specifies the character format for the WEP key:

- **HEX** Selected by default, this option uses hexadecimal characters. 0-9, A-F or a-f are valid characters.
- **ASCII** ASCII uses the standard English alphabet and numeric characters.

**WEP Key** Enter the WEP encryption key adhering to the selections you made for key length and key type:

Type	HEX	ASCII
64-bit	10 Hexadecimal Characters (0-9, A-F or a-f) Example: <b>00112233AA</b>	5 ASCII Characters Example: <b>ubnt1</b>
128-bit	26 Hexadecimal Characters (0-9, A-F or a-f) Example: <b>00112233445566778899AABCC</b>	13 ASCII characters Example: <b>ubntproducts1</b>

**Key Index** Specifies the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used. The effective key is set by choosing 1, 2, 3 or 4.

## WPA™/WPA2™

The configuration options are the same for all of the WPA™ and WPA2™ options. WPA2-AES is the strongest security method. If all of the wireless devices on your network support this option, it is recommended that you select it.

The screenshot shows the 'Wireless Security' configuration page. The 'Security' dropdown is set to 'WPA'. The 'WPA Authentication' dropdown is set to 'PSK'. The 'WPA Preshared Key' field contains a masked password (\*\*\*\*\*). The 'MAC ACL' checkbox is unchecked, and the 'Show' button is visible.

**WPA Authentication** One of the following WPA™ key selection methods should be specified if WPA™ or WPA2™ security method is used:

- **PSK** Pre-shared Key method (selected by default).
- **EAP** EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in Enterprise networks.

### PSK

This screenshot is identical to the one above, showing the 'Wireless Security' configuration page with 'WPA Authentication' set to 'PSK'.

**WPA Preshared Key** A passphrase needs to be specified when the *Pre-shared Key* method is selected. The pre-shared key is an alpha-numeric password between 8 and 63 characters long. Click *Show* to see the actual characters being typed.

See “**MAC ACL**” on page 17 for more information on this option.

### EAP

#### EAP - Station Mode

The screenshot shows the 'Wireless Security' configuration page. The 'Security' dropdown is set to 'WPA'. The 'WPA Authentication' dropdown is set to 'EAP-TTLS'. The 'WPA Anonymous Identity' field is empty. The 'WPA User Name' and 'WPA User Password' fields are also empty. The 'Show' button is visible.

**WPA Anonymous Identity** (Only applicable in *Station* or *Station WDS* mode with EAP-TTLS.) Identification credential (also known as identity) used by the supplicant for EAP authentication.

**WPA User Name** (Only applicable in *Station* and *Station WDS* mode.) Identification credential (also known as anonymous identity) used by the supplicant for EAP tunneled authentication (EAP-TTLS) in unencrypted form.

**WPA User Password** (Only applicable in *Station* and *Station WDS* mode.) Password credential used by the supplicant for EAP authentication.

#### EAP - Access Point Mode

The screenshot shows the 'Wireless Security' configuration page. The 'Security' dropdown is set to 'WPA'. The 'WPA Authentication' dropdown is set to 'EAP'. The 'RADIUS Server IP' field is empty. The 'RADIUS Server Port' field is set to '1812'. The 'RADIUS Server Secret' field contains a masked password (\*\*\*\*\*). The 'MAC ACL' checkbox is unchecked, and the 'Show' button is visible.

**Radius Server IP** Specifies the RADIUS Server’s IP address. RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers in order to connect to, and use a network service.

**Radius Server Port** Specifies the RADIUS Server’s UDP port. The most commonly used port is 1812, but that depends on the RADIUS Server you are using.

**Radius Server Secret** Specifies the password. A shared secret is a case-sensitive text string used to validate communication between two RADIUS devices. Click *Show* to see the actual characters being typed.

See “**MAC ACL**” on page 17 for more information on this option.



**Note:** When connecting devices in AP-WDS-to-AP-WDS mode, the WPA/WPA2 security methods will not function. When connecting AP-WDS devices to another AP-WDS device use none or the WEP security method. However, this may compromise the security of your network. In case of connecting STA-WDS clients to an AP-WDS device, all security methods are available and work properly.

## MAC ACL

Wireless Security

Security: WPA2

WPA Authentication: PSK

WPA Preshared Key: \*\*\*\*\*  Show

MAC ACL:  Enabled

Policy: Allow

Add

Remove

**MAC ACL** (Only applicable in *Access Point* and *Access Point WDS* mode) MAC Access Control List (ACL) lets you allow or deny clients connectivity to the AirRouter HP.

MAC ACL:  Enabled

Policy: Allow

Add

Remove



**Note:** The maximum number of MAC ACL entries that can be managed through the AirOS Web Management interface is 32. In order to manage more than 32 entries, read [this guide](#), which explains how to manage more MAC addresses by modifying the configuration file.

When enabled, select one of the policies:

- **Allow** Wireless clients in the list have access to the AirRouter HP. Any wireless clients that have not been added to the list will not have access to the AirRouter HP.
- **Deny** Wireless clients in the list will be denied access to the AirRouter HP. Any wireless client that is not in the list can access the AirRouter HP.
- **Add/Remove** The MAC addresses of the wireless clients can be added and removed to the list using the *Add* and *Remove* buttons.

The MAC addresses of the wireless clients can be added and removed using the **Add** and **Remove** buttons.

Click *Show* to see the actual characters being typed.



**Note:** MAC Access Control should be used in combination with a security method such as WPA™ or WPA2™. It should not be used as the only method of security on your network.

Click **Change** to save the changes.

## Chapter 6: Network Tab

The *Network* tab allows the administrator to set up bridge or routing functionality. The IP configuration is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the *Network* tab to configure IP settings.

### Network Role

The AirRouter HP can operate in the following modes:

- **“Bridge” on page 19**
- **“Router” on page 21**
- **“SOHO Router” on page 27**



**Note:** *SOHO Router* is the default *Network Mode* for the AirRouter HP.

**Network Mode** Specify the operating network mode for the device. There are three modes: *Bridge*, *Router* and *SOHO Router*. The mode depends on the network topology requirements:

- **Bridge** In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation and the broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional firewall settings can be configured for Layer 2 packet filtering and access control in *Bridge* mode.
- **Router** This operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on a different IP subnet. *Router* mode will block broadcasts while it is not transparent.

The AirRouter HP supports Multicast packet pass-through in *Router* mode.

The AirRouter HP can act as DHCP server and use NAT (Network Address Translation) (Masquerading) feature which is widely used by Access Points. NAT will act as the firewall between LAN and WLAN networks. Additional firewall settings can be configured for Layer 3 packet filtering and access control in *Router* mode.

- **SOHO Router** *SOHO* (Small Office/Home Office) Router mode is a derivation of *Router* mode. In *SOHO Router* mode, the Main Ethernet port labeled <...> functions as the WAN port. The WLAN and LAN ports function as the Local Area Network (LAN). This is the default operating mode of the AirRouter HP.

**Disable Network** This option can be used to disable the WLAN, LAN or WAN interface. This setting should be used with caution as no L2 or L3 connection can be established through the disabled interface. It will be impossible to access the AirRouter HP from the wireless/wired network which is connected to the disabled interface. Disable WAN is only applicable while operating in *SOHO Router* mode.

## Bridge

In *Bridge* mode, the AirRouter HP forwards all network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides an efficient and fully transparent network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment and share the same IP address space. WLAN and LAN interfaces form the virtual bridge interface while acting as the bridge ports. The bridge has assigned IP settings for management purposes.

## Bridge > Network Settings

**Bridge IP Address** The device can be set for static IP or can be set to obtain an IP address from the DHCP server it is connected to. One of the IP assignment modes must be selected:

- **DHCP** Choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.

- **DHCP Fallback IP** Enter the IP address for the AirRouter HP to use if a DHCP server is not found.
- **DHCP Fallback Netmask** Enter the netmask for the AirRouter HP to use if a DHCP server is not found.
- **Static** Choose this option to assign the static IP settings for the bridge interface.



**Note:** IP Address and Netmask settings should be consistent with the address space of the network segment where the AirRouter HP resides.

- **IP Address** Enter the IP address of the device while Static Bridge IP Address mode is selected. This IP will be used for AirRouter HP management purposes.
- **Netmask** This is a value which when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where the AirRouter HP resides. 255.255.255.0 (or /24) Netmask is commonly used on many C Class IP networks.
- **Gateway IP** Typically, this is the IP address of the host router which provides the point of connection to the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The AirRouter HP will direct the packets of data to the gateway if the destination host is not within the local network.



**Note:** In *Bridge* mode, the Gateway IP address should be from the same address space (on the same network segment) as the AirRouter HP.

- **Primary DNS IP** Enter the IP address of the Primary DNS (Domain Name System) server.
- **Secondary DNS IP** Enter the IP address of the Secondary DNS (Domain Name System) server. This entry is optional and only used if the primary DNS server is not responding.

**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Spanning Tree Protocol** Multiple interconnected bridges create larger networks using the IEEE 802.1d Spanning Tree Protocol (STP), which is used for finding the shortest path within network and to eliminate loops from the topology.

If enabled, the AirRouter HP Bridge will communicate with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). STP should be turned off (selected by default) when the AirRouter HP is the only bridge on the LAN or when there are no loops in the topology as there is no need for the bridge to participate in the Spanning Tree Protocol in this case.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

IP	Netmask	Comment	Enabled
1.			<input type="checkbox"/>
2.			<input type="checkbox"/>
3.			<input type="checkbox"/>
4.			<input type="checkbox"/>
5.			<input type="checkbox"/>
6.			<input type="checkbox"/>
7.			<input type="checkbox"/>
8.			<input type="checkbox"/>

Save Cancel

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.
- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

## Bridge > VLAN Network Settings

**Enable VLAN** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**VLAN ID** The VLAN ID is a unique value assigned to each VLAN at a single device; every VLAN ID represents a different Virtual Network. In AirOS 5.3.3 VLAN ID range values between 2 and 4094 are allowed. AirOS 5.3.3 only allows for one VLAN ID per device.

**VLAN Network** Defines which network interface will be assigned to the specified VLAN ID.

## Bridge > Firewall Settings

Firewall functionality on the bridge interface can be enabled by selecting **Enable Firewall**. Bridge Firewall rules can be configured, enabled or disabled while using *Firewall* configuration window which opens when you click **Configure**.

Action	Interface	IP Type	Not Source IPMask	Not Src Port	Not Destination IPMask	Not Dst Port	Comment	On
1. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
2. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
3. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
4. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
5. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
6. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
7. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
8. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
9. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
10. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
11. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
12. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
13. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
14. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
15. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
16. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
17. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
18. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
19. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>
20. (DROP)	(ANY)	(IP)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>

Save Cancel

Firewall entries can be specified by using the following criteria:

**Interface** The interface (WLAN or LAN) where filtering of the incoming/passing-through packets are processed.

**IP Type** Sets which particular L3 protocol type (IP, ICMP, TCP, UDP) should be filtered.

**Source IP/Mask** The source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets.

**Src Port** The source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets.

**Destination IP/Mask** The destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to.

**Dst Port** The destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.



**Comment** Field used to enter a brief description of the firewall entry.

**On** Enables or disables the effect of the particular firewall entry. All added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active on the AirRouter HP.

**Not** Can be used for inverting the Source IP/mask, Source Port, Destination IP/mask and Destination Port filtering criteria (i.e. if not is enabled for the specified Destination Port value 443, the filtering criteria will be applied to all the packets sent to any Destination Port except the 443 which is commonly used by HTTPS).

Click **Save** to save your firewall entries or click **Cancel** to discard your changes.

All active firewall entries are stored in the FIREWALL chain of the ebtables filter table, while the device is operating in *Bridge* mode. Please refer to the ebtables manual for a detailed description of the firewall functionality in Bridge mode.

Click **Change** to save the changes made in the *Network* tab.

## Bridge > Static Routes

In this section you can manually add static routing rules to the System Routing Table, this allows you to specify that a specific target IP address (es) passes through a determined gateway. Click **Configure** to add an entry.

	Target Network IP	Netmask	Gateway IP	Comment	On
1.					<input type="checkbox"/>
2.					<input type="checkbox"/>
3.					<input type="checkbox"/>
4.					<input type="checkbox"/>
5.					<input type="checkbox"/>
6.					<input type="checkbox"/>
7.					<input type="checkbox"/>
8.					<input type="checkbox"/>
9.					<input type="checkbox"/>
10.					<input type="checkbox"/>
11.					<input type="checkbox"/>
12.					<input type="checkbox"/>
13.					<input type="checkbox"/>
14.					<input type="checkbox"/>
15.					<input type="checkbox"/>
16.					<input type="checkbox"/>
17.					<input type="checkbox"/>
18.					<input type="checkbox"/>
19.					<input type="checkbox"/>
20.					<input type="checkbox"/>

For each entry you must specify a valid Target Network IP, Netmask, Gateway IP, and optionally a comment. Select **On** to enable the rule. Click **Save** to save your entries or **Cancel** to discard them.

## Router

The role of the LAN and WLAN interface will change depending on the Wireless Mode selected while the AirRouter HP is operating in *Router* mode:

- The wireless interface and all connected wireless clients are considered as part of the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the AirRouter HP is operating in *Access Point* or *Access Point WDS* mode.
- The wireless interface and all of the connected wireless clients are considered part of the external network and all network devices on the LAN side as well as the Ethernet interface itself are considered as part of the internal network when the AirRouter HP is operating in *Station* or *Station WDS* mode.

Wireless/wired clients are routed from the internal network to the external one by default. Network Address Translation (NAT) functionality works the same way.

The screenshot shows the AirRouter HP web interface with the 'Network' tab selected. The 'Network Role' section is visible, showing 'Network Mode' set to 'SOHO Router' and 'Disable Network' set to 'None'. The 'WAN Network Settings' section includes options for 'WAN IP Address' (DHCP selected, IP: 192.168.1.1), 'DHCP Falback IP' (192.168.1.1), 'DHCP Falback NetMask' (255.255.255.0), 'MTU' (1500), 'Enable DMZ' (unchecked), 'Auto IP Alasing' (unchecked), 'IP Alases' (Configure...), and 'Change MAC Address' (unchecked). The 'LAN Network Settings' section includes 'IP Address' (192.168.1.1), 'Netmask' (255.255.255.0), 'Auto IP Alasing' (unchecked), 'IP Alases' (Configure...), 'Enable NAT' (checked), 'Enable NAT Protocol' (SIP, PPTP, FTP, RTSP all checked), 'MTU' (1500), 'Enable DHCP Server' (unchecked), and 'Port Forwarding' (Configure...). The 'VLAN Network Settings' section has 'Enable VLAN' (unchecked). The 'Multicast Routing Settings' section has 'Enable Multicast Routing' (unchecked) and 'Multicast Upstream' (WAN). The 'Firewall Settings' section has 'Enable Firewall' (unchecked, Configure...). The 'Static Routes' section has a 'Static Routes' (Configure...) button. A 'Change' button is at the bottom right. The footer shows '© Copyright 2006-2011 Ubiquiti Networks, Inc.'

## Router > WLAN Network Settings

**IP Address** This is the IP address to be represented by the WLAN interface which is connected to the internal network according to the wireless operation mode described above. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network). This IP address can be used to access the management interface of the AirRouter HP.

**Netmask** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identify the host.

**Enable NAT** Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on the local network while the AirRouter HP is operating in *Access Point* or *Access Point WDS* mode and in the reverse direction in *Station* and *Station WDS* mode.

**Enable NAT Protocol** While NAT is enabled, data packets could be modified in order to allow pass-through to the Router. To avoid packet modification of some specific packets, like: *SIP*, *PPTP*, *FTP*, *RTSP*; uncheck the respective checkbox.

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table, while the device is operating in *Router* mode. Please refer to the iptables tutorial for detailed description of the NAT functionality in *Router* mode.

Static routes should be specified in order for the packets to pass-through the AirRouter HP if NAT is disabled in while operating in *Router* mode.

**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Enable DHCP Server** Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients which will associate to the wireless interface while the AirRouter HP is operating in *Access Point* or *Access Point WDS* mode and assigns IP addresses to clients which will connect to the LAN interface while the AirRouter HP is operating in *Station* or *Station WDS* mode.

Enable DHCP Server:

Range Start:

Range End:

Netmask:

Lease Time:  seconds

- **Range Start/End** This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.
- **Netmask** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identify the host.

- **Lease Time** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensures client operation without interruption, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it acquires a new IP addresses from the DHCP server. The time is expressed in seconds.

**Enable DNS Proxy** The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while the AirRouter HP is in operating in *Router* mode. A valid Primary DNS Server IP needs to be specified for DNS Proxy functionality. The internal network interface IP of the AirRouter HP should be specified as the DNS server in the host configuration in order for the DNS Proxy to be able to get the DNS requests and translate domain names to IP addresses afterwards.

**Port Forwarding** Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network. This is useful for number of applications such as FTP servers, gaming, etc. where different host systems need to be seen using a single common IP address/port.

Port Forwarding rules can be set in the *Port Forwarding* window, which is opened by enabling **Port Forwarding** and then clicking **Configure**.

	Private IP	Private Port	Type	Public Port	Comment	Enabled
1.			TCP			<input type="checkbox"/>
2.			TCP			<input type="checkbox"/>
3.			TCP			<input type="checkbox"/>
4.			TCP			<input type="checkbox"/>
5.			TCP			<input type="checkbox"/>
6.			TCP			<input type="checkbox"/>
7.			TCP			<input type="checkbox"/>
8.			TCP			<input type="checkbox"/>
9.			TCP			<input type="checkbox"/>
10.			TCP			<input type="checkbox"/>
11.			TCP			<input type="checkbox"/>
12.			TCP			<input type="checkbox"/>
13.			TCP			<input type="checkbox"/>
14.			TCP			<input type="checkbox"/>
15.			TCP			<input type="checkbox"/>
16.			TCP			<input type="checkbox"/>
17.			TCP			<input type="checkbox"/>
18.			TCP			<input type="checkbox"/>
19.			TCP			<input type="checkbox"/>
20.			TCP			<input type="checkbox"/>

Save Cancel

Port Forwarding entries can be specified by using the following criteria:

- **Private IP** The IP of the host which is connected to the internal network and needs to be accessible from the external network.
- **Private Port** The TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network.
- **Type** The L3 protocol (IP) type which needs to be forwarded from the internal network.

- **Public Port** The TCP/UDP port of the AirRouter HP which will accept and forward the connections from the external network to the host connected to the internal network.
- **Comment** Enter a brief description of the port forwarding functionality such as FTP server, Web server, or game server.
- **Enabled** Enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in the system configuration file, however only the enabled port forwarding entries are used on the AirRouter HP.

Save your port forwarding entries by clicking **Save** or discard your changes by clicking **Cancel**.

## Router > LAN Network Settings

**LAN IP Address** This is the IP address to be represented by the LAN or WLAN interface which is connected to the external network according to the wireless operation mode described previously. This IP address can be used for routing and device management purposes.

The external network interface can be set for static IP or can be set to obtain an IP address from the DHCP server which should reside in the external network. One of the IP assignment modes must be selected for the external network interface:

- **DHCP** Choose this option to obtain the IP address, Gateway and DNS address dynamically from the external DHCP server.
- **PPPoE** Choose this option to obtain the IP address, Gateway and DNS address dynamically from the external PPPoE server.
- **Static** Choose this option to assign the static IP settings for the external interface.

## DHCP

**DHCP Fallback IP** If the AirRouter HP is set to Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

**DHCP Fallback Netmask** If the AirRouter HP is set to Dynamic IP Address mode (DHCP) and unable to obtain an IP address from a valid DHCP server, it will fall back to the static Netmask listed here.

**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Enable DMZ** The Demilitarized Zone (DMZ) can be enabled and used so that services such as Web Servers, Proxy Servers, and E-mail Servers can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with NAT functionality as an alternative to Port Forwarding but DMZ opens all ports of the host network device to the external network.

- **DMZ Management Port** Web Management Port for the AirRouter HP (TCP/IP port 80 by default) will be used for the host device if the DMZ Management Port option is enabled.
- **DMZ IP** Enter the IP address of the internal network device and the device will be completely exposed to the external network.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

IP	Netmask	Comment	Enabled
1.			<input type="checkbox"/>
2.			<input type="checkbox"/>
3.			<input type="checkbox"/>
4.			<input type="checkbox"/>
5.			<input type="checkbox"/>
6.			<input type="checkbox"/>
7.			<input type="checkbox"/>
8.			<input type="checkbox"/>

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.

- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

**Change MAC Address** When enabled, the MAC address of the respective interface can be changed. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address; usually used by Cable operators or some WISPs.

## PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers (typically DSL).

Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP. Only the external network interface can be configured as a PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. The broadcast address is used for the PPPoE server discovery and tunnel establishment.

The screenshot shows the 'LAN Network Settings' window with the following options:

- LAN IP Address:  DHCP  PPPoE  Static
- PPPoE Username:
- PPPoE Password:   Show
- PPPoE MTU/MRU: 1492 / 1492
- PPPoE Encryption:
- Enable DMZ:
- Auto IP Aliasing:
- IP Aliases:
- Change MAC Address:

A valid username and password are required for the PPPoE connection:

**PPPoE Username** Username to connect to the server (must match the configured on the PPPoE server).

**PPPoE Password** Password to connect to the server (must match the configured on the PPPoE server).

**Show** Check this box to display the PPPoE password characters.

**PPPoE MTU/MRU** The size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for data encapsulation while transferring through the PPP tunnel; (MTU/MRU default value: 1492)

**PPPoE Encryption** Enables the use of MPPE encryption.

The IP address of the PPP interface will be displayed on the *Main* tab next to the PPP interface statistics if it is obtained through the established PPPoE connection, otherwise a *Not Connected* message will be displayed.

A PPPoE tunnel reconnection routine can be initiated using the **Reconnect** button which is located in the *Main* tab next to the PPP interface statistics.

The screenshot shows the 'LAN Network Settings' window with the following options:

- LAN IP Address:  DHCP  PPPoE  Static
- DHCP Fallback IP: 192.168.10.1
- DHCP Fallback NetMask: 255.255.255.0
- Enable DMZ:
- DMZ Management Port:
- DMZ IP:
- Auto IP Aliasing:
- IP Aliases:
- Change MAC Address:

**Enable DMZ** The Demilitarized Zone (DMZ) can be enabled and used so that services such as Web Servers, Proxy Servers, and E-mail Servers can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with NAT functionality as an alternative to Port Forwarding but DMZ opens all ports of the host network device to the external network.

- **DMZ Management Port** Web Management Port for the AirRouter HP (TCP/IP port 80 by default) will be used for the host device if the DMZ Management Port option is enabled.
- **DMZ IP** Enter the IP address of the internal network device and the device will be completely exposed to the external network.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

The screenshot shows the 'LAN IP Aliases' window with a table for configuring aliases:

IP	Netmask	Comment	Enabled
1.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

Buttons:

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.

- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

**Change MAC Address** When enabled, the MAC address of the respective interface can be changed. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address; usually used by Cable operators or some WISPs.

## Static

IP Address and Netmask settings should be consistent with the address space of the network segment where the AirRouter HP resides. If the IP of the AirRouter HP and the IP of the administrator PC use a different address space, the AirRouter HP will become unreachable (Applicable for Static mode only).

**Netmask** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. A Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identify the host. (Applicable for Static mode only)

**Gateway IP** The IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The AirRouter HP will direct all the packets to the gateway if the destination host is not within the local network. (Applicable for Static mode only)

The Gateway IP address should be from the same address space (on the same network segment) as the AirRouter HP's external network interface (Wireless interface in the *Station* or *Station WDS* mode and the LAN interface in *Access Point* or *Access Point WDS* mode). (Applicable for Static mode only)

**Primary DNS IP** Enter the IP address of the Primary DNS (Domain Name System) server.

**Secondary DNS IP** Enter the IP address of the Secondary DNS (Domain Name System) server. This entry is optional and only used if the primary DNS server is not responding.

**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Enable DMZ** The Demilitarized Zone (DMZ) can be enabled and used so that services such as Web Servers, Proxy Servers, and E-mail Servers can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with NAT functionality as an alternative to Port Forwarding but DMZ opens all ports of the host network device to the external network.

- **DMZ Management Port** Web Management Port for the AirRouter HP (TCP/IP port 80 by default) will be used for the host device if the DMZ Management Port option is enabled.
- **DMZ IP** Enter the IP address of the internal network device and the device will be completely exposed to the external network.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

	IP	Netmask	Comment	Enabled
1.				<input type="checkbox"/>
2.				<input type="checkbox"/>
3.				<input type="checkbox"/>
4.				<input type="checkbox"/>
5.				<input type="checkbox"/>
6.				<input type="checkbox"/>
7.				<input type="checkbox"/>
8.				<input type="checkbox"/>

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.
- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

**Change MAC Address** When enabled, the MAC address of the respective interface can be changed. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address; usually used by Cable operators or some WISPs.

## Router > VLAN Network Settings

**Enable VLAN** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**VLAN ID** The VLAN ID is a unique value assigned to each VLAN at a single device; every VLAN ID represents a different Virtual Network. In AirOS 5.3.3 VLAN ID range values between 2 and 4094 are allowed. AirOS 5.3.3 only allows for one VLAN ID per device.

**VLAN Network** Defines which network interface will be assigned to the specified VLAN ID.

## Router > Multicast Routing Settings

With a multicast design, applications can send one copy of each packet and address it to a group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts which need to receive them. Common routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however the AirRouter HP provides the multicast traffic pass-through functionality.

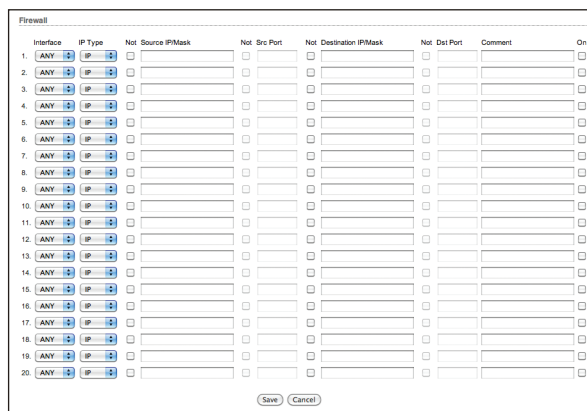


**Enable Multicast Routing** Option enables multicast packet pass-through between internal and external networks while the AirRouter HP is operating in *Router* mode. Multicast intercommunication is based on Internet Group Management Protocol (IGMP).

**Multicast Upstream** Specify the source of Multicast traffic, i.e. defines where multicast traffic comes from.

## Router > Firewall Settings

Firewall functionality on any router interface can be enabled using the *Enable Firewall* option. Router Firewall rules can be configured, enabled or disabled in the *Firewall* configuration window which is opened by clicking **Configure**.



Firewall entries can be specified by using the following criteria:

- **Interface** The interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed.
- **IP Type** Sets which particular L3 protocol type (IP, ICMP, TCP, UDP, P2P) should be filtered.
- **Source IP/Mask** The source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets.
- **Src Port** The source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets.
- **Destination IP/mask** The destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to.
- **Dst Port** The destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.
- **Comment** Field used to enter a brief description of the firewall entry.
- **On** Enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in the system configuration file, however only the enabled firewall entries will be active during AirRouter HP operation.
- **Not** Can be used for inverting the Source IP/mask, Source Port, Destination IP/mask and Destination Port filtering criteria (i.e. if not is enabled for the specified Destination Port value 443, the filtering criteria will be applied to all the packets sent to any Destination Port except the 443 which is commonly used by HTTPS).

Firewall entries can be saved by clicking **Save** or discarded by clicking **Cancel** in the *Firewall* configuration window.

All active firewall entries are stored in the FIREWALL chain of the iptables filter table, while the device is operating in *Router* mode. Please refer to the iptables tutorial for detailed description of the firewall functionality in *Router* mode.

Click **Change** to save the changes made on the *Network* tab.

## Router > Static Routes

In this section you can manually add static routing rules to the System Routing Table, this allows you to specify that a specific target IP address (es) passes through a determined gateway. Click **Configure** to add an entry.

Static Routes					
	Target Network IP	Netmask	Gateway IP	Comment	On
1.					<input type="checkbox"/>
2.					<input type="checkbox"/>
3.					<input type="checkbox"/>
4.					<input type="checkbox"/>
5.					<input type="checkbox"/>
6.					<input type="checkbox"/>
7.					<input type="checkbox"/>
8.					<input type="checkbox"/>
9.					<input type="checkbox"/>
10.					<input type="checkbox"/>
11.					<input type="checkbox"/>
12.					<input type="checkbox"/>
13.					<input type="checkbox"/>
14.					<input type="checkbox"/>
15.					<input type="checkbox"/>
16.					<input type="checkbox"/>
17.					<input type="checkbox"/>
18.					<input type="checkbox"/>
19.					<input type="checkbox"/>
20.					<input type="checkbox"/>

For each entry you must specify a valid Target Network IP, Netmask, Gateway IP, and optionally a comment. Select **On** to enable the rule. Click **Save** to save your entries or **Cancel** to discard them.

## SOHO Router

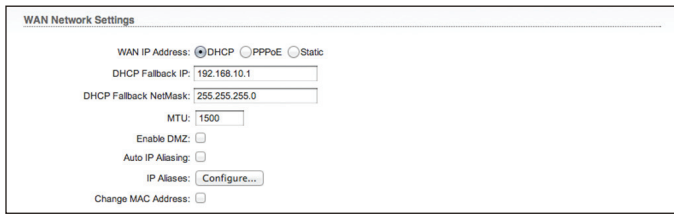
*SOHO* (Small Office/Home Office) *Router* mode is a derivation of *Router* mode. In *SOHO Router* mode, the Main Ethernet port labeled <...> functions as the WAN port. The WLAN and LAN ports function as the Local Area Network (LAN). This is the default operating mode of the AirRouter HP.

The screenshot shows the AirRouter HP web interface with the 'Network' tab selected. The 'Network Role' section shows 'Network Mode' set to 'SOHO Router' and 'Disable Network' set to 'None'. The 'WAN Network Settings' section includes options for 'WAN IP Address' (DHCP, PPPoE, or Static), 'DHCP Fallback IP' (192.168.10.1), 'DHCP Fallback NetMask' (255.255.255.0), 'MTU' (1500), 'Enable DMZ', 'Auto IP Aliasing', 'IP Aliases' (Configure...), and 'Change MAC Address'. The 'LAN Network Settings' section includes 'IP Address' (192.168.1.1), 'Netmask' (255.255.255.0), 'Auto IP Aliasing', 'IP Aliases' (Configure...), 'Enable NAT' (checked), 'Enable NAT Protocol' (SIP, PPTP, FTP, RTSP checked), 'MTU' (1500), 'Enable DHCP Server', and 'Port Forwarding' (Configure...). The 'VLAN Network Settings' section has 'Enable VLAN' (unchecked). The 'Multicast Routing Settings' section has 'Enable Multicast Routing' (unchecked) and 'Multicast Upstream' (WAN). The 'Firewall Settings' section has 'Enable Firewall' (unchecked) and 'Configure...'. The 'Static Routes' section has 'Static Routes' (Configure...). A 'Change' button is located at the bottom right of the page.



**Note:** *SOHO Router* mode only works properly in *Access Point* or *Access Point WDS* mode, since it has not been designed to act as a wireless client.

## SOHO Router > WAN Network Settings



WAN Network Settings

WAN IP Address:  DHCP  PPPoE  Static

DHCP Fallback IP:

DHCP Fallback NetMask:

MTU:

Enable DMZ:

Auto IP Aliasing:

IP Aliases:

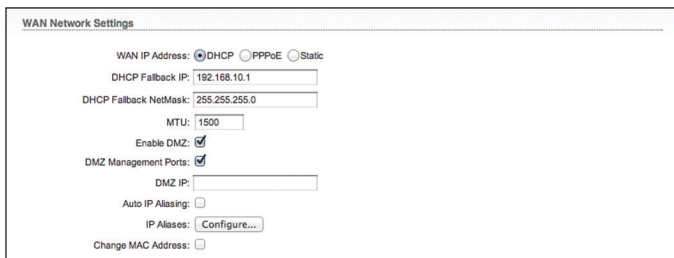
Change MAC Address:

**WAN IP Address** This is the IP address to be represented by the WAN interface which is connected to the external network. This IP address can be used for routing and device management purposes.

The WAN interface can be set for static IP or can be set to obtain an IP address from the DHCP server which should reside on the external network. One of the IP assignment modes must be selected for the external network interface:

- **DHCP** Choose this option to obtain the IP address, Gateway and DNS address dynamically from an external DHCP server.
- **PPPoE** Choose this option to obtain the IP address, Gateway and DNS address dynamically from an external PPPoE server.
- **Static** Choose this option to assign static IP settings for the external interface.

### DHCP



WAN Network Settings

WAN IP Address:  DHCP  PPPoE  Static

DHCP Fallback IP:

DHCP Fallback NetMask:

MTU:

Enable DMZ:

DMZ Management Ports:

DMZ IP:

Auto IP Aliasing:

IP Aliases:

Change MAC Address:

**DHCP Fallback IP** If the AirRouter HP is set to DHCP but is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

**DHCP Fallback Netmask** If the AirRouter HP is set to DHCP but is unable to obtain an IP address from a valid DHCP server, it will fall back to the static Netmask listed here.

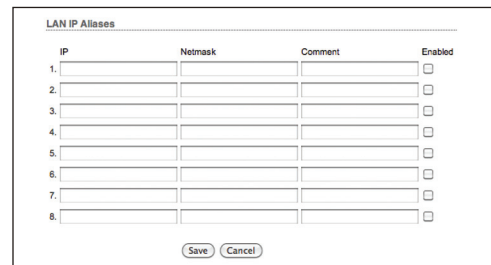
**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Enable DMZ** The Demilitarized Zone (DMZ) can be enabled and used so that services such as Web Servers, Proxy Servers, and E-mail Servers can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with NAT functionality as an alternative to Port Forwarding but DMZ opens all ports of the host network device to the external network.

- **DMZ Management Port** Web Management Port for the AirRouter HP (TCP/IP port 80 by default) will be used for the host device if the DMZ Management Port option is enabled.
- **DMZ IP** Enter the IP address of the internal network device and the device will be completely exposed to the external network.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.



IP	Netmask	Comment	Enabled
1.			<input type="checkbox"/>
2.			<input type="checkbox"/>
3.			<input type="checkbox"/>
4.			<input type="checkbox"/>
5.			<input type="checkbox"/>
6.			<input type="checkbox"/>
7.			<input type="checkbox"/>
8.			<input type="checkbox"/>

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.
- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.



**Change MAC Address** When enabled, the MAC address of the respective interface can be changed. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address; usually used by Cable operators or some WISPs.

## PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems which enables encapsulated data transport. It is commonly used as the medium for subscribers to connect to Internet Service Providers (typically DSL).

Select the IP Address option PPPoE to configure a PPPoE tunnel in order to connect to an ISP. Only the external network interface can be configured as a PPPoE client as all the traffic will be sent via this tunnel. The IP address, Default gateway IP and DNS server IP address will be obtained from the PPPoE server after PPPoE connection is established. The broadcast address is used for the PPPoE server discovery and tunnel establishment.

A valid username and password are required for the PPPoE connection:

**PPPoE Username** Username to connect to the server (must match the configured on the PPPoE server).

**PPPoE Password** Password to connect to the server (must match the configured on the PPPoE server).

**Show** Check this box to display the PPPoE password characters.

**PPPoE MTU/MRU** The size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for data encapsulation while transferring through the PPP tunnel; (MTU/MRU default value: 1492)

**PPPoE Encryption** Enables the use of MPPE encryption.

The IP address of the PPP interface will be displayed on the *Main* tab next to the PPP interface statistics if it is obtained through the established PPPoE connection, otherwise a *Not Connected* message will be displayed.

A PPPoE tunnel reconnection routine can be initiated using the **Reconnect** button which is located in the *Main* tab next to the PPP interface statistics.

**Enable DMZ** The Demilitarized Zone (DMZ) can be enabled and used so that services such as Web Servers, Proxy Servers, and E-mail Servers can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with NAT functionality as an alternative to Port Forwarding but DMZ opens all ports of the host network device to the external network.

- **DMZ Management Port** Web Management Port for the AirRouter HP (TCP/IP port 80 by default) will be used for the host device if the DMZ Management Port option is enabled.
- **DMZ IP** Enter the IP address of the internal network device and the device will be completely exposed to the external network.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

IP	Netmask	Comment	Enabled
1.			<input type="checkbox"/>
2.			<input type="checkbox"/>
3.			<input type="checkbox"/>
4.			<input type="checkbox"/>
5.			<input type="checkbox"/>
6.			<input type="checkbox"/>
7.			<input type="checkbox"/>
8.			<input type="checkbox"/>

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.
- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

**Change MAC Address** When enabled, the MAC address of the respective interface can be changed. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address; usually used by Cable operators or some WISPs.

## Static

WAN Network Settings

WAN IP Address:  DHCP  PPPoE  Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

MTU:

Enable DMZ:

DMZ Management Ports:

DMZ IP:

Auto IP Aliasing:

IP Aliases:

Change MAC Address:

**IP Address** This is the IP address to be represented by the WAN interface which is connected to the external network. This IP address can be used for the routing and device management purposes.

**Netmask** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. A Class C network Netmask uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identify the host.

**Gateway IP** The IP address of the host router which resides on the external network and provides the point of connection to the next hop towards the Internet. This can be a DSL modem, Cable modem, or a WISP gateway router. The AirRouter HP will direct all the packets to the gateway if the destination host is not within the local network.

**Primary DNS IP** Enter the IP address of the Primary DNS (Domain Name System) server.

**Secondary DNS IP** Enter the IP address of the Secondary DNS (Domain Name System) server. This entry is optional and only used if the primary DNS server is not responding.

**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Enable DMZ** The Demilitarized Zone (DMZ) can be enabled and used so that services such as Web Servers, Proxy Servers, and E-mail Servers can still serve the local network and are at the same time isolated from it for additional security. DMZ is commonly used with NAT functionality as an alternative to Port Forwarding but DMZ opens all ports of the host network device to the external network.

WAN Network Settings

WAN IP Address:  DHCP  PPPoE  Static

IP Address:

Netmask:

Gateway IP:

Primary DNS IP:

Secondary DNS IP:

MTU:

Enable DMZ:

DMZ Management Ports:

DMZ IP:

Auto IP Aliasing:

IP Aliases:

Change MAC Address:

- **DMZ Management Port** Web Management Port for the AirRouter HP (TCP/IP port 80 by default) will be used for the host device if the DMZ Management Port option is enabled.
- **DMZ IP** Enter the IP address of the internal network device and the device will be completely exposed to the external network.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

LAN IP Aliases

IP	Netmask	Comment	Enabled
1.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.

- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

**Change MAC Address** When enabled, the MAC address of the respective interface can be changed. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address; usually used by Cable operators or some WISPs.

## SOHO Router > LAN Network Settings

**IP Address** This is the IP address to be represented by the LAN (including WLAN) interface which is connected to the internal network. This IP will be used for the routing of the internal network (it will be the Gateway IP for all the devices connected on the internal network). This IP address is used for the management of the AirRouter HP.

**Netmask** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. A Class C network Netmask uses 24 bits to identify the network (alternative notation “/24”) and 8 bits to identify the host.

**Enable NAT** Network Address Translation (NAT) enables packets to be sent from the external network (WAN) to the local interface IP address and then sub-routed to other client devices residing on the local network while the AirRouter HP is operating in *Access Point* or *Access Point WDS* wireless mode.

**Enable NAT Protocol** While NAT is enabled, data packets could be modified in order to allow pass-through to the Router. To avoid packet modification of some specific packets, like: *SIP*, *PPTP*, *FTP*, *RTSP*; uncheck the respective checkbox.

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table, while the device is operating in *Router* mode. Please refer to the iptables tutorial for detailed description of the NAT functionality in *Router* mode.

Static routes should be specified in order for the packets to pass-through the AirRouter HP if NAT is disabled while operating in *SOHO Router* network mode.

**MTU** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**Enable DHCP Server** Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients connected to the wireless interface and LAN interface while the AirRouter HP is operating in *Access Point* or *Access Point WDS* wireless mode. IP addresses are assigned to clients that connect to the LAN interface while the AirRouter HP is operating in *Station* or *Station WDS* mode.

- **Range Start/End** This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.
- **Netmask** This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. A Class C network Netmask uses 24 bits to identify the network (alternative notation “/24”) and 8 bits to identify the host.
- **Lease Time** The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensures client operation without interruption, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to the client while it will acquire new IP addresses from the DHCP server. The time is expressed in seconds.

**Enable DNS Proxy** The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while AirRouter HP is operating in *SOHO Router* mode. A valid Primary DNS Server IP needs to be specified for DNS Proxy functionality. The internal network interface IP of the AirRouter HP should be specified as the DNS server in the host configuration in order for the DNS Proxy to be able to get DNS requests and translate domain names to IP addresses afterwards.

**Port Forwarding** Port forwarding allows specific ports of the hosts residing in the internal network to be forwarded to the external network (WAN). This is useful for a number of applications such as FTP servers, VoIP, gaming, etc. where different host systems need to be seen using a single common IP address/port.

Port Forwarding rules can be set in the *Port Forwarding* window, which is opened by enabling **Port Forwarding** and then clicking **Configure**.

	Private IP	Private Port	Type	Source IP/mask	Public Port	Comment	Enabled
1.			TCP				<input type="checkbox"/>
2.			TCP				<input type="checkbox"/>
3.			TCP				<input type="checkbox"/>
4.			TCP				<input type="checkbox"/>
5.			TCP				<input type="checkbox"/>
6.			TCP				<input type="checkbox"/>
7.			TCP				<input type="checkbox"/>
8.			TCP				<input type="checkbox"/>
9.			TCP				<input type="checkbox"/>
10.			TCP				<input type="checkbox"/>
11.			TCP				<input type="checkbox"/>
12.			TCP				<input type="checkbox"/>
13.			TCP				<input type="checkbox"/>
14.			TCP				<input type="checkbox"/>
15.			TCP				<input type="checkbox"/>
16.			TCP				<input type="checkbox"/>
17.			TCP				<input type="checkbox"/>
18.			TCP				<input type="checkbox"/>
19.			TCP				<input type="checkbox"/>
20.			TCP				<input type="checkbox"/>

Port Forwarding entries can be specified by using the following criteria:

- **Private IP** The IP of the host which is connected to the internal network and needs to be accessible from the external network.
- **Private Port** The TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network.
- **Type** The L3 protocol (IP) type which needs to be forwarded from the internal network.
- **Source IP/mask** Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system that sends the packets.
- **Public Port** The TCP/UDP port of the AirRouter HP which will accept and forward the connections from the external network to the host connected to the internal network.
- **Comment** Enter a brief description of the port forwarding functionality such as FTP server, Web server, or game server.
- **Enabled** Enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in the system configuration file, however only the enabled port forwarding entries are used on the AirRouter HP.

Save your port forwarding entries by clicking **Save** or discard your changes by clicking **Cancel**.

**Auto IP Aliasing** Automatically generates an IP Address for the corresponding WLAN/LAN interface if enabled. The generated IP address is a unique Class B IP address from the 169.254.X.Y range (Netmask 255.255.0.0) which is intended for use within the same network segment only. Auto IP always starts with 169.254.X.Y while X and Y are last 2 digits from the MAC address of the device (i.e. if the MAC is 00:15:6D:A3:04:FB, Generated unique Auto IP will be 169.254.4.251).

**IP Aliases** IP aliases for the internal and external network interface can be configured. IP Aliases can be specified using the *IP Aliases* configuration window which is opened when you click **Configure**.

	IP	Netmask	Comment	Enabled
1.				<input type="checkbox"/>
2.				<input type="checkbox"/>
3.				<input type="checkbox"/>
4.				<input type="checkbox"/>
5.				<input type="checkbox"/>
6.				<input type="checkbox"/>
7.				<input type="checkbox"/>
8.				<input type="checkbox"/>

- **IP** The alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes.
- **Netmask** The network address space identifier for the particular IP Alias.
- **Comment** Field used for a brief description of the purpose of the alias.
- **Enabled** Enables or disables the particular IP Alias. All added IP Aliases are saved in the system configuration file, however only the enabled IP Aliases are active on the AirRouter HP.

Newly-added IP Aliases can be saved by click the **Save** button or discarded by clicking the **Cancel** button in the *Aliases* configuration window.

## SOHO Router > VLAN Network Settings

**Enable VLAN** Defines the size (in bytes) of the largest protocol data unit the layer can pass on. When using slow links, large packets can cause some delays thereby increasing lag and latency.

**VLAN ID** The VLAN ID is a unique value assigned to each VLAN at a single device; every VLAN ID represents a different Virtual Network. In AirOS 5.3.3 VLAN ID range values between 2 and 4094 are allowed. AirOS 5.3.3 only allows for one VLAN ID per device.

**VLAN Network** Defines which network interface will be assigned to the specified VLAN ID.

## SOHO Router > Multicast Routing Settings

With a multicast design, applications can send one copy of each packet and address it to a group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver. It depends on the network to forward the packets to the hosts which need to receive them. Common routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however the AirRouter HP provides the multicast traffic pass-through functionality.

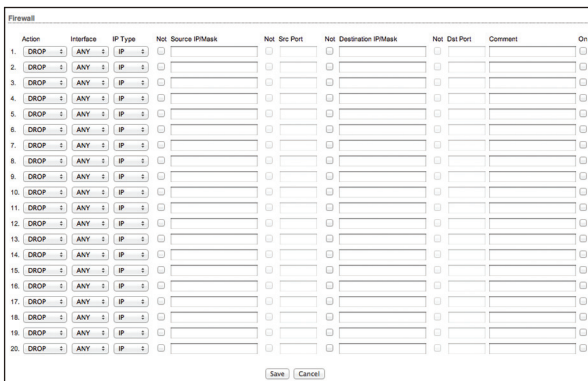


**Enable Multicast Routing** Option enables multicast packet pass-through between internal and external networks while the AirRouter HP is operating in *Router* mode. Multicast intercommunication is based on Internet Group Management Protocol (IGMP).

**Multicast Upstream** Specify the source of Multicast traffic, i.e. defines where multicast traffic comes from.

## SOHO Router > Firewall Settings

Firewall functionality on any router interface can be enabled using the *Enable Firewall* option. Router Firewall rules can be configured, enabled or disabled in the *Firewall* configuration window which is opened by clicking **Configure**.



Firewall entries can be specified by using the following criteria:

- **Interface** The interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed.
- **IP Type** Sets which particular L3 protocol type (IP, ICMP, TCP, UDP, P2P) should be filtered.
- **Source IP/Mask** The source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets.

- **Src Port** The source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets.
- **Destination IP/mask** The destination IP of the packet (specified within the packet header), usually it is the IP of the system which the packet is addressed to.
- **Dst Port** The destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.
- **Comment** Field used to enter a brief description of the firewall entry.
- **On** Enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in the system configuration file, however only the enabled firewall entries will be active during AirRouter HP operation.
- **Not** Can be used for inverting the Source IP/mask, Source Port, Destination IP/mask and Destination Port filtering criteria (i.e. if not is enabled for the specified Destination Port value 443, the filtering criteria will be applied to all the packets sent to any Destination Port except the 443 which is commonly used by HTTPS).

Firewall entries can be saved by clicking **Save** or discarded by clicking **Cancel** in the *Firewall* configuration window.

All active firewall entries are stored in the FIREWALL chain of the iptables filter table, while the device is operating in *Router* mode. Please refer to the iptables tutorial for detailed description of the firewall functionality in *Router* mode.

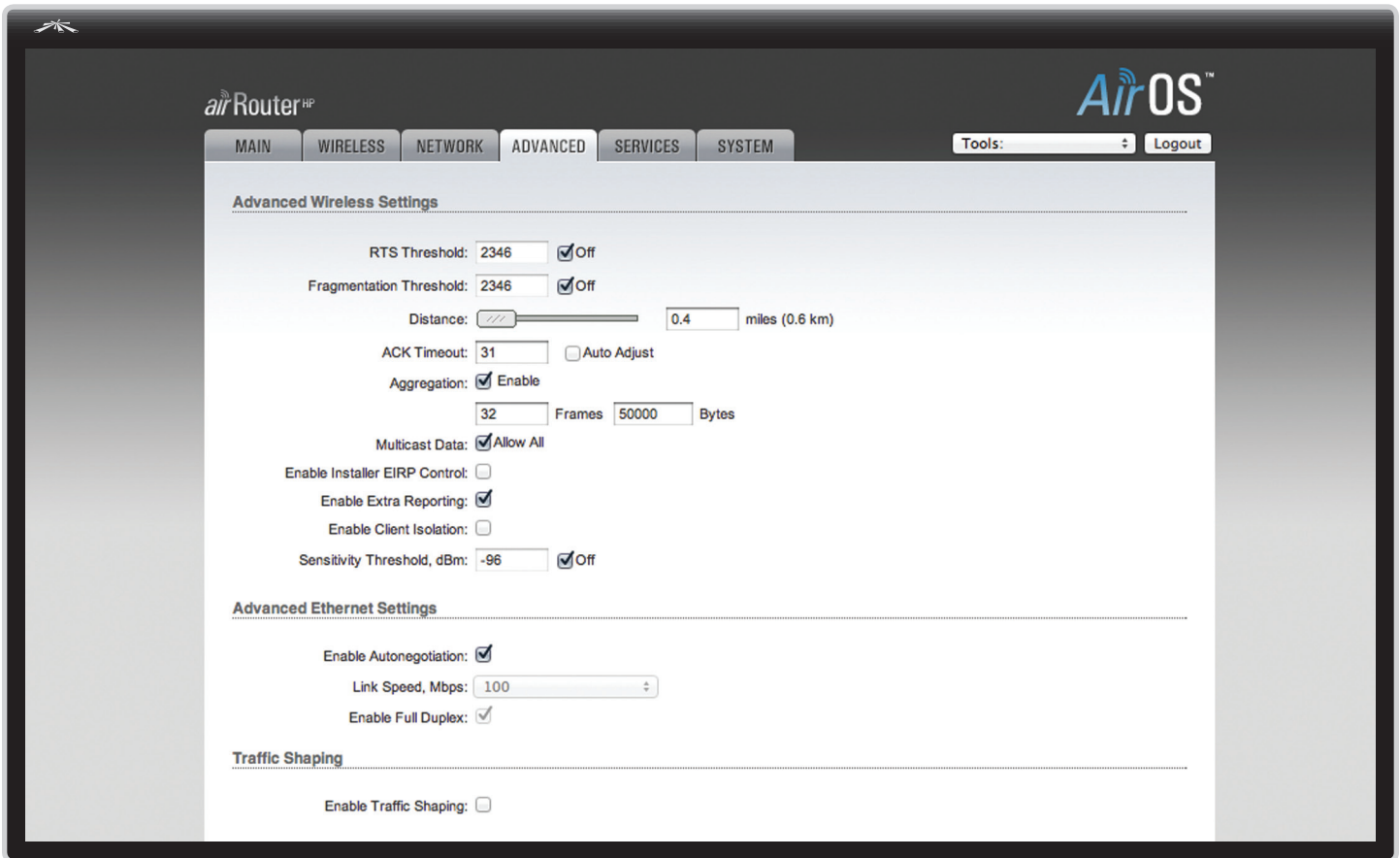
Click **Change** to save the changes made on the *Network* tab.

## SOHO Router > Static Routes

In this section you can manually add static routing rules to the System Routing Table, this allows you to specify that a specific target IP address (es) passes through a determined gateway. Click **Configure** to add an entry.

	Target Network IP	Netmask	Gateway IP	Comment	On
1.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
2.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
3.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
4.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
5.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
6.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
7.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
8.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
9.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
10.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
11.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
12.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
13.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
14.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
15.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
16.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
17.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
18.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
19.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>
20.	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>

For each entry you must specify a valid Target Network IP, Netmask, Gateway IP, and optionally a comment. Select **On** to enable the rule. Click **Save** to save your entries or **Cancel** to discard them.

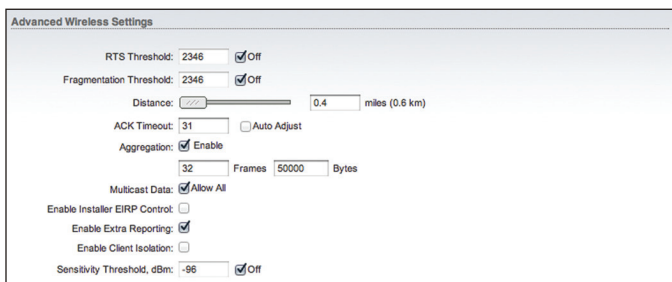


## Chapter 7: Advanced Tab

The *Advanced* tab handles advanced routing and wireless settings. The advanced wireless settings should be used by technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know the effect the changes will have on your AirRouter HP.

### Advanced Wireless Settings

The 802.11n data rates include MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7 for 1x1 chain devices and MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS14, MCS15 for 2x2 chain devices. The ACK timeout has a critical impact on performance in 802.11n outdoor links.



**RTS Threshold** Determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2346 bytes, or word "off". The default value is 2346 which means that RTS is disabled.

RTS/CTS (Request to Send/Clear to Send) are the mechanisms used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2346 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

The system uses a Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is sent only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which provides clear media for the requesting station to send the data. CTS collision control management has a time interval defined during which all other stations hold off transmission and wait until the requesting station finishes transmission.

**Fragmentation Threshold** Specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word "off". Setting the Fragmentation Threshold too low may result in poor network performance.

The use of fragmentation can increase the reliability of frame transmissions. When sending smaller frames, collisions are much less likely to occur. However lower values of the Fragmentation Threshold will result in lower throughput as well. It is recommended that you only make slight modifications or none at all to the Fragmentation Threshold value. The default setting of 2346 is optimum in most wireless network use cases.

The AirRouter HP has a new auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance 802.11n outdoor links. The user also has the ability to enter the value manually, but it's not recommended.

**Distance** Specify the distance value in miles (or kilometers) using the slider or entering the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

**ACK Timeout** Specify the ACK Timeout. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set timeout it re-sends the frame. The performance drops because if too many data frames are re-sent, thus if the timeout is set too short or too long, it will result poor connection and throughput performance.

Changing the ACK Timeout value will change the Distance to the appropriate distance value for the ACK Timeout.

- **Auto Adjust** Control will enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm (used in AirOS v3.4). It is very recommended to use the Auto Adjust option for 802.11n.

If two or more stations are located at a considerably different distance from the Access Point they are associated with, the highest ACK Timeout for the farthest station should be set on the AP side. The AirRouter HP includes an improved ACK Timeout algorithm.

**Aggregation** A part of the 802.11n standard that allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.

- **Frames** Determines the number of frames combined on the new larger frame.
- **Bytes** Determines the size (in Bytes) of the larger frame.

**Multicast Data** This option allows all the Multicast packet pass-through functionality. By default this option is disabled.

**Enable Extra Reporting** Feature will report additional information (i.e. Device Name) in the 802.11 management frames. This information is commonly used for system identification and status reporting in discovery utilities and Router operating systems.

**Enable Client Isolation** This option allows packets only to be sent from the external network to the CPE and vice versa (applicable for Access Point and Access Point WDS mode only). If Client Isolation is enabled, wireless stations connected to the same AP will not be able to interconnect on both the layer 2 (MAC) and layer 3 (IP) level. This is effective for associated stations and WDS peers as well.

**Sensitivity Threshold, dBm** Defines the minimum client signal level accepted by the Access Point, for the client to remain associated. Any client with a signal level lower than that specified will be kicked out. This feature is helpful to maintain good signal levels within associated stations, assuring better overall performance.

- **Off** Clearing the checkbox disables the feature.



## Advanced Ethernet Settings

**Enable Autonegotiation** When enabled, the device will automatically negotiate transmission parameters with the counterpart, such as speed and duplex. In this process, the connected devices first share their capabilities and then choose the fastest transmission mode they both support. If you want to specify the values manually, disable the *Enable Autonegotiation* option and select the values:

- **Link Speed, Mbps** Selects the maximum transmission link speed. There are two options: 10Mbps or 100Mbps. If running extra long Ethernet cables, a link speed of 10Mbps could help to achieve better stability.
- **Enable Full Duplex** Selects the duplex mode; if enabled, the device operates in Full Duplex (allowing bidirectional communication in both directions simultaneously). While disabled, the device operates in Half-Duplex mode (allowing bidirectional communication in both directions, but not simultaneously and only in one direction at a time).

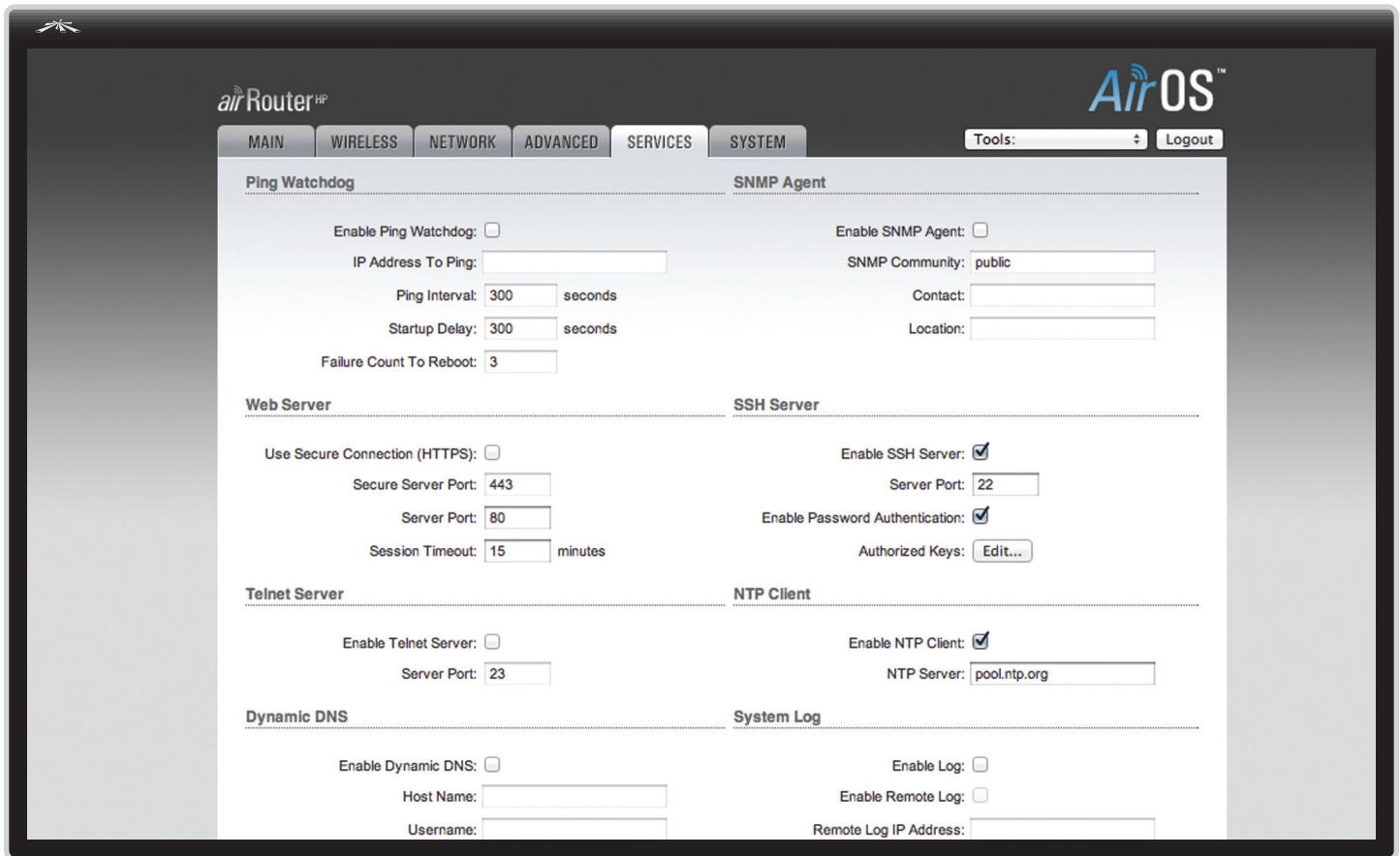
## Traffic Shaping

Wireless Traffic shaping is dedicated to upstream and downstream bandwidth control while looking from the client (connected on the Ethernet interface) perspective.

The traffic can be limited at the AirRouter HP in the upload and download direction based on a user defined rate limit. This is layer 3 QoS.

**Enable Traffic Shaping** This option will enable bandwidth control on the device.

- **Incoming Traffic Limit** Specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from the wireless interface to the Ethernet interface.
- **Incoming Traffic Burst** Specify the data volume (in kilobytes) to which the Incoming Traffic Limit will not be effective afterwards data connection is initiated.
- **Outgoing Traffic Limit** Specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from the Ethernet interface to the wireless interface.
- **Outgoing Traffic Burst** Specify the data volume (in kilobytes) to which the Outgoing Traffic Limit will not be effective after data connection is initiated.



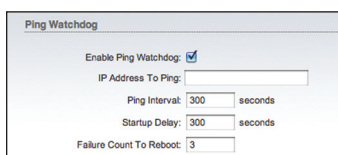
## Chapter 8: Services Tab

The *Services* tab covers the configuration of system management services including: Ping Watchdog, SNMP Agent, Web Server, SSH Server, Telnet Server, NTP Client, Dynamic DNS and System Log.

### Ping Watchdog

Ping Watchdog sets the AirRouter HP to continuously ping a user defined IP address (it can be the Internet gateway for example). If it is unable to ping under the user defined constraints, the AirRouter HP will automatically reboot. This option creates a kind of “fail-proof” mechanism.

Ping Watchdog is dedicated for continuous monitoring of the particular connection to remote host using the Ping tool. The Ping works by sending ICMP “echo request” packets to the target host and listening for ICMP “echo response” replies. If the defined number of replies is not received, the tool reboots the device.



**Enable Ping Watchdog** Enables the Ping Watchdog tool.

- **IP Address To Ping** Specify the IP address of the target host which to be monitored by the Ping Watchdog tool.
- **Ping Interval** Specify time interval (in seconds) between the ICMP “echo requests” are sent by the Ping Watchdog Tool. The default value is 300 seconds.
- **Startup Delay** Specify initial time delay (in seconds) until the first ICMP echo requests are sent by the Ping Watchdog tool. The default value is 300 seconds.  
The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes a considerable amount of time if the device is rebooted.
- **Failure Count to Reboot** Specify the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, the Ping Watchdog tool will reboot the device. The default value is 3.

## SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. The AirRouter HP contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.

The SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve network problems. For the purpose of equipment identification, it is always a good idea to configure SNMP agents with contact and location information:

**Enable SNMP Agent** Enables the SNMP Agent.

- **SNMP Community** Specify the SNMP community string. It is required to authenticate access to MIB objects and functions as an embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access. The AirRouter HP supports SNMP v1. The default SNMP Community is *public*.
- **Contact** Specify the contact who that should be notified in case an emergency situation arises.
- **Location** Specify the physical location of the device.

## Web Server

The following Web Server parameters can be set:

**Use Secure Connection (HTTPS)** If checked Web server will use secure HTTPS mode. HTTPS mode is unchecked by default.

- **Secure Server Port** Defines the Web Server TCP/IP port *Use Secure Connection (HTTPS)* is enabled.

**Server Port** Web Server TCP/IP port setting while using HTTP mode.

**Session timeout** Specifies the maximum timeout before the session expires. Once a session expires, you must login again using the username and password.

## SSH Server

The following SSH Server parameters can be set:

**Enable SSH Server** This option enables SSH access to the AirRouter HP.

- **Server Port** SSH service TCP/IP port setting.
- **Enable Password Authentication** When enabled, you must authenticate using Administrator credentials in order to grant SSH access to the device, otherwise an Authentication Key will be required.
- **Authorized Keys** Click Edit to import a public key file working to get SSH access to the device instead of using an admin password. Click **Browse** to locate and select the key file, then click **Import**. Click **Save** to save your changes or **Close** to discard your changes.

## Telnet Server

The following Telnet Server parameters can be set:

**Enable Telnet Server** This option activates the Telnet access to the AirOS Device.

**Server Port** Telnet service TCP/IP port setting.

## NTP Client

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the AirRouter HP system time. System Time is reported next to the every System Log entry while registering system events if the *Log* option is enabled.

**Enable NTP Client** Enables the AirRouter HP to obtain the system time from a time server on the Internet.

- **NTP Server** Specify the IP address or domain name of the NTP Server.

## System Log

**Enable Log** This option enables the registration routine of the system log messages. By default it is disabled.

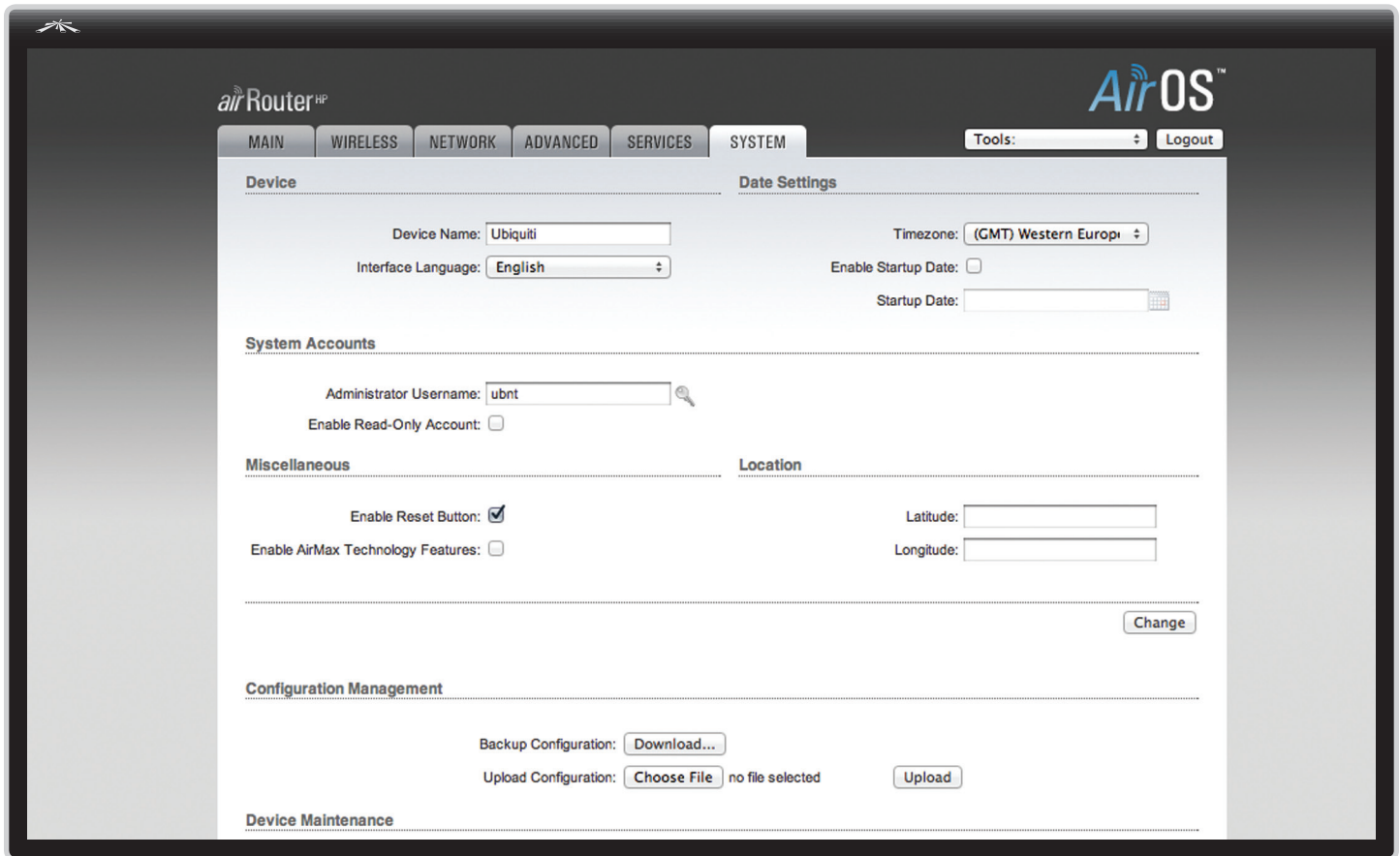
- **Enable Remote Log** Enables the syslog remote sending function while System log messages are sent to a remote server specified in the *Remote Log IP Address* and *Remote Log Port* fields.
  - **Remote Log IP Address** The host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.
  - **Remote Log Port** The TCP/IP port of the host syslog messages should be sent. *514* is the default port for the commonly used system message logging utilities.

Every logged message contains at least a System Time and a Host Name. Usually a particular service name which generates the system event is specified also within the message. Messages from different services have different context and different level of the details. Usually error, warning or informational system service messages are reported, however more detailed Debug level messages can be reported also. The more detailed system messages are reported, the greater volume of log messages will be generated.

## Device Discovery

**Enable Discovery** Enables device discovery, allowing the AirRouter HP to be discovered by other Ubiquiti Networks' devices through the built-in Device Discovery tool.

See **"Discovery" on page 44.**



## Chapter 9: System Tab

The *System* tab contains administrative options. This tab enables the administrator to reboot the device, set it back to factory defaults, upload new firmware, enable AirMax Technology Features (and the *Ubiquiti Logo* tab), backup or update the configuration and configure the administrator account.

### Device

Device Name (Host name) is the system wide device identifier. It is reported by the SNMP Agent to authorized management stations. Device Name will be represented in popular Router Operating Systems registration screens and discovery tools.



**Device Name** Specifies the system identity.

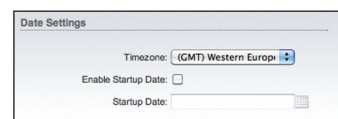
**Interface Language** Allows you to select the language displayed in the management interface. *English* is the default language.

Additional language profiles may be uploaded.

Refer to our wiki page at the following URL:

[www.ubnt.com/wiki/How to import Language Profile](http://www.ubnt.com/wiki/How_to_import_Language_Profile)

### Date Settings



**Timezone** Specifies the timezone according to GMT (Greenwich Mean Time).

**Enable Startup Date** When enabled, you are able to modify the device's startup date.

- **Startup Date** Specifies the device's startup date. You can select a date by clicking the **Calendar** icon or typing it in manually. Type the date in the following format: 2 digit month/2 digit day/4 digit year. An example would be for May 20th, 2010 your would type **05/20/2010**

## System Accounts

In this section you can modify the administrator password to protect your device from unauthorized configuration. The default administrator's password should be changed on the very first system setup:

**Administrator Username** Specifies the name of the system user.

**Key Button** Press this button in order to change the administrator password.

- **Current Password** Enter the current password associated with the administrator account. It is required to change the *Password* or *Administrator Username*.
- **New Password** Enter the new password for the administrator account.
- **Verify New Password** Re-enter the new password for the administrator account.



**Note:** Password length is 8 characters maximum, passwords exceeding 8 characters will be truncated.

**Enable Read-Only Account** Click to enable the read-only account and configure the username and password to protect your device from unauthorized access. The default option is *disabled*.

- **Read-Only Username** Specifies the name of the system user.
- **Key button** Press this button in order to change the Read-only password.
  - **New Password** New password used for read-only administrator authentication should be specified.
  - **Show** Check this to display the read-only password characters you have typed.

**Change** Click to save changes to any of the fields on the *System* tab.

## Miscellaneous

**Enable Reset Button** To prevent accidental device reset to default settings, check to enable the AirRouter HP's physical reset button. Clear to disable the AirRouter HP's physical reset button.

Even if the option is disabled, the device may still reset through the **TFTP Recovery Procedure**.

## Enable AirMax Technology Features

Adds the *Ubiquiti Logo* tab to the AirRouter HP Web Management interface which lists options for enabling, launching and modifying settings for Ubiquiti proprietary features including:

- **AirMax** When enabled, provides superior wireless performance, more clients per Access Point (Access Point) and lower latency.
- **AirSelect** An innovative technology that dynamically changes the wireless channel used in order to avoid interference.
- **AirView** Ubiquiti's spectrum analyzer.

## Location

Latitude and Longitude define the device coordinates; they are used to automatically update device location in AirControl.

## Configuration Management

The AirRouter HP configuration is stored in plain text file (cfg file). Use the *Configuration Management* controls to backup, restore or update the system configuration file:

**Backup Configuration** Click **Download** to download the current system configuration file.

**Upload Configuration** Click **Choose File** to navigate to and select the new configuration file or specify the full path to the configuration file location. Click **Upload** to use a previously downloaded configuration file to the system. The settings of the new configuration will be visible in the *Wireless*, *Network*, *Advanced*, *Services* and *System* tabs of the Web Management Interface.



**Note:** The new configuration is active after clicking **Apply** and the system reboot cycle is completed. The previous system configuration is deleted after you click **Apply**. It is highly recommended to backup the system configuration before uploading the new configuration.

## Device Maintenance

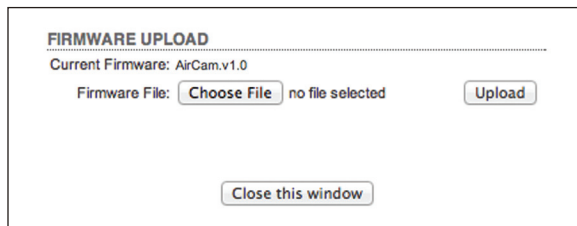
The controls in this section are dedicated for the device maintenance routines: rebooting, resetting, generating of the support information report.



**Firmware Version** Shows the current firmware version.

**Build Number** Displays the build number of the firmware version loaded.

**Update** Click to update the device with new firmware.



### • Firmware Upload

The device firmware update is compatible with all configuration settings. System configurations are preserved while the device is updated with a new firmware version.

- **Current Firmware** Displays the version of the AirOS firmware which is currently operating.
- **Firmware File** Click **Browse** to locate new firmware file. Select the file and click **Open**. Once you've selected a new firmware file, click **Upload** to upload the new firmware to the device. Click **Close this window** to cancel the new firmware upload process.
- **Update** Click the *Update* button to proceed with the firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. The AirRouter HP will be inaccessible until the firmware upgrade routine is completed.
- Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!
- It is highly recommended that you back up the system configuration and the Support Info file before uploading the new configuration.
- **Close this window** At this point, closes the firmware upgrade window if activated. This action will not cancel the firmware upgrade process.

**Reboot** Click *Reboot* in order to initiate the full reboot cycle of the device. Reboot is the same as the hardware reboot which is similar to the power off - power on cycle. The system configuration is not modified after the reboot cycle completes. Any non-applied changes will be lost.

**Reset to Defaults** Use this to reset the AirRouter HP to the factory default settings. This option will reboot the AirRouter HP and all factory default settings will be restored. You may want to use the *Backup Configuration* option to download your current settings before selecting this option.

**Support Info** This will generate a support information file that the Ubiquiti support engineers can use when providing customer support. This file only needs be generated at their request.

## Tools

AirOS on the AirRouter HP includes network administration and monitoring tools that are available on every tab.

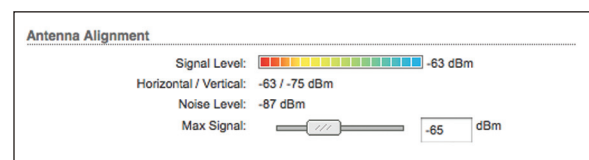
- Align Antenna
- Site Survey
- Ping
- Traceroute
- Speed Test
- AirView



### Align Antenna

The *Align Antenna* utility allows the installer to point and optimize the antenna in the direction of maximum link signal.

Selection of the *Align Antenna* tool will open a new window with signal strength indicator. Window reloads every second displaying the signal strength of the last received packet.



**Signal Level/Horizontal/Vertical** Displays the received wireless signal levels for each polarity, while operating in Station (or Station WDS) mode on MIMO 2x2 devices. Signals Strength is measured in dBm.

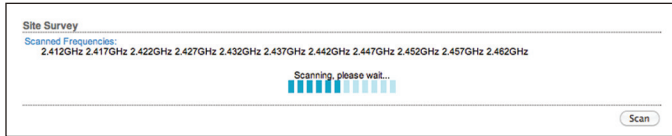
**Noise Level** Value displays the value of the noise level wireless signal was received.

**Max Signal** The *Max Signal* slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations indicating the offset of the maximum indicator value and the scale itself.

## Site Survey

The *Site Survey* tool will search for wireless networks in range on all supported channels while the device is operating in *Access Point* or *Station* mode. In *Station* mode, the channel list can be modified.

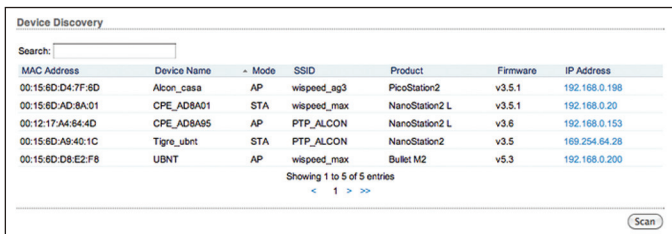
Site Survey reports the MAC Address, SSID, Device Name, Encryption type (if any), Signal Strength/Noise in dBm, Frequency in GHz and the wireless channel of all surrounding Access Points.



**Scan** Refresh the window using the **Scan** button.

## Discovery

The *Device Discovery* tool will scan for all Ubiquiti Networks devices within the network the AirRouter HP is a member of. The search field will automatically filter devices containing specified names or numbers as you type them.



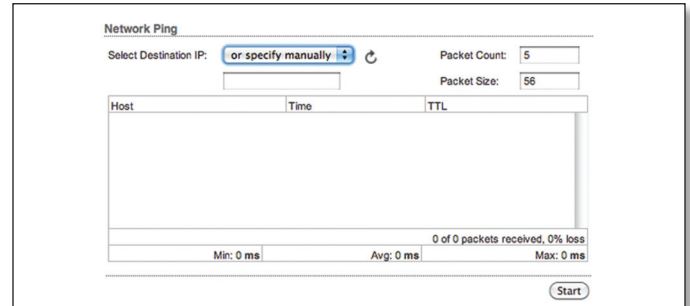
**Device Discovery** Shows device MAC Address, Device Name, Wireless Mode, SSID, Product type, Firmware version and IP Address. To access a device configuration through his Web GUI, click the device's IP Address.

**Scan** Discovery can be updated using the *Scan* button.

## Ping

The *Ping* tool will ping other devices on the network directly from the AirOS device and is used to check the preliminary link quality and packet latency estimation between two network devices using ICMP packets.

### Network Ping



**Select Destination IP** A remote system IP can be selected from the list which is generated automatically or can be specified manually.

**Packet Count** Enter the number of packets to send for the ping test.

**Packet Size** The size of the ICMP packets can be specified in this field.

**Start** The test is started using this button.

Packet loss statistics and latency time evaluation is provided after the test is completed.

## Traceroute

The *TraceRoute* tool allows tracing the hops from the AirRouter HP to a selected outgoing IP address. It should be used for finding the route taken by ICMP packets across the network to the Destination host.



**Destination Host** Enter the IP address of the destination host to which you want to find the route.

**Resolve IP Addresses** Resolution of the IP addresses (symbolically rather than numerically) can be enabled by selecting this option.

**Start** The test is started using this button.



## Speed Test

The *Speed Test* tool allows you to test the connection speed between two Ubiquiti Networks devices that are using firmware version 5.2 or above. It should be used for a preliminary throughput estimation between two network devices.

**Select Destination IP** A remote system IP can be selected from the list, which is generated automatically (Select destination IP) or may be specified manually.

Remote system access credentials (administrator username - User and Password) should be provided for the communication between two AirOS-powered devices. This is required in order to establish the TCP/IP based throughput test.

**Remote WEB port** The remote Web port the AirOS powered device should be specified in order to establish TCP/IP based throughput test (i.e. 443 port should be specified if HTTPS is enabled in the remote system). The ICMP throughput measurement routine will be initiated if the WEB port of the remote system is incorrect.

**Show Advanced Options** Enables additional *Speed Test* tool options. There are 3 options available for the traffic direction while estimating the throughput maximum:

**Direction** There are three directions to choose from:

- **Duplex** Estimates the incoming (Rx) and the outgoing (Tx) throughput at the same time.
- **Receive** Estimates the incoming (Rx) throughput.
- **Transmit** Estimates the outgoing (Tx) throughput.

**Test Results** Displays three result categories:

- **Rx** Displays the estimated incoming throughput.
- **Tx** Displays the estimated out-coming throughput.
- **Total** Displays the aggregated throughput.

## AirView

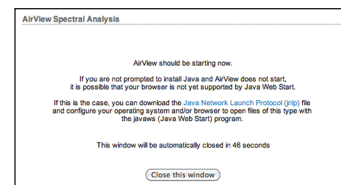
AirView is a Spectrum Analyzer allowing you to see the crowdedness of the radio spectrum. You need to run this tool on a system connected to the AirRouter HP via Ethernet. All wireless connections will be disconnected from the AirRouter HP.

**AirView** Click **Airview** from the Tools menu to launch AirView. On first use, the following window appears.



- **Do NOT warn me about this in the future** Select the check box to bypass this window in future launches of AirView Spectrum Analyzer.

**Launch AirView** Click **Launch Airview** to download the Java Network Launch Protocol (jnlp) file and complete launch of AirView. Java Runtime Environment 1.6 (or above) is required on the client machine to use AirView.



**Close this window** Click *Close this window* to cancel AirView launch and close this window.



**Note:** Launching AirView will terminate all wireless connections on the device.

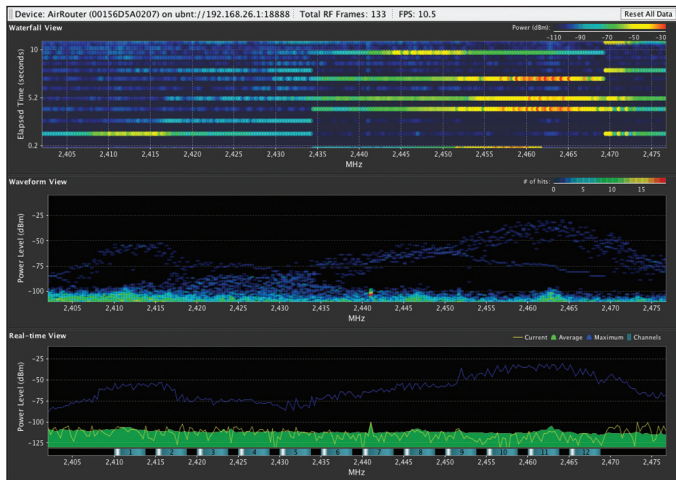
## Main View

**Device** Displays the device name, MAC and IP Address of the device running AirView.

**Total RF Frames** Displays the total number of RF frames gathered for as long as AirView has been running or since the “Reset All Data” button was pressed.

**FPS** Indicates the total number of frames gathered per second. The wider the interval amplitude, the fewer frames per second will be gathered.

**Reset All Data** Press this button to reset all gathered data. Use this function when you want to analyze the spectrum for another place or address.



## View

**Enable Chart Panel 1 (top)** Enable this option to display the top chart, Waterfall or Channel Usage, depending on which you have selected in Preferences. These are time-based graphs showing the aggregate energy collected or Channel Usage over time for each frequency for as long as AirView has been running.

**Enable Chart Panel 2 (middle)** Enable this option to display the middle chart, Waveform. This is a time-based graph showing the aggregate energy collected for each frequency over time. The color of the energy designates its amplitude: colder colors stand for lower energy levels (with blue representing the lowest levels) at that frequency bin, whereas warmer colors (like yellow, orange or red) mean higher energy levels at that frequency bin.

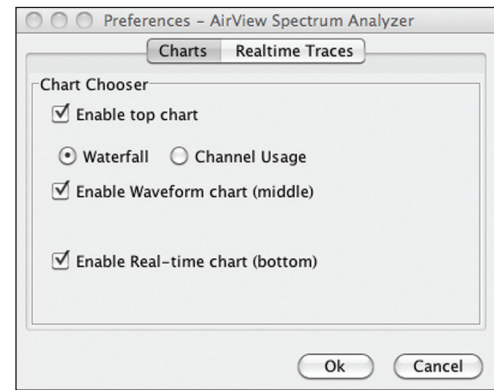
**Enable Chart Panel 3 (bottom)** When enabled, this graph displays a traditional Spectrum Analyzer in which energy (in dBm) is shown in real-time as a function of frequency.

**Clear All Markers** Press to reset all previously assigned markers. Markers are assigned by clicking a point, which corresponds with a frequency, on the third chart.

**Preferences** In this section you can modify AirView Settings, such as enabling or disabling charts, or specifying the frequency interval.

## Preferences

### Charts



**Enable Top Chart** Select the chart to be displayed in the top chart on the main view. There are two options:

- **Waterfall** This is a time-based graph showing the aggregate energy collected over time for each frequency while AirView has been running. The color of energy designates its amplitude. Colder colors stand for lower energy levels (with blue representing the lowest levels) at that frequency bin, whereas warmer colors (like yellow, orange or red) mean higher energy levels at that frequency bin.

The Waterfall View’s legend (top-right corner) provides a numerical guide associating the various colors to power levels (dBm). The low end of that legend (left) is always adjusted to the calculated noise floor, and the high end (right) is set to the highest detected power level since the start of the session.

- **Channel Usage** In this graph, each 2.4GHz Wi-Fi channel is represented by a bar displaying a percentage showing the relative “crowdedness” of that specific channel. This percentage is calculated by analyzing both the popularity and the strength of RF energy in that channel since the start of an AirView session.

**Enable Waveform chart (middle)** Like the Waterfall chart, this is a time-based graph showing the aggregate energy collected for each frequency over time while AirView has been running. The color of the energy designates its amplitude: colder colors stand for lower energy levels (with blue representing the lowest levels) at that frequency bin, whereas warmer colors (like yellow, orange or red) mean higher energy levels at that frequency bin.

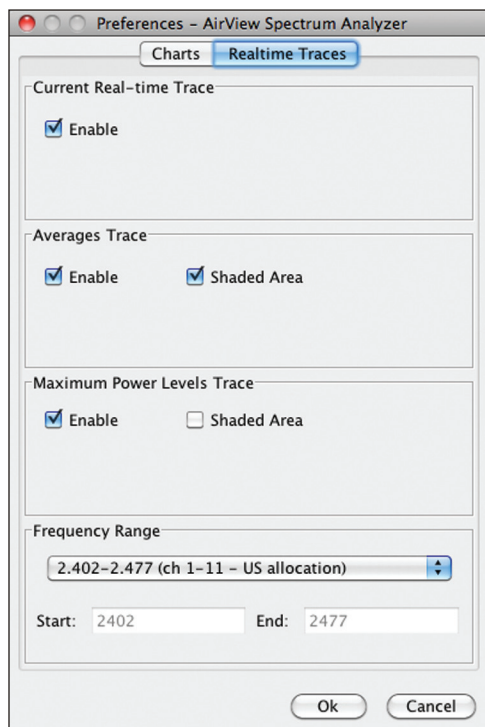
The spectral view over time will essentially display the steady-state RF energy signature of a given environment.

**Enable Real-time chart (bottom)** This graph displays a traditional Spectrum Analyzer in which energy (in dBm) is shown in real time as a function of frequency. There are three traces in this view:

- **Current** (Yellow) Shows the real-time energy seen by the AirRouter HP as a function of frequency.
- **Average** (Green) Shows the running average energy across frequency.
- **Maximum** (Blue) This trace will update and hold maximum power levels across the frequency since the start of an AirView session.

### Realtime Traces

The following settings apply only to the Real-time chart:

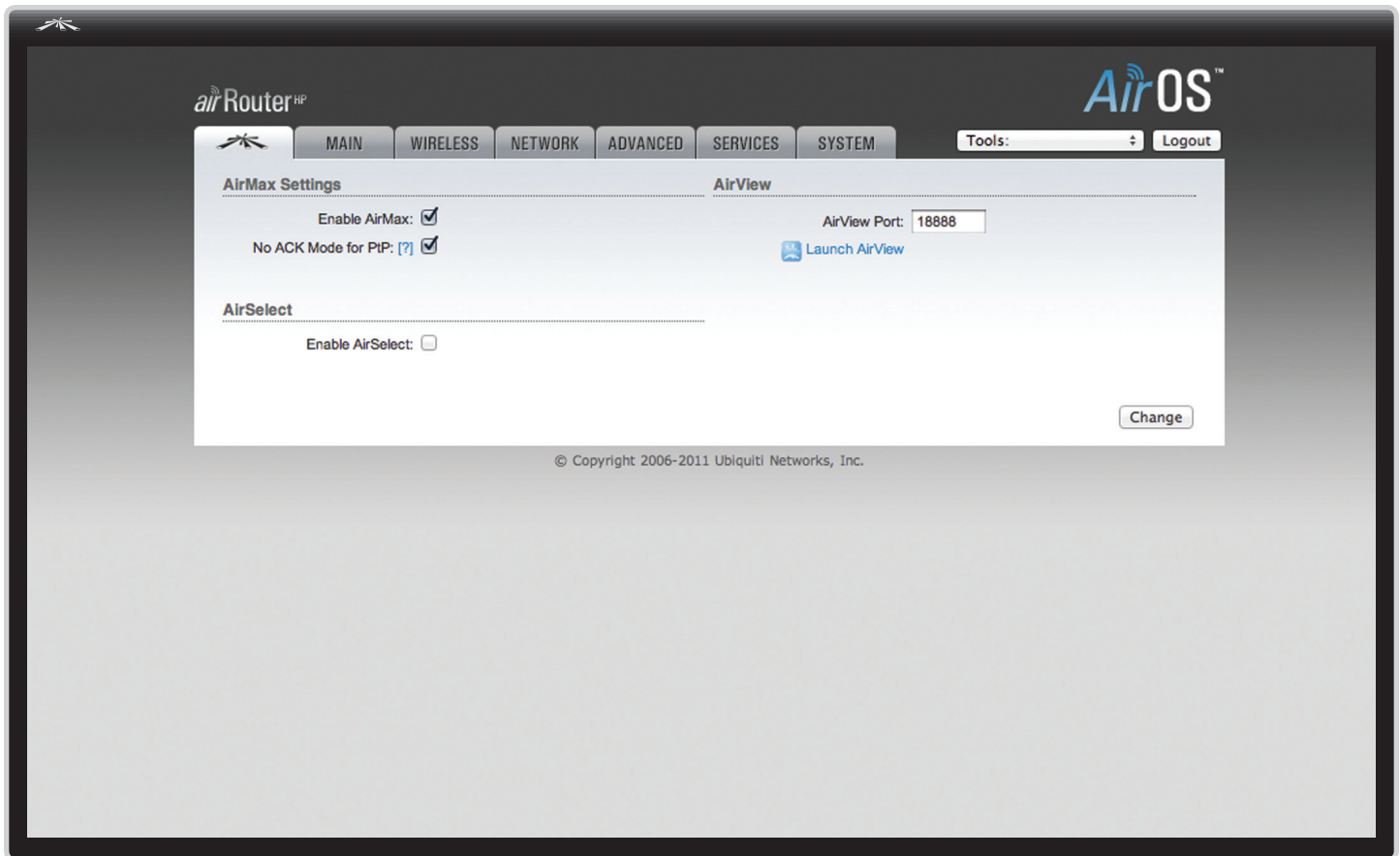


**Current Real-time Trace** When enabled, the real-time trace will be turned on. This is the yellow outline on the *Real-time* chart, which represents real-time power level of each frequency. The refresh speed depends on the FPS.

**Averages Trace** This is the green area on the *Real-time* chart, which represents the average received power level and considers data for as long as AirView has been running. You can disable this graph by unchecking the *Enable* checkbox. You may enable only a green outline, without the shaded area, by unchecking the *Shaded Area* checkbox.

**Maximum Power Trace** This is the blue area on the third chart, which represents the maximum received power level and considers data for as long as AirView has been running. You can disable this graph by unchecking the *Enable* checkbox. You may enable only a blue outline, without the shaded area, by unchecking the *Shaded Area* checkbox.

**Frequency Range** Here you can select the amplitude of the frequencies interval to be scanned. There are some pre-defined ranges for the most popular bands. However, you can specify a custom range according to your needs.



## Chapter 10: Ubiquiti Logo Tab

The *Ubiquiti Logo* tab lists options for enabling, launching and modifying settings for Ubiquiti proprietary features including:

- **AirMax** When enabled, provides superior wireless performance, more clients per Access Point (Access Point) and lower latency.
- **AirSelect** An innovative technology that dynamically changes the wireless channel used in order to avoid interference.
- **AirView** Ubiquiti's spectrum analyzer.



**Note:** The *Ubiquiti Logo* tab is only visible when *Enable AirMax Technology Features* is selected under *System* tab > *Miscellaneous*.

## AirMax Settings

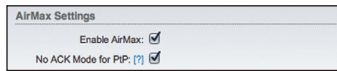
AirMax is Ubiquiti's proprietary Time Division Multiple Access (TDMA) polling technology. AirMax offers better tolerance against interference and increases the maximum number of users associated to an Access Point (Access Point) that is AirMax capable. AirMax works by assigning time slots for each device communication, to avoid the "hidden node" problem, which occurs when a node is visible from a wireless access Access Point, but not from other nodes communicating with the originating Access Point.

While operating in *Access Point* or *Access Point WDS* mode with AirMax enabled, the device only accepts AirMax stations.



**Note:** Disable AirMax for legacy 802.11a/b/g device compatibility.

*AirMax Settings* include:



- **Enable AirMax** This feature is available when the device is in *Access Point* or *Access Point WDS* mode under the *Wireless* tab > *Wireless Mode*. If enabled, the device will operate in AirMax mode, including all its benefits. When AirMax is activated, the device only accepts connections from AirMax stations.



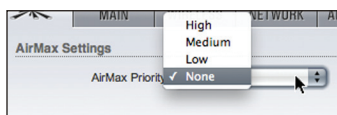
**Note:** When the device is in *Station* or *Station WDS* mode under the *Wireless* tab > *Wireless Mode*, AirMax will be selected automatically when connecting to an AirMax Access Point.

- **No ACK Mode for PtP** Acknowledgment (ACK) timeout settings are limited by device hardware specifications. *No ACK Mode for PtP* should be used in a Point to Point (PtP) situation where actual link distance exceeds hardware ACK timeout limits (17km in 40MHz mode or 51km in 20MHz mode). In all other scenarios, static or automatically-adjusted values should be used (See the *Advanced* tab > *Advanced Wireless Settings* > *ACK Timeout* to adjust ACK timeout settings).



**Important:** While *No ACK Mode for PtP* is enabled, only one station can be connected. To connect more than one station, select *Auto Adjust* mode under the *Advanced* tab > *Advanced Wireless Settings* > *ACK Timeout*.

- **AirMax Priority** This feature (available when the device is in *Station* or *Station WDS* mode under the *Wireless* tab > *Wireless Mode*), defines the amount of time slots (or Airtime) assigned to each client.



- By default the Access Point will give all active clients the same amount of time. However, if the clients are configured with different priorities, the Access Point will give clients more or less time, depending on the priority.

*AirMax Priority* options include:

- None: 1 time slot (Default setting for clients; 1:1 ratio)
- Low: 2 time slots (2:1 ratio)
- Medium: 3 time slots (3:1 ratio)
- High: 4 time slots (4:1 ratio)

Clients with a higher priority have access to more of the Access Point's airtime, providing higher possible throughput and lower latency when sharing with other active clients. For example, if there are 3 clients, 1 set to *None*, 1 set to *Medium*, and 1 set to *High*, the *None* client will get 1 time slot, the *Medium* client will get 3 time slots, and the *High* client will get 4 time slots.



**Note:** AirMax Priority only functions when multiple clients have it enabled.

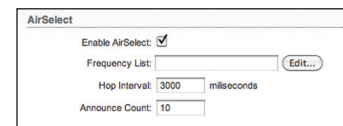
## AirSelect

AirSelect is a technology that avoids interference and increases throughput by dynamically changing the wireless channel by periodically hopping to the least-used channel in the Frequency List (user defined) within a designated time interval (user-defined in *ms*, or milliseconds). Furthermore, AirSelect tracks interference levels on each channel used, hopping to those with the least amount of interference more frequently.

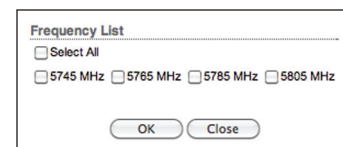


**Note:** AirMax Priority only functions when multiple clients have it enabled.

*AirSelect* options include:



- **Enable AirSelect** Selecting the check box enables AirSelect. Clearing the check box disables AirSelect. When AirSelect is enabled, the Access Point and all associated clients will quickly hop between frequencies attempting to avoid interference.
- **Frequency List** Available when AirSelect is enabled. Clicking **Edit** allows the selection of frequencies that the Access Point will use for AirSelect. Available frequencies will vary based on the Ubiquiti M Series product being configured.

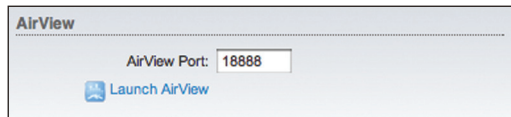


- **Hop Interval** Available when AirSelect is enabled. The duration (in milliseconds) that the Access Point will stay on one frequency before moving to the next. The default value is 3000ms.

- **Announce Count** Available when AirSelect is enabled. *Announce Count* is the number of times between hops the Access Point will announce the next hop information (frequency, etc) to clients. For instance, if the *Hop Interval* is set to 10000ms, and *Announce Count* is set to 10, every 1000ms the Access Point will send an announcement to the clients with upcoming hop information. The larger the time period between *Announce Count* and *Hop Interval*, the higher risk of timing drift (hops not being synchronized), so it is recommended to keep the *Hop Interval* set to every 100ms (or *Announce Count* to 1/100th of *Hop Interval*).

## AirView

**AirView** Click **Launch Airview**.



For more information on configuration and usage, see **"AirView" on page 45.**

## Appendix A: Specifications

---

Dimensions	162 X 132 X 30 mm
Weight	318 g
Ports	(1) 10/100 WAN Ethernet Port (4) 10/100 LAN Ethernet Ports 1 USB 2.0 Port 1 Power Port
Buttons	1 Reset Button
LEDs	4 LAN 1 Main (WAN by default) 1 Internet 1 WLAN (Wireless LAN) 1 Power
Wireless Security	WEP, WPA, and WPA2
Wi-Fi Standards	802.11 b/g/n
Bands	2.4 GHz
Antennas	RP-SMA External Antenna
Power Method	Passive Power over Ethernet 5V DC Input via WAN Port
Operating Temperature	-20 to 60° C
Storage Temperature	-40 to 70° C
Certifications	CE, FCC, IC

## Appendix B: Safety Notices

1. Read, follow, and keep these instructions.
2. Heed all warnings.
3. Only use attachments/accessories specified by the manufacturer.



**WARNING:** Do not use this product in location that can be submerged by water.



**WARNING:** Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

### Electrical Safety Information

1. Compliance is required with respect to voltage, frequency, and current requirements indicated on the manufacturer's label. Connection to a different power source than those specified may result in improper operation, damage to the equipment or pose a fire hazard if the limitations are not followed.
2. There are no operator serviceable parts inside this equipment. Service should be provided only by a qualified service technician.
3. This equipment is provided with a detachable power cord which has an integral safety ground wire intended for connection to a grounded safety outlet.
  - a. Do not substitute the power cord with one that is not the provided approved type. Never use an adapter plug to connect to a 2-wire outlet as this will defeat the continuity of the grounding wire.
  - b. The equipment requires the use of the ground wire as a part of the safety certification, modification or misuse can provide a shock hazard that can result in serious injury or death.
  - c. Contact a qualified electrician or the manufacturer if there are questions about the installation prior to connecting the equipment.
  - d. Protective earthing is provided by Listed AC adapter. Building installation shall provide appropriate short-circuit backup protection.
  - e. Protective bonding must be installed in accordance with local national wiring rules and regulations.



## Appendix C: Warranty

### General Warranty

UBIQUITI NETWORKS, Inc (“UBIQUITI NETWORKS”) represents and warrants that the Products furnished hereunder shall be free from defects in material and workmanship for a period of one (1) year from the date of shipment by UBIQUITI NETWORKS under normal use and operation. UBIQUITI NETWORKS sole and exclusive obligation under the foregoing warranty shall be to repair or replace, at its option, any defective Product that fails during the warranty period. The expense of removal and reinstallation of any item is not included in this warranty.

The foregoing warranty is exclusive and in lieu of all other warranties, express or implied, including the implied warranties of merchantability and fitness for a particular purpose and any warranties arising from a course of dealing, usage or trade practice with respect to the products. Repair or replacement in the manner provided herein shall be the sole and exclusive remedy of Buyer for breach of warranty and shall constitute fulfillment of all liabilities of UBIQUITI NETWORKS with respect to the quality and performance of the Products. UBIQUITI NETWORKS reserves the right to inspect all defective Products (which must be returned by Buyer to UBIQUITI NETWORKS factory freight prepaid).

No Products will be accepted for replacement or repair without obtaining a Return Materials Authorization (RMA) number from UBIQUITI NETWORKS. Products returned without an RMA number will not be processed and will be returned to Buyer freight collect. UBIQUITI NETWORKS shall have no obligation to make repairs or replacement necessitated by catastrophe, fault, negligence, misuse, abuse, or accident by Buyer, Buyer’s customers or any other parties. The warranty period of any repaired or replaced. Product shall not extend beyond its original term.

### Warranty Conditions

The foregoing warranty shall apply only if:

- (I) The Product has not been subjected to misuse, neglect or unusual physical, electrical or electromagnetic stress, or some other type of accident.
- (II) No modification, alteration or addition has been made to the Product by persons other than UBIQUITI NETWORKS or UBIQUITI NETWORKS’ authorized representatives or otherwise approved by UBIQUITI NETWORKS.
- (III) The Product has been properly installed and used at all times in accordance, and in all material respects, with the applicable Product documentation.
- (IV) All Ethernet cabling runs use CAT5 (or above) shielded cabling.

### Disclaimer

UBIQUITI NETWORKS does not warrant that the operation of the products is error-free or that operation will be uninterrupted. In no event shall UBIQUITI NETWORKS be responsible for damages or claims of any nature or description relating to system performance, including coverage, buyer’s selection of products for buyer’s application and/or failure of products to meet government or regulatory requirements.

### Returns

In the unlikely event a defect occurs, please work through the dealer or distributor from which this product was purchased.

## Appendix D: Compliance Information

### Installer Compliance Responsibility

Devices must be professionally installed and it is the professional installer's responsibility to make sure the device is operated within local country regulatory requirements.

### FCC

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operations of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

### RF Exposure Warning

The transceiver described here emits radio frequency energy. Although the power level is low, the concentrated energy from a directional antenna may pose a health hazard. Do not allow people to come closer than 20 cm to the antenna when the transmitter is operating.

Additional information on RF exposure is available on the Internet at [www.fcc.gov/oet/info/documents/bulletins](http://www.fcc.gov/oet/info/documents/bulletins)

L'émetteur-récepteur décrit ici émet de l'énergie de fréquence radio. Bien que le niveau de puissance est faible, l'énergie concentrée à partir d'une antenne directionnelle peut présenter un danger pour la santé. Ne pas permettre aux gens de se rapprocher de 20 cm à l'antenne lorsque l'émetteur est en marche.

Des renseignements supplémentaires sur l'exposition aux RF est disponible sur Internet à [www.fcc.gov/oet/info/documents/bulletins](http://www.fcc.gov/oet/info/documents/bulletins)

### Industry Canada

This Class A digital apparatus complies with Canadian ICES-003. Operation is subject to the following two conditions:

1. This device may not cause interference, and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

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.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 Canada. Son fonctionnement est soumis aux deux conditions suivantes:

1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences susceptibles de provoquer un fonctionnement du dispositif.

Pour réduire le risque d'interférence aux autres utilisateurs, l'antenne type et son gain doivent être choisies de façon que l'équivalent puissance isotrope rayonnée équivalente (pire) n'est pas plus que cela autorisé pour une communication réussie.

### CE Marking

CE marking on this product represents the product is in compliance with all directives that are applicable to it.

### Alert sign! Follows CE marking

Alert sign must be indicated if a restriction on use applied to the product and it must follow the CE marking.



### NB-Identification number (if there is any)

Notified body number is indicated if it is involved in the conformity assessment procedure.



Please check the CE mark on the product label to find out which notified body was involved during assessment.

## RoHS/WEEE Compliance Statement



### English

European Directive 2002/96/EC requires that the equipment bearing this symbol on the product and/or its packaging must not be disposed of with unsorted municipal waste. The symbol indicates that this product should be disposed of separately from regular household waste streams. It is your responsibility to dispose of this and other electric and electronic equipment via designated collection facilities appointed by the government or local authorities. Correct disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about the disposal of your old equipment, please contact your local authorities, waste disposal service, or the shop where you purchased the product.

### Deutsch

Die Europäische Richtlinie 2002/96/EC verlangt, dass technische Ausrüstung, die direkt am Gerät und/oder an der Verpackung mit diesem Symbol versehen ist, nicht zusammen mit unsortiertem Gemeindeabfall entsorgt werden darf. Das Symbol weist darauf hin, dass das Produkt von regulärem Haushaltsmüll getrennt entsorgt werden sollte. Es liegt in Ihrer Verantwortung, dieses Gerät und andere elektrische und elektronische Geräte über die dafür zuständigen und von der Regierung oder örtlichen Behörden dazu bestimmten Sammelstellen zu entsorgen. Ordnungsgemäßes Entsorgen und Recyceln trägt dazu bei, potentielle negative Folgen für Umwelt und die menschliche Gesundheit zu vermeiden. Wenn Sie weitere Informationen zur Entsorgung Ihrer Altgeräte benötigen, wenden Sie sich bitte an die örtlichen Behörden oder städtischen Entsorgungsdienste oder an den Händler, bei dem Sie das Produkt erworben haben.

### Español

La Directiva 2002/96/CE de la UE exige que los equipos que lleven este símbolo en el propio aparato y/o en su embalaje no deben eliminarse junto con otros residuos urbanos no seleccionados. El símbolo indica que el producto en cuestión debe separarse de los residuos domésticos convencionales con vistas a su eliminación. Es responsabilidad suya desechar este y cualesquiera otros aparatos eléctricos y electrónicos a través de los puntos de recogida que ponen a su disposición el gobierno y las autoridades locales. Al desechar y reciclar correctamente estos aparatos estará contribuyendo a evitar posibles consecuencias negativas para el medio ambiente y la salud de las personas. Si desea obtener información más detallada sobre la eliminación segura de su aparato usado, consulte a las autoridades locales, al servicio de recogida y eliminación de residuos de su zona o pregunte en la tienda donde adquirió el producto.

### Français

La directive européenne 2002/96/CE exige que l'équipement sur lequel est apposé ce symbole sur le produit et/ou son emballage ne soit pas jeté avec les autres ordures ménagères. Ce symbole indique que le produit doit être éliminé dans un circuit distinct de celui pour les déchets des ménages. Il est de votre responsabilité de jeter ce matériel ainsi que tout autre matériel électrique ou électronique par les moyens de collecte indiqués par le gouvernement et les pouvoirs publics des collectivités territoriales. L'élimination et le recyclage en bonne et due forme ont pour but de lutter contre l'impact néfaste potentiel de ce type de produits sur l'environnement et la santé publique. Pour plus d'informations sur le mode d'élimination de votre ancien équipement, veuillez prendre contact avec les pouvoirs publics locaux, le service de traitement des déchets, ou l'endroit où vous avez acheté le produit.

### Italiano

La direttiva europea 2002/96/EC richiede che le apparecchiature contrassegnate con questo simbolo sul prodotto e/o sull'imballaggio non siano smaltite insieme ai rifiuti urbani non differenziati. Il simbolo indica che questo prodotto non deve essere smaltito insieme ai normali rifiuti domestici. È responsabilità del proprietario smaltire sia questi prodotti sia le altre apparecchiature elettriche ed elettroniche mediante le specifiche strutture di raccolta indicate dal governo o dagli enti pubblici locali. Il corretto smaltimento ed il riciclaggio aiuteranno a prevenire conseguenze potenzialmente negative per l'ambiente e per la salute dell'essere umano. Per ricevere informazioni più dettagliate circa lo smaltimento delle vecchie apparecchiature in Vostro possesso, Vi invitiamo a contattare gli enti pubblici di competenza, il servizio di smaltimento rifiuti o il negozio nel quale avete acquistato il prodotto.

# Appendix E: Declaration of Conformity

<b>Česky</b> [Czech]	UBIQUITI NETWORKS tímto prohlašuje, že tento UBIQUITI NETWORKS device, je ve shodě se základními požadavky a dále splňuje všechny podmínky ustanovené v směrnici 1999/5/ES.
<b>Dansk</b> [Danish]	Undertegnede UBIQUITI NETWORKS erklærer herved, at følgende udstyr UBIQUITI NETWORKS device, overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
<b>Nederlands</b> [Dutch]	Hierbij verklaart UBIQUITI NETWORKS dat het toestel UBIQUITI NETWORKS device, in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG. Bij deze verklaart UBIQUITI NETWORKS dat deze UBIQUITI NETWORKS device, voldoet aan de essentiële eisen en aan de overige relevante bepalingen van Richtlijn 1999/5/EC.
<b>English</b>	Hereby, UBIQUITI NETWORKS, declares that this UBIQUITI NETWORKS device, is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
<b>Eesti</b> [Estonian]	Käesolevaga kinnitab UBIQUITI NETWORKS seadme UBIQUITI NETWORKS device, vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
<b>Suomi</b> [Finnish]	UBIQUITI NETWORKS vakuuttaa täten että UBIQUITI NETWORKS device, tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
<b>Français</b> [French]	Par la présente UBIQUITI NETWORKS déclare que l'appareil UBIQUITI NETWORKS, device est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE. Par la présente, UBIQUITI NETWORKS déclare que ce UBIQUITI NETWORKS device, est conforme aux exigences essentielles et aux autres dispositions de la directive 1999/5/CE qui lui sont applicables.
<b>Deutsch</b> [German]	Hiermit erklärt UBIQUITI NETWORKS, dass sich diese UBIQUITI NETWORKS device, in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet". (BMW) Hiermit erklärt UBIQUITI NETWORKS die Übereinstimmung des Gerätes UBIQUITI NETWORKS device, mit den grundlegenden Anforderungen und den anderen relevanten Festlegungen der Richtlinie 1999/5/EG. (Wien)
<b>Ελληνική</b> [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ UBIQUITI NETWORKS ΔΗΛΩΝΕΙ ΟΤΙ UBIQUITI NETWORKS device, ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
<b>Magyar</b> [Hungarian]	Alulírott, UBIQUITI NETWORKS nyilatkozom, hogy a UBIQUITI NETWORKS device, megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
<b>Íslenska</b> [Icelandic]	Hér með tilkynni UBIQUITI NETWORKS yfir við UBIQUITI NETWORKS device, er í samræmi við grunnkröfur og allar kröfur, sem gerar eru í tilskipun 1999/5/EC.
<b>Italiano</b> [Italian]	Con la presente UBIQUITI NETWORKS dichiara che questo UBIQUITI NETWORKS device, è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
<b>Latviski</b> [Latvian]	Ar o UBIQUITI NETWORKS deklar, ka UBIQUITI NETWORKS device, atbilst Direktīvas 1999/5/EK prasībām un citiem ar to saistītiem noteikumiem.
<b>Lietuvi</b> [Lithuanian]	UBIQUITI NETWORKS deklaruoja, kad šis UBIQUITI NETWORKS įrenginys atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
<b>Malti</b> [Maltese]	Hawnhekk, UBIQUITI NETWORKS, jiddikjara li dan UBIQUITI NETWORKS device, jikkonforma mal- ti ijjiet essenzjali u ma provvedimenti o rajn rilevanti li hemm fid-Direttiva 1999/5/EC.
<b>Norsk</b> [Norwegian]	UBIQUITI NETWORKS erklærer herved at utstyret UBIQUITI NETWORKS device, er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

<b>Slovensky</b> [Slovak]	UBIQUITI NETWORKS týmto vyhlasuje, že UBIQUITI NETWORKS device, spĺňa základné požiadavky a v etky príslušné ustanovenia Smernice 1999/5/ES.
<b>Svenska</b> [Swedish]	Härmed intygar UBIQUITI NETWORKS att denna UBIQUITI NETWORKS device, står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.
<b>Español</b> [Spanish]	Por medio de la presente UBIQUITI NETWORKS declara que el UBIQUITI NETWORKS device, cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
<b>Polski</b> [Polish]	Niniejszym, firma UBIQUITI NETWORKS oświadczam, że produkt serii UBIQUITI NETWORKS device, spełnia zasadnicze wymagania i inne istotne postanowienia Dyrektywy 1999/5/EC.
<b>Português</b> [Portuguese]	UBIQUITI NETWORKS declara que este UBIQUITI NETWORKS device, está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.

## Appendix F: Contact Information

---

### Ubiquiti Networks Support

Ubiquiti Support Engineers are located in the U.S. and Europe and are dedicated to helping customers resolve software, hardware compatibility, or field issues as quickly as possible. We strive to respond to support inquiries within a 24 hour period.

Email: [support@ubnt.com](mailto:support@ubnt.com)

Phone: 408-942-1153 (9 a.m. - 5 p.m. PST)

### Online Resources

Wiki Page: [www.ubnt.com/wiki](http://www.ubnt.com/wiki)

Support Forum: [www.ubnt.com/forum](http://www.ubnt.com/forum)

Downloads: [www.ubnt.com/support/downloads](http://www.ubnt.com/support/downloads)



91 E. Tasman Drive  
San Jose, CA 95134  
[www.ubnt.com](http://www.ubnt.com)

© 2011 Ubiquiti Networks, Inc. All rights reserved.