UBIQUITI®
NETWORKS

airOS®8

*air*OS®8

**Operating System for Ubiquiti®
airMAX® ac Series Products**

Release Version: 8

USER GUIDE

Table of Contents

Chapter 1: Overview

Introduction

Welcome to airOS® 8 – the latest evolution of the airOS Configuration Interface by Ubiquiti Networks. Sporting an all-new design for improved usability, airOS is the revolutionary operating system for Ubiquiti® airMAX® ac products, offering the following powerful wireless features:

• Access Point PtMP airMAX Mixed Mode

• airMAX ac Protocol Support

• Long-Range Point-to-Point (PtP) Link Mode

• Selectable Channel Width: 10/20/30/40/50/60/80 MHz (channel selection varies by product model)

• Automatic Channel Selection

• Transmit Power Control: Automatic/Manual

• Automatic Distance Selection (ACK Timing)

• Strongest WPA2 security

Usability enhancements include:

• airMagic™ Channel Selection Tool

• Redesigned User Interface

• Dynamic Configuration Changes

• Instant Input Validation

• HTML5 Technology

• Optimization for Mobile Devices

• Detailed Device Statistics

• Comprehensive Array of Diagnostic Tools, including RF Diagnostics and airView® Spectrum Analyzer

This User Guide describes the airOS operating system version 8, which works with all airMAX ac Series products provided by Ubiquiti Networks.

Note: airOS 8 is compatible with airMAX M stations running airOS 6.

Supported Products

airOS 8 supports the following airMAX ac Series products:

• Rocket® ac

• NanoBeam® ac

• PowerBeam™ ac

• LiteBeam® ac

airOS 8 is compatible with airMAX M stations running airOS 6.

For more information, visit **www.ubnt.com**

airOS 8 Network Modes

airOS 8 supports the following network modes:

• Transparent Layer 2 Bridge

• Router

airOS 8 Wireless Modes

airOS 8 supports the following wireless modes:

- Access Point PTP
- Access Point Point-to-MultiPoint (PtMP) airMAX ac
- Access Point PtMP airMAX Mixed
- Station PtP
- Station PtMP

System Requirements

- Microsoft Windows 7, Windows 8, Windows 10; Linux; or Mac OS X
- Web Browser: Mozilla Firefox, Apple Safari, Google Chrome, Microsoft Internet Explorer 11 (or above), or Microsoft Edge

Getting Started

To access the airOS 8 Configuration Interface, perform the following steps:

1. Configure the Ethernet adapter on your computer with a static IP address on the 192.168.1.x subnet (for example, IP address: *192.168.1.100* and subnet mask: *255.255.255.0*).

2. Launch your web browser. Enter **https://192.168.1.20** in the address field. Press **Enter** (PC) or **Return** (Mac).

> Note: airOS 8 does not support legacy products such as AirRouter.

3. Upon initial login, the *Terms of Use* appear on the login screen. Enter **ubnt** in the *Username* and *Password* fields, and select the appropriate choices from the *Country* and *Language* drop-down lists. Check the box next to *I agree to these terms of use*, and click **Login**.

4. Upon subsequent login, the standard login screen appears. Enter **ubnt** in the *Username* and *Password* fields, and click **Login**.
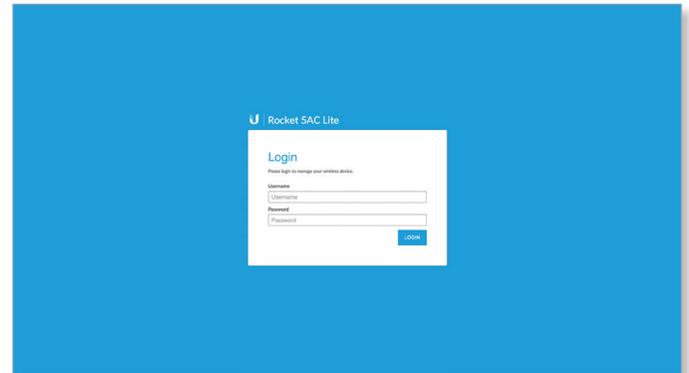
> Note: To enhance security, we recommend that you change the default login on the *System* page. (Changing the password is also required before changes to settings can be saved.) For details on changing login credentials, go to **"System Accounts" on page 41**.

airMAX ac Series Product Verification

The airOS Configuration Interface will display the following logo at the lower edge of the *Dashboard* screen if the product is genuine.

If the authenticity of the Ubiquiti product cannot be verified, airOS will display the error message below. Please contact Ubiquiti at **support@ubnt.com** regarding this product.

Navigation

The airOS 8 Configuration Interface contains three main pages. Each web-based management page is used to configure a specific aspect of the Ubiquiti device, and is accessed by clicking its icon in the navigation bar on the left side of the interface:

Icon	Web-Based Management Page
	Displays the *Dashboard*, containing device and link status, statistics, and network monitoring and RF performance data. For detailed information, refer to **"Dashboard" on page 5**.
	Displays the *Settings* page which contains the following tabs: • **Wireless** Configures wireless settings, including the wireless mode, Service Set Identifier (SSID), channel and frequency, output power, and wireless security. For detailed information, refer to **"Wireless" on page 13**. • **Network** Configures the network operating mode; Internet Protocol (IP) settings; IP aliases; VLANs; packet filtering, bridging, and routing routines; and traffic shaping. For detailed information, refer to **"Network" on page 21**. • **Services** Configures system management services: Ping Watchdog, Simple Network Management Protocol (SNMP), servers (web, SSH, Telnet), Network Time Protocol (NTP) client, Dynamic Domain Name System (DDNS) client, system log, and device discovery. For detailed information, refer to **"Services" on page 35**. • **System** Controls system maintenance routines, including firmware update, date settings, administrator account management, location management, device maintenance, and configuration backup. You can also change the language of the web management interface. For detailed information, refer to **"System" on page 39**.
	Displays the *airMagic* tool, which is used to identify the three most spectrally efficient channels in your system. For detailed information, see **"airMagic" on page 43**.

At the lower left and upper right of the window are icons used to access additional tools and information:

Icon	Web-Based Management Page
	Displays the system log. For details, refer to **"Log" on page 50**.
	Displays a list of network administration and monitoring tools. For details, refer to **"Tools and Information" on page 45**.
	Click this icon to immediately log out of airOS 8.

Help Information

Help information, indicated by *[?]*, is available for selected settings throughout the Configuration Interface. To display the help information, click **[?]**.

WIRELESS MODE [?]

airOS Notifications

Pending Changes

When you make changes to any settings on any page, the following buttons appear at the bottom of the page

TEST CHANGES   REVERT CHANGES   SAVE CHANGES

Use the buttons to perform operations on all unsaved changes. You have three options:

Test Changes   Click **Test Changes** to try changes without saving them. You have two options:

• **Apply** Click **Apply** to save changes.
• **Discard** Click *Discard* to cancel changes.

> Note: If you do not click *Apply* within 180 seconds (the countdown is displayed), the device times out and resumes its earlier configuration.

Revert Changes   Click **Revert Changes** to cancel all changes on all pages.

Save Changes   Click **Save Changes** to immediately apply and save changes.
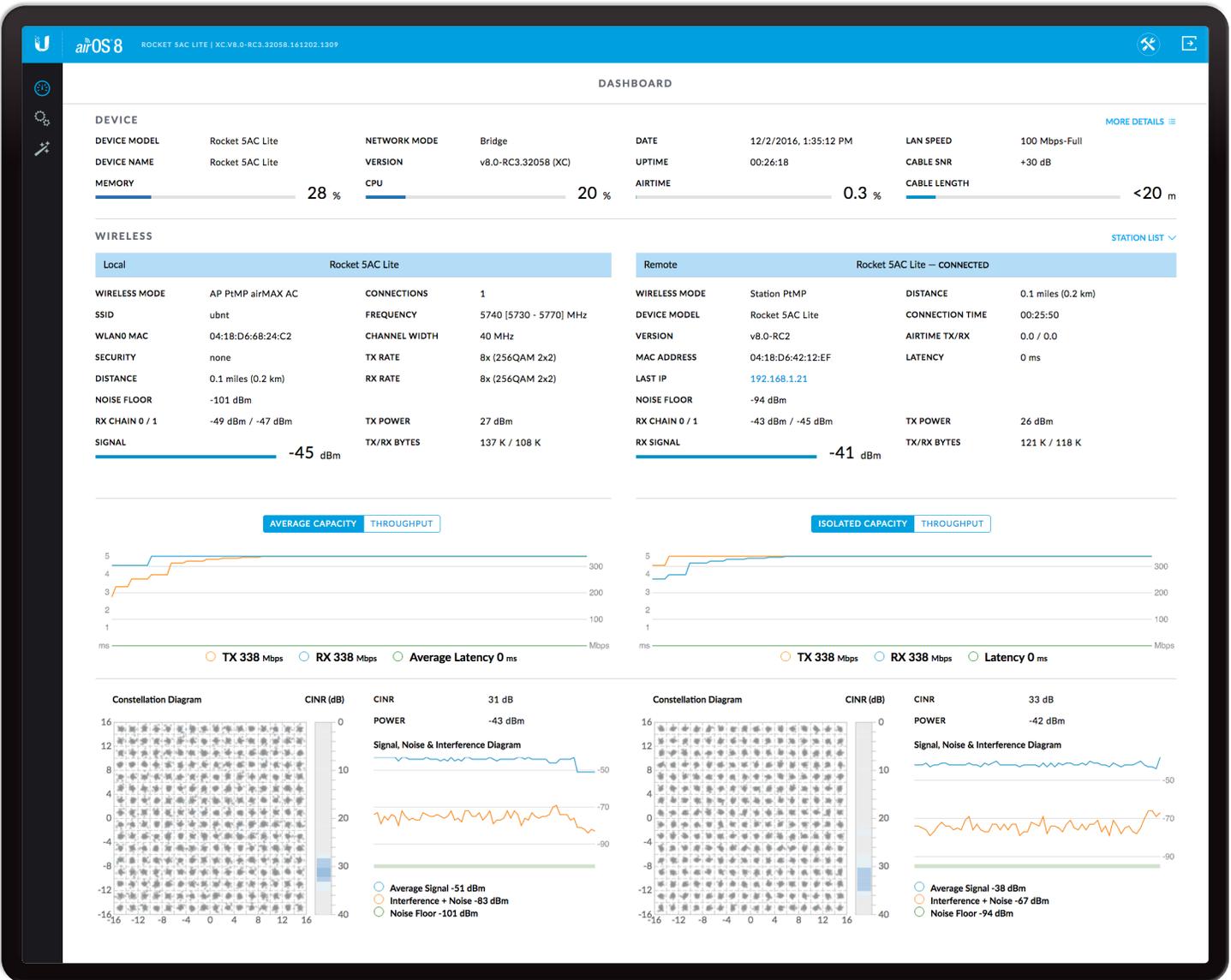
Chapter 2: Dashboard

The *Dashboard* page provides 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.

Device

The *Device* section displays basic identifying and status information on the device.

Device Model Displays the model name of the device.

Device Name Displays the customizable name or identifier of the device. The *Device Name* (also known as host name) is displayed in registration screens and discovery tools.

Memory Displays the percentage of memory currently being used.

Network Mode Displays the network operating mode: *Bridge* or *Router*. The default setting is *Bridge*. Configure the *Network Mode* on the *Network* tab.

Version Displays the airOS firmware version.

CPU Displays the percentage of CPU capacity currently being used.

Date Displays the current system date and time (the format is browser and location-dependent). The system date and time is retrieved from the Internet using NTP (Network Time Protocol). The NTP Client is disabled by default on the *Services* page. The device doesn't have an internal clock, and the date and time may be inaccurate if the NTP Client is disabled or the device isn't connected to the Internet.

Uptime This is the total time the device has been running since the latest reboot (when the device was powered up) or software upgrade. The time is displayed in days, hours, minutes, and seconds.

Airtime Displays the average wireless bandwidth usage (calculated using the sum of all successful and failed transmissions) as a percentage of the maximum theoretical bandwidth utilization.

LAN Speed Displays the Ethernet port mode (speed, duplex mode), such as *1000Mbps-Full* or *100Mbps-Full*.

Cable SNR (Available on non-Rocket Prism devices only.) Displays the cable Signal-to-Noise Ratio (SNR) in dBm. A value of 0 indicates that the cable is not connected or the Ethernet port is down.

Cable Length (Available on non-Rocket Prism devices only.) Displays the length of the cable attached to the device.

Location (Available on Rocket Prism devices only.) Displays the device's location as degrees latitude/longitude and altitude.

GPS Signal (Available on Rocket Prism devices only.) Displays the strength of the GPS signal.

More Details Click **More Details** to display the following additional information:

- **"Interfaces" on page 6**
- **"PPPoE Information" on page 6**
- **"ARP Table" on page 7**
- **"Bridge Table" on page 7**
- **"Routes" on page 7**
- **"Firewall" on page 8**
- **"Port Forward" on page 8**
- **"DHCP Leases" on page 8**

Interfaces

Click **Interfaces** to display the name, MAC address, MTU, IP address, and traffic information for the device's interfaces.

Interface Displays the name of the interface.

MAC Address Displays the MAC address of the interface.

MTU Displays the Maximum Transmission Unit (MTU), which is the maximum frame size (in bytes) that a network interface can transmit or receive. The default is *1500*.

IP Address Displays the IP address of the interface.

RX Bytes Displays the total amount of data (in bytes) received by the interface.

RX Errors Displays the number of receive errors.

TX Bytes Displays the total amount of data (in bytes) transmitted by the interface.

TX Errors Displays the number of transmit errors.

Manage airGateway (Available only from a station connected to an airMAX airGateway.) Click **Manage airGateway** to remotely provision the airGateway.

Close To close the window, click **Close**.

PPPoE Information

(Available if *PPPoE* is enabled in *Router* mode.) Click **PPPoE** to display information on the PPPoE connection if PPPoE has been configured on the *Network* page (for detailed information, see **"PPPoE" on page 25**).

Username Displays the username used to connect to the PPPoE server.

Local IP Address Displays the IP address of the local PPPoE tunnel endpoint.

Remote IP Address Displays the IP address of the remote PPPoE tunnel endpoint.

Primary DNS IP Displays the IP address of the primary DNS server.

Secondary DNS IP Displays the IP address of the secondary DNS server.

Connection Time Displays the total elapsed time of the PPPoE connection.

Bytes Transmitted Displays the total number of bytes transmitted over the PPPoE connection.

Bytes Received Displays the total number of bytes received over the PPPoE connection.

TX/RX Packets Displays the total number of packets transmitted and received.

TX/RX Compression Ratio Displays the compression ratio of transmitted and received data.

Refresh To update the information, click **Refresh**.

Restart Service To restart PPPoE service, click **Restart Service**.

Close To close the window, click **Close**.

ARP Table

Click **ARP Table** to list all entries in the Address Resolution Protocol (ARP) table currently recorded on the device.

ARP is used to associate each IP address to the unique hardware MAC address of each device on the network. It is important to have unique IP addresses for each MAC address or else there will be ambiguous routes on the network.
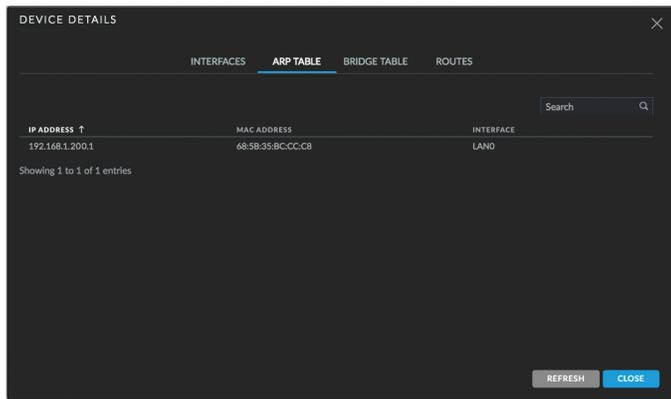
IP Address Displays the IP address assigned to a network device.

MAC Address Displays the MAC address of the device.

Interface Displays the interface that connects to the device.

**Refresh** To update the information, click **Refresh**.

Close To close the window, click **Close**.

Bridge Table

(Available in *Bridge* mode only.) Click **Bridge Table** to display the entries in the system *Bridge Table*.

> 📋 Note: A *bridge* is a logical device used to connect different physical or virtual network interfaces (bridge ports): Wireless, Ethernet, VLAN. A *bridge table* shows a list of all learned MAC addresses for a bridge.
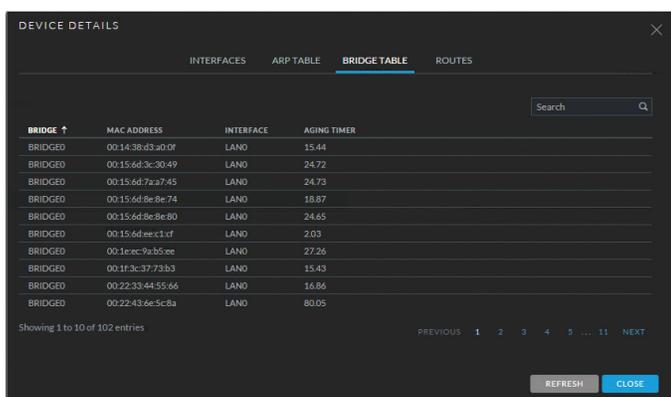
Bridge The name of the bridge.

MAC Address Displays the learned MAC address of a network device on a specific bridge port.

Interface Displays the network interface (bridge port) on which the MAC address is located. airOS can forward packets only to the specified port of the device, eliminating redundant copies and transmits.

Aging Timer Displays aging time for each address entry (in seconds). After a specific timeout, if the device has not seen a packet coming from a listed address, it will delete that address from the *Bridge Table*.

Refresh To update the information, click **Refresh**.

Close To close the window, click **Close**.

Routes

Click **Routes** to list all the entries in the system routing table.
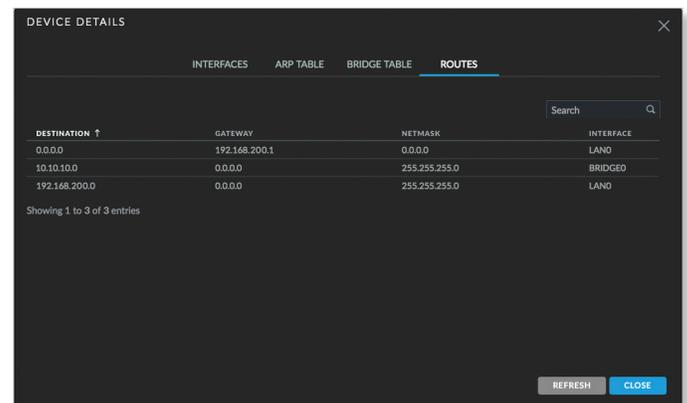
airOS examines the destination IP address of each data packet traveling through the system and chooses the appropriate interface to forward the packet to. The system choice depends on static routing rules, the entries that are registered in the system routing table. Static routes to specific hosts, networks, or the default gateway are set up automatically according to the IP configuration of all the airOS Configuration Interfaces.

> 📋 Note: Static routes also can be added manually. For more information, refer to **"Static Routes" on page 30**.

Destination Displays the IP address of the destination network or destination host.

Gateway Displays the IP address of the appropriate gateway.

Netmask Displays the netmask for the destination network: *255.255.255.255* for a host destination, and *0.0.0.0* for the default route.

> 📋 Note: The default route is the route used when no other routes for the destination are found in the routing table.

Interface Displays the interface to which packets for a particular route will be sent.

Refresh To update the information, click **Refresh**.

Close To close the window, click **Close**.

Firewall

(Available if *Firewall* is enabled on the *Network* page.) Click **Firewall** to list all the entries in the firewall table.
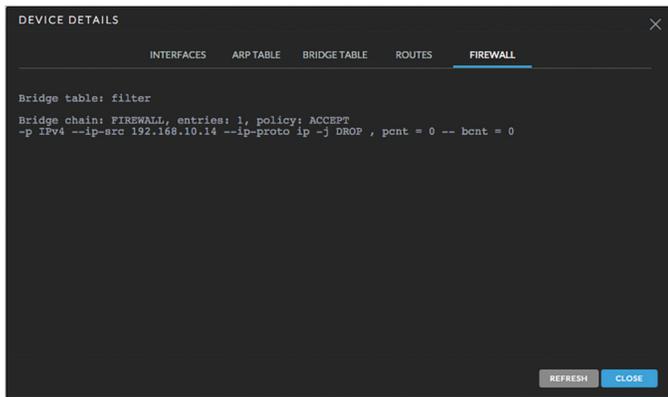
By default, there are no firewall rules.

If the device is operating in *Bridge* mode, the table lists active firewall entries in the FIREWALL chain of the standard ebtables filter table.

If the device is operating in *Router* mode, the table lists active firewall entries in the FIREWALL chain of the standard iptables filter table.

IP and MAC level access control and packet filtering in airOS are implemented using an ebtables (bridging) or iptables (routing) firewall that protects the resources of a private network from outside threats by preventing unauthorized access and filtering specified types of network communication.

Refresh To update the information, click **Refresh**.

Close To close the window, click **Close**.

Configure firewall rules on the *Network* page. See **"Firewall" on page 31** for additional details.

Port Forward

(Available if *Port Forwarding* is enabled in *Router* mode.) Click **Port Forward** to list all port forwarding rules.
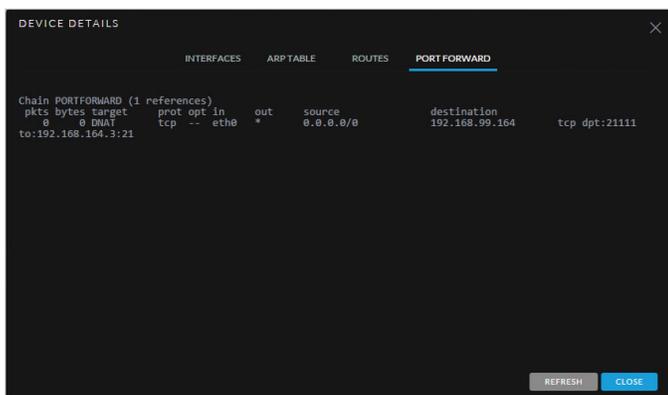
Port forwarding allows you to connect to a specific service such as an FTP server or web server. Port forwarding creates a transparent tunnel through a firewall/NAT, granting access from the WAN side to the specific network service running on the LAN side.

Chain PortForward Displays active port forward entries in the PREROUTING chain of the standard iptables nat table, while the device is operating in Router mode (DNAT).

Refresh To update the information, click **Refresh**.

Close To close the window, click **Close**.

Configure port forwarding rules on the *Network* page. See **"Port Forwarding" on page 32** for additional details.

DHCP Leases

(Available if *DHCP* is enabled on the *Network* page.) Click **DHCP Leases** to display the current status of the IP addresses assigned by the device's DHCP server to its local clients.
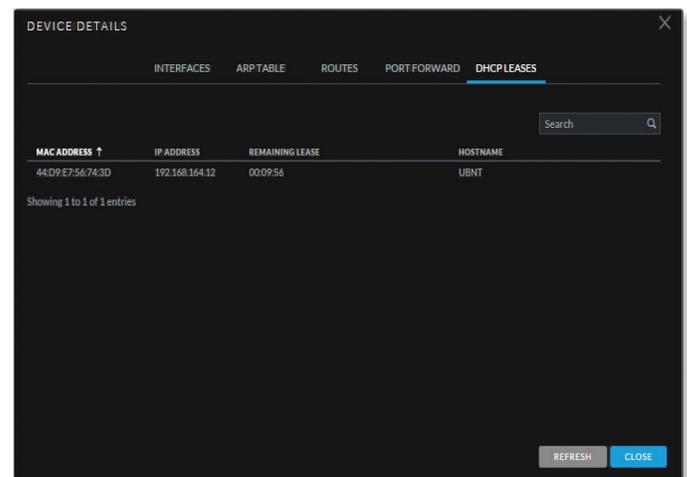
Search Enter the keyword to search for the desired *MAC Address*, *IP Address*, *Remaining Lease* time, or *Hostname*. To filter the list of entries, enter a string in the *Search* box and press **Enter** (PC) or **return** (Mac). Only entries with matching text will be displayed.

MAC Address Displays the client's MAC address.

IP Address Displays the client's IP address.

Remaining Lease Displays the remaining time of the leased IP address assigned by the DHCP server.

Hostname Displays the device name of the client.

Refresh To update the information, click **Refresh**.

Close To close the window, click **Close**.

Configure DHCP on the *Network* page. See **"DHCP" on page 23** for additional details.

Wireless

The *Wireless* section of the dashboard displays the following information for all local and remote devices:

- Link information and statistics
- Average/isolated capacity and throughput data
- Constellation diagrams, Carrier to Interference-plus-Noise Ratio (CINR) histograms, and signal, noise, and interference time series plots
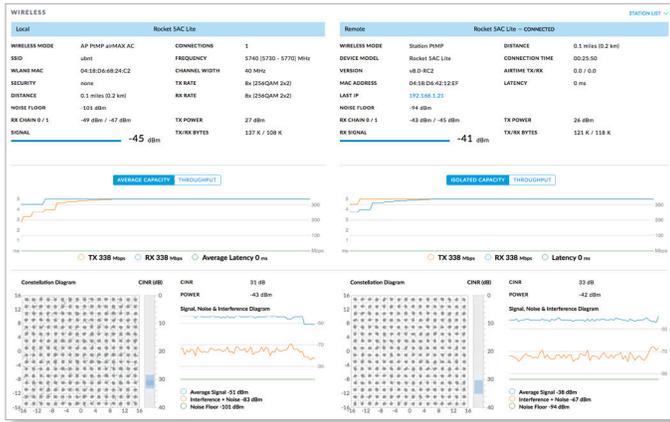
Link Information and Statistics

In *Access Point PTP*, *Station PTP*, and *Station PTMP* modes, airOS displays statistics on the local and remote devices, as shown below.
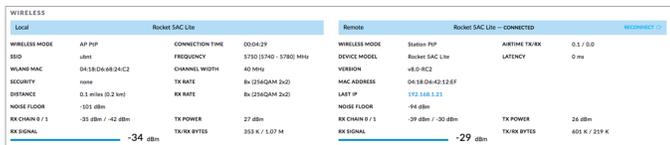
In *Access Point PTMP* modes, airOS also displays information on the connected stations. By default, this information is minimized as shown below; click **Station List** to display the information (refer to **"Station List" on page 10** for a detailed description of this information).
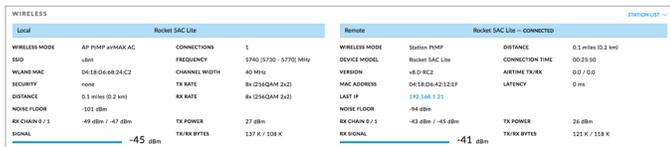
Local

Wireless Mode Displays the operating mode of the local radio interface. airOS supports five operating modes (not all products support all modes): *Station PTP*, *Station PTMP*, *Access Point PTP*, *Access Point PTMP AirMax AC*, and *Access Point PTMP AirMax Mixed*. The default setting is device-specific. Configure the *Wireless Mode* on the *Wireless* tab (see **"Basic Wireless Settings" on page 13** for additional details).

Any airMAX ac series device may operate in only one of these modes at a time. For example, if the device is running in an *Access Point* mode, it cannot simultaneously run in a *Station* mode.

SSID Displays the wireless network name (SSID), which depends upon the wireless mode selected:

- In *Station* modes, this displays the SSID of the AP the device is associated with.
- In *Access Point* modes, this displays the SSID configured on the device using the *Wireless* tab.

Configure the SSID on the *Wireless* page. See **"SSID" on page 14** for additional details.

WLAN0 MAC Displays the MAC address of the device as seen on the wireless network.

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

Distance (Available in *Access Point PTP* modes only.) Displays the current distance between devices in kilometers and miles for Acknowledgement (ACK) frames. Changing the distance value will change the ACK (Acknowledgement) timeout accordingly. The ACK timeout specifies how long the device should wait for an acknowledgement from a partner device confirming frame reception before it concludes that there has been an error and resends the frame. You can adjust the *Distance* value on the *Wireless* page (see **"Distance" on page 16**).

Noise Floor Displays the device's noise floor level in dBm.

RX Chain 0 / 1 Displays the wireless signal level (in dBm) of each chain.

RX Signal Displays the received signal level in dBm.

Connections (Available in *Access Point PTMP* modes only.) Displays the number of stations that are connected to the device.

Connection Time (Available in *Access Point PTP* and *Station* modes only.) Displays the association time of the connected access point or station. The time is expressed in days, hours, minutes, and seconds.

Frequency Displays the actual operating frequency center and operating frequency range (in MHz) which depends on the channel width being used. If "DFS" is displayed next to the frequency, this indicates that the selected channel has DFS (Dynamic Frequency Selection) capabilities.

Channel Width This is the spectral width of the radio channel used by the device. airOS 8 supports 10, 20, 30, 40, 50, 60, and 80 MHz; however, available channel widths are device-specific. Default values are as follows:

- *Access Point PTP* mode: Default is *80 MHz*.
- *Access Point PTMP AirMax AC* mode: Default is *40 MHz*.
- *Access Point PTMP AirMax Mixed* mode: Default is *40 MHz*.
- *Station PTP* mode: Default is *Auto 20/40/80 MHz*.
- *Station PTMP* mode: Default is *Auto 20/40 MHz*.

TX Rate Displays the transmit data rate: *1x (BPSK 1x1)*, *2x (QPSK 1x1)*, *4x (16QAM 2x2)*, *6x (64QAM 2x2)*, and *8x (256QAM 2x2)*.

RX Rate Displays the received data rate: *1x (BPSK 1x1)*, *2x (QPSK 1x1)*, *4x (16QAM 2x2)*, *6x (64QAM 2x2)*, and *8x (256QAM 2x2)*.

TX Power Displays the transmit power level in dBm. If the local device is a station, and if the *Automatic Power Control* (APC) option is enabled, the APC status is also displayed as follows:

• **Auto** APC target achieved.

• **Adjusting** APC in progress.

• **Auto, limits reached** APC target achieved due to power limits being reached.

• **Auto failed** APC aborted due to excess number of trials or oscillations.

For details on the *Automatic Power Control* option, refer to **"Automatic Power Control" on page 18**.

TX/RX Bytes Displays the number of bytes transmitted and received in bytes.

Remote

Wireless Mode Displays the operating mode of the remote device: *Station PTP*, *Station PTMP*, *Access Point PTP*, *Access Point PTMP AirMax AC*, and *Access Point PTMP AirMax Mixed*. The default setting is device-specific.

Device Model Displays the model of the AP or station.

Version Displays the firmware version of airOS on the AP or station.

AP MAC (Available in *Station* modes.) This displays the MAC address of the AP the device is associated with.

MAC Address (Available in *Access Point* modes.) Displays the MAC address of the station.

RX Chain 0 / 1 Displays the wireless signal level (in dBm) of each chain.

RX Signal Displays the received signal level in dBm.

Distance (Available in *Access Point PTMP* modes only.) Displays the current distance between devices in kilometers and miles for Acknowledgement (ACK) frames. With *Auto Adjust* enabled, the device's auto-acknowledgement timeout algorithm dynamically optimizes the frame acknowledgement timeout value without user intervention.

Connection Time (Available in *Access Point PTMP* modes only.) Displays the association time of the connected access point or station. The time is expressed in days, hours, minutes, and seconds.

Airtime TX/RX Displays the transmit and receive airtime values. The airtime is the averaged wireless bandwidth utilization (percentage of theoretical transmission maximum), for both failed and successful transmission attempts.

Desired Priority (Available in *Station* modes only.) Displays the requested airMAX station priority level that is configured on the *Wireless* tab of the *Settings* page (for more information, refer to **"airMAX Station Priority" on page 18**).

Priority (Available in *Station* modes only.) Displays the current operating priority of the station.

> Note: The *Priority* may be lower than the configured *Desired Priority*. The AP automatically lowers the priority depending upon RF conditions and performance.

Latency Displays the latency value, in ms, for wireless frames.

TX Power Displays the transmit power level in dBm. If the remote device is a station, and if the *Automatic Power Control* (APC) option is enabled, the APC status is also displayed as follows:

• **Auto** APC target achieved.

• **Adjusting** APC in progress.

• **Auto, limits reached** APC target achieved due to power limits being reached.

• **Auto failed** APC aborted due to excess number of trials or oscillations.

For details on the *Automatic Power Control* option, refer to **"Automatic Power Control" on page 18**.

TX/RX Bytes Displays the total number of bytes transmitted and received during the connections uptime.

Reconnect (Available in *Station* modes.) To establish the wireless link to the AP or station again, click **Reconnect**.

Station List

In *Access Point PTMP AirMax AC* or *Access Point PTMP AirMax Mixed* mode, airOS displays a table with statistics for all stations that are connected to the device (if the table is not displayed, click **Station List** to display it):

You can modify this table as follows:

• To filter the list of stations, enter a string in the *Search* box and press **Enter** (PC) or **return** (Mac). Only stations with matching text will be displayed.

• To sort the table on a particular column (field) click the column heading; each click toggles the sort order.

• To select which fields are displayed in the table, click **Columns**, select all columns to be displayed, deselect all columns to be hidden, and then click **OK**.

The table displays the following fields by default: *Station MAC*, *Device Model*, *Device Name*, *Signal RX*, *Signal TX*, *Distance*, *Isolated Capacity TX*, *Isolated Capacity RX*, *Airtime TX*, *Airtime RX*, *Connection Time*, *Last IP*.

The table contains the following columns of information (use the table's horizontal scroll bar to view all the fields):

Station MAC Displays the MAC address of the station.

Device Model Displays the model name of the station.

Firmware Displays the current firmware version number.

Device Name Displays the station's host name. The device name can be changed on the *System* tab.

Signal RX Displays the receive signal level in dBm.

> 📄 Note: The *Signal RX* value is displayed in red if it is too high (above -40 dBm).

Signal TX Displays the transmit signal level in dBm.

RX Chain 0 / 1 Displays the last received wireless signal level per chain.

> 📄 Note: The *RX Chain 0* and *RX Chain 1* values are displayed in red if the difference between them exceeds the recommended maximum of 5 dBm.

Noise The *Noise* value represents the AP noise level.

Latency Displays the latency value in ms.

Distance Displays the current distance between devices in kilometers and miles for Acknowledgement (ACK) frames. With *Auto Adjust* enabled, the device's auto-acknowledgement timeout algorithm dynamically optimizes the frame acknowledgement timeout value without user intervention.

TX Rate Displays the data rate of the last transmitted packet.

RX Rate Displays the data rate of the last received packet.

TX/RX Bytes Displays the total number of bytes transmitted and received from the station during the connection uptime.

TX/RX PPS (Packets per Second) Displays the mean value of the transmitted and received packet rates.

TX Power Displays the remote station transmit power in dBm.

Isolated Capacity TX/RX Displays the transmit and receive capacity that the station would have if it were the only station on the network.

airTime TX Displays the transmit airtime percentage value. The airtime is the percentage of the time the radio resource is utilized in the specified direction (TX).

airTime RX Displays the receive airtime percentage value. The airtime is the percentage of the time the radio resource is utilized in the specified direction (RX).

Desired Priority Displays the requested airMAX station priority level that is configured on the *Wireless* page (for details, see **"airMAX Station Priority" on page 18**).

Priority (Available in *Station PTMP* mode only.) Displays the current operating priority of the station.

> 📄 Note: The *Priority* may be lower than the configured *Desired Priority*. The AP automatically lowers the priority depending upon RF conditions and performance.

Connection Time Displays the total time elapsed for the connection.

Last IP Displays the station's last IP address.

Action Displays available options for this station. For example, click **Kick** to drop the connection to this station.

Isolated/Average Capacity and Throughput

(Isolated Capacity available in *AP PTP* and *Station* modes. Average Capacity available in *AP PTMP* modes only.)
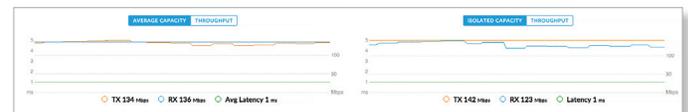
This section displays the isolated or average capacity, or the throughput, for both the local and remote devices. To display the isolated/average capacity, click **Isolated Capacity** or **Average Capacity**. To display the throughput, click **Throughput**.

The capacity and throughput plots display the current data transmission rate, data reception rate, and latency in graphical and numerical form.

The isolated capacity is the expected maximum rate at which data can be transmitted over the channel (accounting for protocol overhead and interference). The average capacity is the average TX/RX isolated capacity of the associated stations.

For the throughput graph, the chart scale and throughput dimension (bps, kbps, Mbps) change dynamically depending on the mean throughput value. The statistics are updated automatically.

RF Performance

The *RF Performance* section displays persistent RF Error Vector Magnitude (EVM) constellation diagrams, Carrier to Interference-plus-Noise Ratio (CINR) histograms, and Signal, Noise, and Interference time series plots:
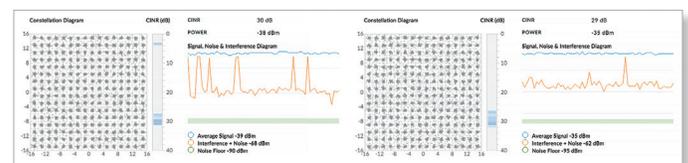
The *RF Performance* section displays the following information for both the local and remote devices:

Local/Remote Constellation Diagram Provides a real-time visual depiction of the modulation for the local or remote device. The modulation, which can be 1x (BPSK), 2x (QPSK), 4x (16-QAM), 8x (64-QAM), or 16x (256-QAM), adjusts dynamically as the system adapts to changing conditions. The plotted points' appearance indicates the signal quality: tightly defined points indicate higher signal quality, while diffuse points indicate lower signal quality.

CINR (dB) These histograms display the CINR, in dB, for the local and remote devices. The CINR is a measure of signal quality. It is the median value of how high the signal is over the combined interference and noise. In each histogram, the color shows the distribution of CINR values; the darker the color, the greater the number of occurrences of that value.

Signal, Noise and Interference Displays a time-based plot of the system signal, noise, and interference levels in dBm for both the local and remote devices. The power and CINR levels for the local and remote devices are also displayed above each constellation diagram.
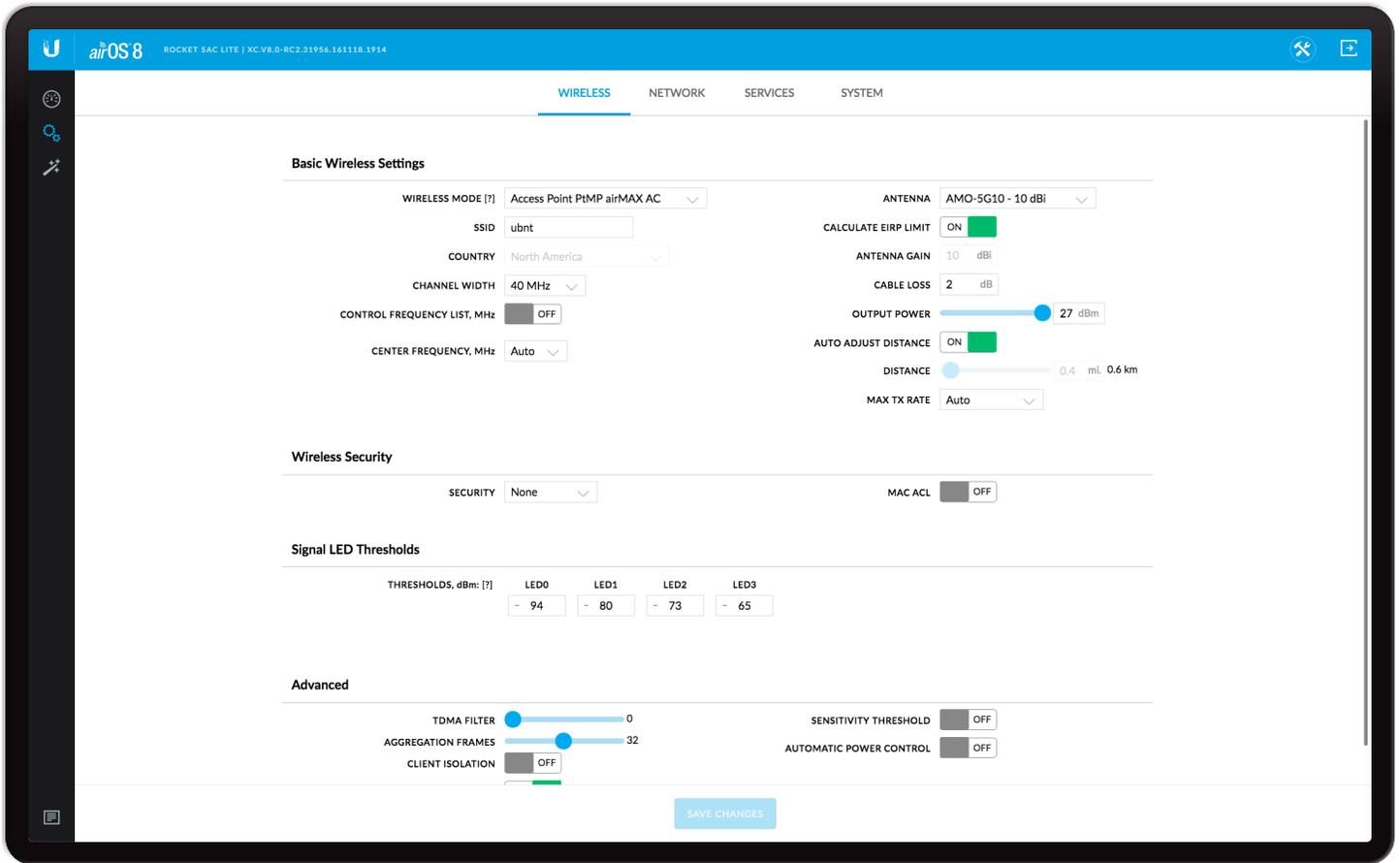
Chapter 3: Wireless

The *Wireless* tab contains everything needed to set up the wireless part of the link, including the wireless mode, SSID, channel and frequency, output power, data rates, and wireless security.

Basic Wireless Settings

Configure the basic wireless settings.

Wireless Mode Specify the *Wireless Mode* of the device. The mode depends on the product model and network topology requirements. airOS 8 supports the following modes:

• **Access Point PTP** If you have a single device to act as an access point (AP) in a Point-to-Point (PtP) link, configure it as *Access Point PTP* mode. The device functions as an AP that connects a single client device (the client device must be in *Station PTP* mode).
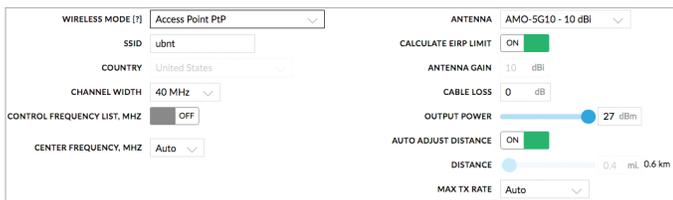
• **Access Point PTMP AirMax AC** If you have a single device to act as an AP in a Point-to-MultiPoint (PtMP)

link, and if your network contains only airMAX AC devices, configure it as *Access Point PTMP* mode. The device functions as an AP that connects multiple client devices (client devices must be in *Station PTMP* mode).
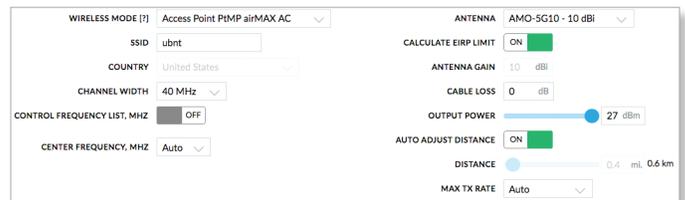
• **Access Point PTMP AirMax Mixed** If you have a single device to act as an AP in a Point-to-MultiPoint (PtMP) link, and if your network contains both airMAX ac and airMAX M Series devices, configure it as *Access Point PTMP* mode. The device functions as an AP that connects multiple client devices (client devices must be in *Station PTMP* mode).
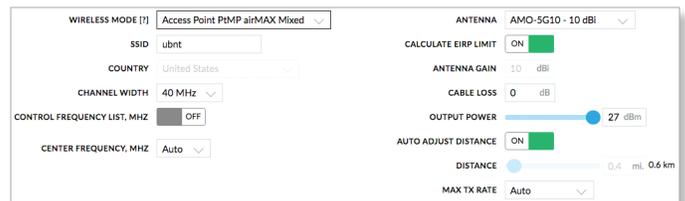
Note: All airMAX M Series devices must use airOS 6 or later.

- **Station PTP** If you have a client device to connect to an AP in a Point-to-Point (PtP) link, configure the client device as *Station PTP* mode. The client device acts as the subscriber station while connecting to the AP (the AP must be in *Access Point PTP* mode). The AP's SSID is used, and all traffic to and from the network devices connected to the Ethernet interface is forwarded to the AP.
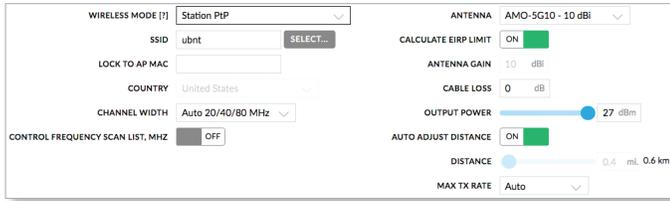
- **Station PTMP** If you have multiple client devices to connect to an AP, configure the client devices as *Station PTMP* mode. The client devices act as the subscriber stations while they are connecting to the AP (which must be in *Access Point PTMP* mode). The AP's SSID is used, and all traffic to and from the network devices connected to the Ethernet interface is forwarded to the AP and other wireless stations.
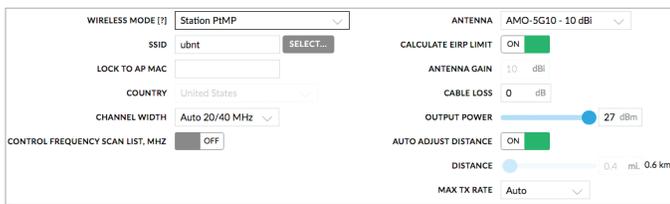
SSID If the device is operating in *Access Point PTP*, *Access Point PTMP AirMax AC*, or *Access Point PTMP AirMax Mixed* mode, specify the wireless network name or SSID (Service Set Identifier) used to identify your WLAN. All the client devices within range will receive broadcast messages from the AP advertising this SSID.

If the device is operating in a *Station* mode, specify the SSID of the AP that the device is associated with.

> **Note:** If there are multiple APs with the same SSID, use the *Lock to AP MAC* field instead to specify the AP to associate with.

Select (Available in *Station PTP* or *Station PTMP* mode only.) To display the list of available APs, click **Select**.
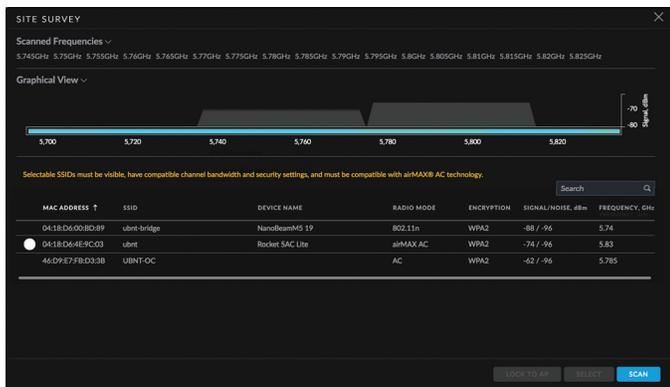
The *Site Survey* tool will search all supported channels for available wireless networks in range and display a radio button next to each network that you can select for association. The tool has incremental scan functionality for more dynamic results. If the selected network uses encryption, you'll need to configure the *Wireless Security* settings (refer to **"Wireless Security" on page 16**).

- **Scanned Frequencies** Click to display the list of frequencies that are being scanned.
- **Graphical View** Click to display a graphical view of the signal strength and frequency for each channel being used by the detected network devices.
- **Search** Enter a keyword to search for the desired AP.
- **Lock to AP** Use this option if there are multiple APs using the same SSID. Select the desired AP and click **Lock To AP** to lock the station to the AP and keep it from roaming between APs with the same SSID. (The AP will be uniquely identified by its MAC address.) Then, click **Save Changes** to connect the station to the AP.
- **Select** Select the AP and click **Select** to associate the station with the AP using the AP's SSID. Then, click **Save Changes** to connect the station to the AP.
- **Scan** Click **Scan** to refresh the list of available wireless networks.

Selected SSIDs must be visible, have compatible channel bandwidth and security settings, and must be compatible with airMAX AC technology. In addition:

- If *Access Point PTMP* mode is selected on a station operating in *Station PTP* mode, the station's mode will automatically be changed to *Station PTMP* mode (the following warning will be displayed: "Wireless Mode: Warning: New wireless mode selected!").
- If *Access Point PTP* is selected on a station operating in *Station PTMP* mode, the station's mode will automatically be changed to *Station PTP* mode (the following warning will be displayed: "Wireless Mode: Warning: New wireless mode selected!").

The list of *Scanned Frequencies* for the *Site Survey* is determined by the *Control Frequency Scan List* option, if the option is enabled.

Lock to AP MAC (Available only in *Station PTP* or *Station PTMP* mode.) Displays the AP MAC address selected by the *Lock to AP* button in the *Site Survey* tool.

Country Each country has their own power level and frequency regulations. *To ensure the device operates under the necessary regulatory compliance rules, you must select the country where your device will be used*. (The country is selected upon initial login, as described in **"Getting Started" on page 2**.) The channels, frequencies, and output power limits will be tuned according to the regulations of the selected country.

> **Note:** For the *Country* setting, U.S. product versions are restricted to a choice of Canada, Puerto Rico, or the U.S. to ensure compliance with FCC/IC regulations.

Channel Width Displays the spectral width of the radio channel. You can use this option to control the bandwidth consumed by your link.

Using higher bandwidth increases throughput. Using lower bandwidth does the following:

- Reduces throughput proportional to the reduction in channel size. For example, as 40 MHz increases possible speeds by 2x, the half-spectrum channel (10 MHz) decreases possible speeds by 2x.

- Increases the number of available, non-overlapping channels, so networks have better scalability.

- Increases the Power Spectral Density (PSD) of the channel, so you can increase the link distance – more robust links over long distances.

Available channel widths depend on the selected *Wireless Mode*. Here are the options for each mode:

- **Access Point PTP** Supported wireless channel spectrum widths: *80 MHz*, *60 MHz**, *50 MHz*, *40 MHz*, *30 MHz**, *20 MHz*, and *10 MHz*.

- **Access Point PTMP AirMax AC** Supported wireless channel spectrum widths: *40 MHz*, *30 MHz**, *20 MHz*, and *10 MHz*.

- **Access Point PTMP AirMax Mixed** Supported wireless channel spectrum widths: *40 MHz*, *20 MHz*, and *10 MHz*.

- **Station PTP** Supported wireless channel spectrum widths: *Auto 20/40/80 MHz* (recommended), *60 MHz**, *50 MHz*, *30 MHz**, and *10 MHz*.

- **Station PTMP** Supported wireless channel spectrum widths: *Auto 20/40 MHz* (recommended), *30 MHz**, and *10 MHz*.

> Note: The 30 MHz* and 60 MHz* channel widths feature improved performance in airOS v7.1.7 or later, and are incompatible with earlier airOS versions. Using the 30 MHz* or 60 MHz* channel width in airOS v7.1.7 or later requires an upgrade to both sides of the link.

Control Frequency List, MHz (Available in *Access Point* modes only.) Multiple frequencies are available to avoid interference between nearby APs. The frequency list varies depending on the selected *Country* and *Channel Width* options. Once enabled, click **Edit** to open the *Control Frequency List* window.
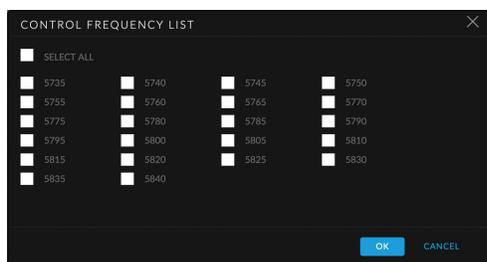
Select the frequencies and click **OK**, or click *Cancel* to close the window without any selections.

Control Frequency Scan List, MHz (Available in *Station* modes only.) This restricts scanning to only the selected frequencies. The benefits are faster scanning as well as filtering out unwanted APs in the results. The *Site Survey* tool will look for APs using only the selected frequencies. Once enabled, click **Edit** to open the *Control Frequency List* window.
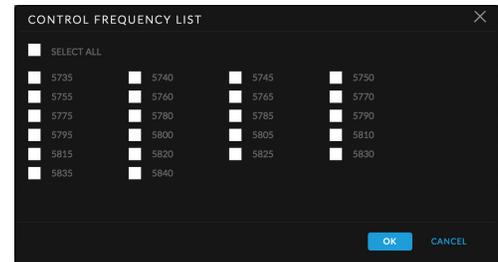
Select the frequencies that you want to scan and click **OK**, or click *Cancel* to close the window without any selections.

Center Frequency, MHz (Available in *Access Point PTP* or *Access Point PTMP* modes only.) The default, *Auto*, allows the device to automatically select the frequency. You can specify a frequency from the drop-down list.

Antenna Select your antenna from the list.

Calculate EIRP Limit This option should remain enabled so it forces the transmit output power to comply with the regulations of the selected country. If enabled, you cannot set EIRP above the amount allowed per regulatory domain (different maximum output power levels and antenna gains are allowed for each regulatory domain or country). The available frequencies depend on the product as well as the regulations of the selected country.

Antenna Gain (Read-only option; cannot be changed.) With *Calculate EIRP Limit* enabled, *Antenna Gain* calculates the TX power backoff needed to remain in compliance with local regulations. The *Antenna Gain* setting complements the *Cable Loss* setting; they both affect the TX power of the device.

Cable Loss (Only applicable to devices with external antenna connectors.) Enter the cable loss in dB. In case you have high amounts of cable loss, you may increase the TX power while remaining in compliance with local regulations. The *Cable Loss* setting complements the *Antenna Gain* setting; they both affect the TX power of the device.

Output Power Defines the maximum average transmit output power (in dBm) of the device. To specify the output power, use the slider or manually enter the output power value. The transmit power level maximum is limited according to country regulations. (If the device has an internal antenna, then *Output Power* is the output power delivered to the internal antenna.)

Auto Adjust Distance Enabled by default. We recommend keeping this option enabled. Every time the station receives a data frame, it sends an ACK (Acknowledgement) frame to the AP (if transmission errors are absent). If the AP does not receive the ACK frame within the set timeout, it re-sends the frame. The same occurs when the AP receives a data frame, but the station does not receive the ACK frame within the set timeout. (The timeout value depends on the value of the *Distance* option.) If too many data frames are re-sent (whether the ACK timeout is too short or too long), then there is a poor connection, and throughput performance drops.

The device has an auto-acknowledgement timeout algorithm, which dynamically optimizes the frame acknowledgement timeout value without user intervention. This critical feature is required for stabilizing long-distance, outdoor links.

Distance To specify the distance value in miles (or kilometers), use the slider or manually enter the value. The signal strength and throughput fall off with range. Changing the distance value will change the ACK timeout value accordingly.

If two or more stations are located at considerably different distances from the AP they are associated with, the distance to the farthest station should be set on the AP side.

Max TX Rate Defines the maximum rate at which the device should transmit wireless packets. The default is *Auto*; the rate algorithm selects the best data rate, depending on link quality conditions. We recommend that you use the *Auto* 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). To set a specific maximum rate, select one of the following: **1x (BPSK)**, **2x (QPSK)**, **4x (16QAM)**, **6x (64QAM)**, or **8x (256QAM)**.

Wireless Security

In *Access Point PTP* or *Access Point PTMP* mode, configure the wireless security settings that will be used by the devices on your wireless network.

In *Station PTP* or *Station PTMP* mode, enter the security settings of the AP that the device is associated with.

Security The following wireless security methods are supported: *None* and *WPA2-AES*. Follow the instructions for your selected method.

None

If you want an open network without wireless security, select **None**.

Note: Not using wireless security may compromise the security of your wireless network.

MAC ACL To configure a MAC Access Control List (ACL), select this option and then configure the *Policy* setting.

Policy Select whether to *Allow* or *Deny* the MAC addresses in the MAC ACL list. To edit the list, click **ACL**. For each entry, enter a MAC address and optional comment, and then click **Add**. When you are done editing, click **Save** to save the changes or *Cancel* to exit without saving.
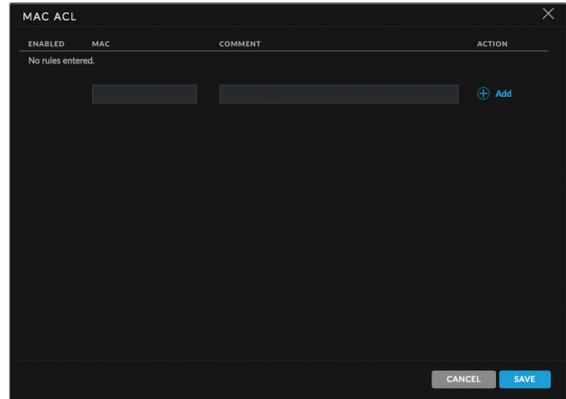
WPA2-AES

To secure your wireless network, select **WPA2-AES**, which is WPA2 (Wi-Fi Protected Access 2) security mode with AES (Advanced Encryption Standard) support only. AES is also known as CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol), which uses the AES algorithm.

WPA Authentication Specify one of the following WPA key selection methods:

• **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

WPA Preshared Key Specify a passphrase. The preshared key is an alpha-numeric password between 8 and 63 characters long.

Show Click **Show** if you want to view the characters of the *WPA Preshared Key*.

MAC ACL To configure a MAC Access Control List (ACL), select this option and then configure the *Policy* setting.

Policy Select whether to *Allow* or *Deny* the MAC addresses in the MAC ACL list. To edit the list, click **ACL**. For each entry, enter a MAC address and optional comment, and then click **Add**. When you are done editing, click **Save** to save the changes or *Cancel* to exit without saving.

EAP

EAP - Access Point PTP or Access Point PTMP Mode

The options below apply only in the following modes: *Access Point PTP, Access Point PTMP AirMax AC*, or *Access Point PTMP AirMax Mixed*.

Wireless Security	
SECURITY	WPA2-AES
WPA AUTHENTICATION	EAP
AUTH SERVER IP/PORT	1812
AUTH SERVER SECRET	SHOW
ACCOUNTING SERVER	OFF
MAC ACL	ON
POLICY	Allow ACL...

Auth Server IP/Port In the first field, enter the IP address of the RADIUS authentication server. RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect to and use a network service.

In the second field, enter the UDP port of the RADIUS authentication server. The most commonly used port is 1812, but this may vary depending on the RADIUS server you are using.

Auth Server Secret Enter the password. A shared secret is a case-sensitive text string used to validate communication between Access Point and RADIUS authentication server.

Show Click **Show** if you want to view the characters of the *Auth Server Secret*.

Accounting Server If you are using an accounting server, select this option.

- **Accounting Server IP/Port** If the *Accounting Server* is enabled, enter the IP address of the accounting server.

  In the second field, enter the UDP port of the RADIUS accounting server. The most commonly used port is 1813, but this may vary depending on the RADIUS server you are using.

- **Accounting Server Secret** If the *Accounting Server* is enabled, enter the password. A shared secret is a case-sensitive text string used to validate communication between two RADIUS devices.

  Show Click **Show** if you want to view the characters of the *Accounting Server Secret*.

MAC ACL To configure a MAC Access Control List (ACL), select this option and then configure the *Policy* setting.

Policy Select whether to *Allow* or *Deny* the MAC addresses in the MAC ACL list. To edit the list, click **ACL**. For each entry, enter a MAC address and optional comment, and then click **Add**. When you are done editing, click **Save** to save the changes or *Cancel* to exit without saving.

EAP - Station PTP or Station PTMP Mode

The options below apply in *Station PTP* or *Station PTMP* mode only.

Wireless Security		
SECURITY	WPA2-AES	
WPA AUTHENTICATION	EAP	
EAP TYPE	EAP-TTLS	MSCHAPV2
WPA ANONYMOUS IDENTITY		
WPA USER NAME		
WPA USER PASSWORD		SHOW

EAP Type Select the authentication protocol (**EAP-TTLS** or **EAP-PEAP**) and the inner authentication protocol (**MSCHAPV2**).

WPA Anonymous Identity Enter the identification credential used by the supplicant for EAP authentication in unencrypted form.

WPA User Name Enter the identification credential used by the supplicant for EAP authentication.

WPA User Password Enter the password credential used by the supplicant for EAP authentication.

Show Click **Show** if you want to view the characters of the *WPA User Password*.

Signal LED Thresholds

You can configure the LEDs on the device to light up when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy an airOS 8 CPE without logging into the device (for example, for antenna alignment operation).

Signal LED Thresholds				
THRESHOLDS, DBM:	LED0	LED1	LED2	LED3
[?]	– 94	– 80	– 73	– 65

Thresholds, dBm The number of LEDs is device-specific, and the default values vary depending on the number of LEDs. The specified LED will light up if the signal strength reaches the value set in the field.

For example, if the device has four LEDs and the signal strength (on the *Main* tab) fluctuates around -63 dBm, then the LED threshold values can be set to the following: -70, -65, -62, and -60.

Note: The "-" character is outside of the field and should not be used for the signal strength value specification.

The following table lists the default threshold values for devices with two, three, four, or six LEDs.

LED	Default Threshold Value
Two LEDs	
1	-94 dBm
2	-65 dBm
Three LEDs	
1	-94 dBm
2	-77 dBm
3	-65 dBm
Four LEDs	
1	-94 dBm
2	-80 dBm
3	-73 dBm
4	-65 dBm
Six LEDs	
1	-94 dBm
2	-88 dBm
3	-82 dBm
4	-77 dBm
5	-71 dBm
6	-65 dBm

Advanced

The *Advanced* section configures advanced wireless settings. Only technically advanced users who have sufficient knowledge about WLAN technology should use the advanced wireless settings. These settings should not be changed unless you know the effects the changes will have on the device.
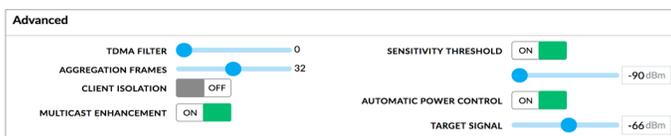
TDMA Filter (Available in *Access Point* modes only.) This option allows you to specify how much the airMAX scheduler should penalize poorly performing clients, on a scale of 0 to 9. The default is *0*.

Aggregation Frames This option allows the device to send 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, destination endpoints, and traffic class (QoS) into one large frame with a common MAC header. To specify the number of frames that will be combined in the new larger frame, use the slider. The default is *32*.

Client Isolation (Available in *Access Point PTMP* modes only.) Isolates traffic between the wireless clients by allowing packets to be sent only from the external network to the CPE and vice versa. 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) levels.

Multicast Enhancement (Available in *Access Point PTMP* modes only.) If clients do not send IGMP (Internet Group Management Protocol) messages, then they are not registered as receivers of your multicast traffic. Using IGMP snooping, the *Multicast Enhancement* option isolates multicast traffic from unregistered clients and allows the device to send multicast traffic to registered clients using higher data rates. This lessens the risk of traffic overload on PtMP links and increases the reliability of multicast traffic since packets are transmitted again if the first transmission fails. If clients do not send IGMP messages but should receive multicast traffic, then you may need to disable the *Multicast Enhancement* option. By default this option is enabled.

airMAX Station Priority (Available in *Station PTMP* mode only.) It defines the number of time slots (or amount of airtime) assigned to each station. By default the AP gives all active stations the same amount of time. However, if the stations are configured with different priorities, the AP will give stations more or less time, depending on the priority.

Note: *airMAX Station Priority* only functions in *Station PTMP* mode only.

airMAX Station Priority options include:

- **High** 4 time slots (4:1 ratio)
- **Medium** 3 time slots (3:1 ratio)
- **Base** 2 time slots (Default setting for stations; 2:1 ratio)
- **Low** 1 time slot (1:1 ratio)

Stations with a higher priority have access to more of the AP's airtime, providing higher possible throughput and lower latency when sharing with other active stations. For example, if there are 3 stations, 1 set to *Base*, 1 set to *Medium*, and 1 set to *High*, the *Base* station will get 2 time slots, the *Medium* station will get 3 time slots, and the *High* station will get 4 time slots.

Sensitivity Threshold (Available for airMAX ac devices only.) Select this option to use the *Sensitivity Threshold* feature, and then use the slider to adjust the sensitivity threshold value. The default is *-90* dBm.

When this option is enabled, the airMAX ac device will ignore any received signal that is below the configured threshold value. This option can help to increase resilience to interference and can be enabled on either the AP, the station, or both (depending on the environment).

Automatic Power Control (Available in *Access Point* modes only.) Select this option to use the *Automatic Power Control* feature. When *Automatic Power Control* is enabled, each radio monitors the amount of power received by

the radio at the other end of the link. If the reported value differs from the received *Target Signal* value, the radio automatically adjusts its transmit output power to match the received *Target Signal* value. The radio will use its *Output Power* setting as the maximum level at which it will transmit to maintain the received *Target Signal*.

- **Target Signal** This setting indicates the minimum received power level allowed at the remote end of the link. If the remote device's received power drops below this level, the *Automatic Power Control* feature automatically adjusts the transmit power to maintain the received power at this level. The default is *-66* dBm.
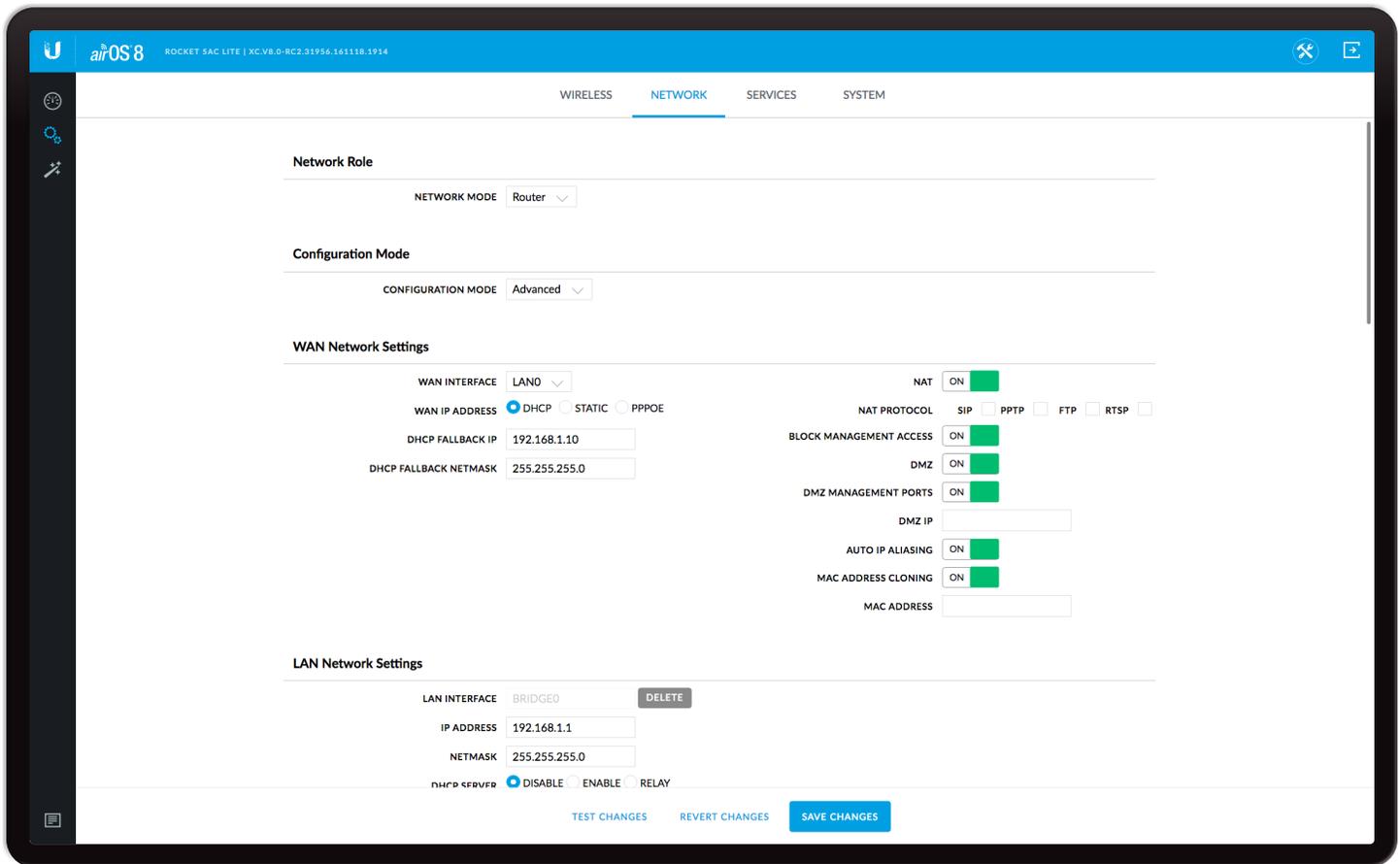
Chapter 4: Network

The *Network* tab allows you to configure bridge or routing functionality and IP settings.

Network Role

airOS 8 supports *Bridge* and *Router* modes.

Network Mode Select the *Network Mode* of the device (the mode depends on network topology requirements). *Bridge* mode is adequate for very small networks. Larger networks have significantly more traffic and need to be managed by a device in *Router* mode to keep broadcast traffic within its respective broadcast domain and prevent it from overloading the overall traffic in the network.

- **Bridge** The device acts as a transparent bridge, operates in Layer 2 (like a managed switch), and usually has only one IP address (for management purposes only).

- **Router** The device contains two networks or subnets: a Wide Area Network (WAN) and a LAN. Each wired or wireless interface on the WAN or LAN has an IP address.

The following summarizes the differences between *Bridge* and *Router* modes:

Bridge mode:

- The device 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.

- There is no network segmentation, and the broadcast domain is the same. *Bridge* mode does not block any broadcast or multicast traffic. You can configure additional firewall settings for Layer 2 packet filtering and access control.

- WLAN and LAN interfaces belong to the same network segment and share the same IP address space. They form the virtual bridge interface while acting as bridge ports. The device features IP settings for management purposes.

Router mode:

- The device operates in Layer 3 to perform routing and enable network segmentation – wireless clients and the WAN interface are on a different IP subnet. *Router* mode blocks broadcasts and can pass through multicast packet traffic. You can configure additional firewall settings for Layer 3 packet filtering and access control.

- The device can act as a DHCP server and use Network Address Translation (Masquerading), which is widely used by APs. NAT acts as the firewall between the LAN and WAN.

- In *Advanced* view, any interface can be selected as the WAN or the LAN, but typical functionality is as follows:

    - **Station** The WLAN functions as the WAN, and the Ethernet port functions as the LAN.

    - **Access Point** The Ethernet port functions as the WAN, and the WLAN functions as the LAN.

- Each wired or wireless interface on the WAN or LAN has its own IP address.

- For example, *Router* mode is used in a typical Customer Premises Equipment (CPE) installation. The device acts as the demarcation (demarc) point between the CPE and Wireless Internet Service Provider (WISP), with the wireless interface of the device connecting to the WISP. There can be only one WAN interface, but there can be many LAN interfaces.

    The following diagram shows the NanoBeam ac at a residence wirelessly connecting to a WISP tower.
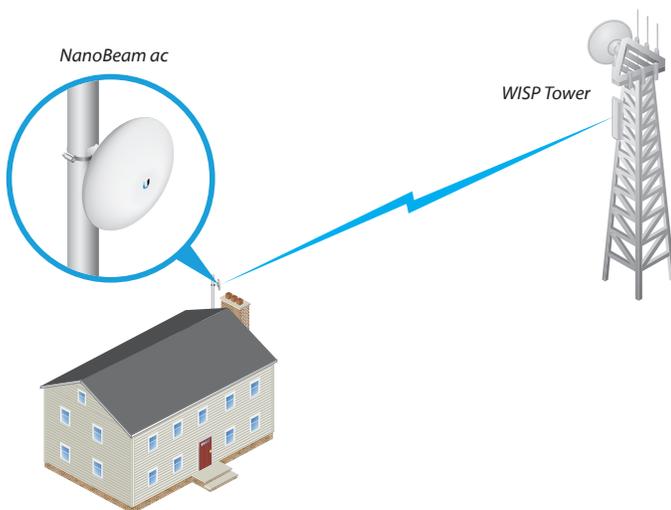
Configuration Mode

The *Network* page has two views, *Simple* and *Advanced*.
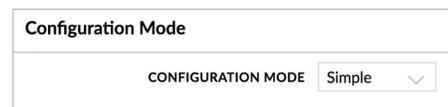
Simple The following basic configuration settings are available (advanced configuration settings are hidden):

- **"Network Role" on page 21**
- **"Configuration Mode" on page 22**
- **"WAN Network Settings" on page 23** (available in *Router* mode only
- **"LAN Network Settings" on page 26** (available in *Router* mode only
- **"Management Network Settings" on page 27** (available in *Bridge* mode only)
- **"Port Forwarding" on page 32** (available in *Router* mode only
- **"Multicast Routing Settings" on page 33** (available in *Router* mode only

Advanced Displays the advanced configuration settings, in addition to the basic configuration settings:

- **"Network Role" on page 21**
- **"Configuration Mode" on page 22**
- **"WAN Network Settings" on page 23** (available in *Router* mode only)
- **"LAN Network Settings" on page 26** (available in *Router* mode only
- **"Management Network Settings" on page 27**)
- **"DHCP Address Reservation" on page 28** (available in *Router* mode only
- **"Interfaces" on page 28**
- **"IP Aliases" on page 29**
- **"VLAN Network" on page 29**
- **"Bridge Network" on page 30**
- **"Static Routes" on page 30**
- **"Firewall" on page 31**
- **"Port Forwarding" on page 32** (available in *Router* mode only
- **"Multicast Routing Settings" on page 33** (available in *Router* mode only
- **"Traffic Shaping" on page 33**

WAN Network Settings

(Available in *Router* mode only.)

WAN Network Settings

WAN INTERFACE	LAN0	NAT OFF
WAN IP ADDRESS	◉ DHCP ○ STATIC ○ PPPOE	BLOCK MANAGEMENT ACCESS OFF
DHCP FALLBACK IP	192.168.10.1	DMZ OFF
DHCP FALLBACK NETMASK	255.255.255.0	AUTO IP ALIASING OFF
MTU	1500	MAC ADDRESS CLONING OFF

**WAN Interface** Select the interface used for connection to the external network (Internet).

WAN IP Address The IP address of the WAN interface connected to the external network. You can use this IP address for routing and device management purposes.

The device can use one of the following:

- **"DHCP" on page 23**
- **"Static" on page 24**
- **"PPPoE" on page 25**

DHCP

The external DHCP server assigns a dynamic IP address, gateway IP address, and DNS address to the device.

WAN INTERFACE	LAN0	NAT ON
WAN IP ADDRESS	◉ DHCP ○ STATIC ○ PPPOE	NAT PROTOCOL SIP PPTP FTP RTSP
DHCP FALLBACK IP	192.168.10.1	BLOCK MANAGEMENT ACCESS ON
DHCP FALLBACK NETMASK	255.255.255.0	DMZ ON
MTU	1500	DMZ MANAGEMENT PORTS ON
		DMZ IP
		AUTO IP ALIASING ON
		MAC ADDRESS CLONING ON
		MAC ADDRESS

DHCP Fallback IP Enter the IP address for the device to use if an external DHCP server is not found.

DHCP Fallback Netmask Enter the netmask for the device to use if an external DHCP server is not found.

MTU (Available in *Simple* view.) The Maximum Transmission Unit (MTU) is the maximum frame size (in bytes) that a network interface can transmit or receive. The default is *1500*.

NAT Network Address Translation (NAT) is an IP masquerading technique that hides private network IP address space (on the LAN interface) behind a single public IP address (on the WAN interface).

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table. Specify static routes to allow packets to pass through the airOS device if NAT is disabled.

- **NAT Protocol** To disable NAT traversal for the SIP, PPTP, FTP, or RTSP protocols, uncheck the respective box(es).

Block Management Access To block device management from the WAN interface, check this box. This feature makes *Router* mode more secure if the device has a public IP address.

DMZ DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become "demilitarized", so all ports from the public network are forwarded to the ports of this private network, similar to a 1:1 NAT.

- **DMZ Management Ports** The airOS device responds to requests from the external network as if it were the host device that is specified with the DMZ IP address. *DMZ Management Ports* is disabled by default; the device is accessible from the WAN port. If *DMZ Management Ports* is enabled, all management ports will be forwarded to the device, so you'll only be able to access the device from the LAN side.

  The default values of the management ports are:

Management Method	Management Port
HTTP/HTTPS	80/443 TCP
SSH	22 TCP
Telnet	23 TCP
SNMP	161 UDP
Discovery	10001 UDP

- **DMZ IP** Enter the IP address of the local host network device. The DMZ host device will be completely exposed to the external network.

Auto IP Aliasing If enabled, automatically generates an IP address for the corresponding WLAN/LAN interface. 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. The Auto IP always starts with 169.254.X.Y, with X and Y as the last two octets from the MAC address of the device. For example, if the MAC is 00:15:6D:A3:04:FB, then the generated unique Auto IP will be 169.254.4.251.

The *Auto IP Aliasing* setting can be useful because you can still access and manage devices even if you lose, misconfigure, or forget their IP addresses. Because an Auto IP address is based on the last two octets of the MAC address, you can determine the IP address of a device if you know its MAC address.

MAC Address Cloning When enabled, you can change the MAC address of the respective interface. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address. This is usually used by cable operators or some WISPs.

- **MAC Address** Enter the MAC address you want to clone to the respective interface. This becomes the new MAC address of the interface.

Static

Assign static IP settings to the device.

> Note: IP settings should be consistent with the address space of the device's network segment.

WAN INTERFACE	LAN0		NAT	ON
WAN IP ADDRESS	DHCP ○ STATIC ● PPPOE ○		NAT PROTOCOL	SIP ☑ PPTP ☑ FTP ☑ RTSP ☑
IP ADDRESS	0.0.0.0		BLOCK MANAGEMENT ACCESS	ON
NETMASK	255.255.255.0		DMZ	ON
GATEWAY IP			DMZ MANAGEMENT PORTS	OFF
PRIMARY DNS IP			DMZ IP	
SECONDARY DNS IP			AUTO IP ALIASING	ON
MTU	1500		MAC ADDRESS CLONING	ON
			MAC ADDRESS	

IP Address Enter the IP address of the device. This IP will be used for device management purposes.

Netmask The netmask defines the address space of the device's network segment. The 255.255.255.0 (or "/24") netmask is commonly used on many Class C 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 WISP gateway router. The device directs data 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. This is used for management purposes only.

Secondary DNS IP Enter the IP address of the secondary DNS server. This entry is optional and used only if the primary DNS server is not responding. It is used for management purposes only.

MTU (Available in *Simple* view.) The Maximum Transmission Unit (MTU) is the maximum frame size (in bytes) that a network interface can transmit or receive. The default is *1500*.

NAT Network Address Translation (NAT) is an IP masquerading technique that hides private network IP address space (on the LAN interface) behind a single public IP address (on the WAN interface).

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table. Specify static routes to allow packets to pass through the airOS device if NAT is disabled.

- **NAT Protocol** To disable NAT traversal for the SIP, PPTP, FTP, or RSTP protocols, uncheck the respective box(es).

Block Management Access To block device management from the WAN interface, check this box. This feature makes *Router* mode more secure if the device has a public IP address.

DMZ DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become "demilitarized", so all ports from the public network are forwarded to the ports of this private network, similar to a 1:1 NAT.

- **DMZ Management Ports** The airOS device responds to requests from the external network as if it were the host device that is specified with the DMZ IP address. *DMZ Management Ports* is disabled by default; the device is accessible from the WAN port. If *DMZ Management Ports* is enabled, all management ports will be forwarded to the device, so you'll only be able to access the device from the LAN side.

  The default values of the management ports are:

Management Method	Management Port
HTTP/HTTPS	80/443 TCP
SSH	22 TCP
Telnet	23 TCP
SNMP	161 UDP
Discovery	10001 UDP

- **DMZ IP** Enter the IP address of the local host network device. The DMZ host device will be completely exposed to the external network.

Auto IP Aliasing If enabled, automatically generates an IP address for the corresponding WLAN/LAN interface. 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. The Auto IP always starts with 169.254.X.Y, with X and Y as the last two octets from the MAC address of the device. For example, if the MAC is 00:15:6D:A3:04:FB, then the generated unique Auto IP will be 169.254.4.251.

The *Auto IP Aliasing* setting can be useful because you can still access and manage devices even if you lose, misconfigure, or forget their IP addresses. Because an Auto IP address is based on the last two octets of the MAC address, you can determine the IP address of a device if you know its MAC address.

MAC Address Cloning When enabled, you can change the MAC address of the respective interface. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address. This is usually used by cable operators or some WISPs.

- **MAC Address** Enter the MAC address you want to clone to the respective interface. This becomes the new MAC address of the interface.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is a virtual private and secure connection between two systems that enables encapsulated data transport. Subscribers sometimes use PPPoE to connect to Internet Service Providers (ISPs), typically DSL providers.

Select **PPPoE** to configure a PPPoE tunnel. You can configure only the WAN interface as a PPPoE client because all the traffic will be sent via this tunnel. After the PPPoE connection is established, the device will obtain the IP address, default gateway IP, and DNS server IP address from the PPPoE server. The broadcast address is used to discover the PPPoE server and establish the tunnel.

If there is a PPPoE connection established, then the IP address of the PPP interface will be displayed on the *Main* tab next to the PPP interface statistics; otherwise a *Not Connected* message and *Reconnect* button will be displayed. To re-connect a PPPoE tunnel, click **Reconnect**.

WAN INTERFACE	LAN0	NAT	ON
WAN IP ADDRESS	DHCP ○ STATIC ○ PPPOE ●	NAT PROTOCOL	SIP ✓ PPTP ✓ FTP ✓ RTSP ✓
USERNAME		BLOCK MANAGEMENT ACCESS	ON
PASSWORD		DMZ	ON
	SHOW	DMZ MANAGEMENT PORTS	OFF
SERVICE NAME		DMZ IP	
FALLBACK IP	192.168.10.1	AUTO IP ALIASING	ON
FALLBACK NETMASK	255.255.255.0	MAC ADDRESS CLONING	ON
MTU/MRU	1492 / 1492	MAC ADDRESS	
ENCRYPTION	OFF		
MTU	1500		

Username Enter the username to connect to the PPPoE server; this must match the username configured on the PPPoE server.

Password Enter the password to connect to the PPPoE server; this must match the password configured on the PPPoE server.

Show Click **Show** to view the characters of the password.

Service Name Enter the name of the PPPoE service. This must match the service name configured on the PPPoE server.

Fallback IP Enter the IP address for the device to use if the PPPoE server does not assign an IP address.

Fallback Netmask Enter the netmask for the device to use if the PPPoE server does not assign a netmask.

MTU/MRU The size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for data encapsulation during transfer through the PPP tunnel. The default value is *1492*.

Encryption Enables the use of Microsoft Point-to-Point Encryption (MPPE).

MTU (Available in *Simple* view.) The Maximum Transmission Unit (MTU) is the maximum frame size (in bytes) that a network interface can transmit or receive. The default is *1500*.

NAT Network Address Translation (NAT) is an IP masquerading technique that hides private network IP address space (on the LAN interface) behind a single public IP address (on the WAN interface).

NAT is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables nat table. Specify static routes to allow packets to pass through the airOS device if NAT is disabled.

- **NAT Protocol** To disable NAT traversal for the SIP, PPTP, FTP, or RTSP protocols, uncheck the respective box(es).

Block Management Access To block device management from the WAN interface, check this box. This feature makes *Router* mode more secure if the device has a public IP address.

DMZ DMZ (Demilitarized Zone) specifically allows one computer/device behind NAT to become "demilitarized", so all ports from the public network are forwarded to the ports of this private network, similar to a 1:1 NAT.

- **DMZ Management Ports** The airOS device responds to requests from the external network as if it were the host device that is specified with the DMZ IP address. *DMZ Management Ports* is disabled by default; the device is accessible from the WAN port. If *DMZ Management Ports* is enabled, all management ports will be forwarded to the device, so you'll only be able to access the device from the LAN side.

  The default values of the management ports are:

Management Method	Management Port
HTTP/HTTPS	80/443 TCP
SSH	22 TCP
Telnet	23 TCP
SNMP	161 UDP
Discovery	10001 UDP

- **DMZ IP** Enter the IP address of the local host network device. The DMZ host device will be completely exposed to the external network.

Auto IP Aliasing If enabled, automatically generates an IP address for the corresponding WLAN/LAN interface. 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. The Auto IP always starts with 169.254.X.Y, with X and Y as the last two octets from the MAC address of the device. For example, if the MAC is 00:15:6D:A3:04:FB, then the generated unique Auto IP will be 169.254.4.251.

The *Auto IP Aliasing* setting can be useful because you can still access and manage devices even if you lose, misconfigure, or forget their IP addresses. Because an Auto IP address is based on the last two octets of the MAC address, you can determine the IP address of a device if you know its MAC address.

MAC Address Cloning When enabled, you can change the MAC address of the respective interface. This is especially useful if your ISP only assigns one valid IP address and it is associated to a specific MAC address. This is usually used by cable operators or some WISPs.

- **MAC Address** Enter the MAC address you want to clone to the respective interface. This becomes the new MAC address of the interface.

LAN Network Settings

(Available in *Router* mode only.)

LAN Interface In *Simple* view, the interface is displayed. Select the interface used for LAN connection. In *Advanced* view, click **Del** to remove the interface. If there is no interface selected, select an interface from the *Add LAN* drop-down list, and click **Add**.

IP Address The IP address of the LAN interface. In case the LAN interface is the bridge, all the bridge ports (i.e., Ethernet and WLAN interfaces) will be considered as local network interfaces. This IP will be used for routing of the local network; it will be the gateway IP for all the devices on the local network. This IP address can be used for management of the device.

Netmask Defines 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 the IP address range of 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. The netmask is used to identify the subnet to which an IP address belongs.

MTU (Available in *Simple* view.) The Maximum Transmission Unit (MTU) is the maximum frame size (in bytes) that a network interface can transmit or receive. The default is *1500*.

DHCP Server The built-in DHCP server assigns IP addresses to clients connected to the LAN interface.

- **Disable** The device does not assign local IP addresses.

- **Enable** The device assigns IP addresses to client devices on the local network.

  - **Range Start, Range End** Determines the range of IP addresses assigned by the DHCP server.
  - **Netmask** Defines 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 an IP address range of 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 identity the host. The netmask is used to identify the subnet to which an IP address belongs.
  - **Lease Time** Defines the duration for which IP addresses assigned by the DHCP server are valid. Increasing the time ensures client operation without interruption, but could introduce potential conflicts. Decreasing the lease time avoids potential address conflicts, but might cause more slight interruptions to the client while it acquires a new IP address from the DHCP server. The time is expressed in seconds.
  - **DNS Proxy** If this option is enabled, the device (LAN port) will act as the Domain Name System (DNS) proxy server, and will forward DNS requests from hosts on the local network to the real DNS server. This option is enabled by default. If disabled, specify the following:
    - **Primary DNS** Enter the IP address of the primary DNS server.
    - **Secondary DNS** Enter the IP address of the secondary DNS server.

- **Relay** Relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

  - **DHCP Server IP** Enter the IP address of the DHCP server that should get the DHCP messages.
  - **Agent-ID** Enter the identifier of the DHCP relay agent.

UPnP Enables Universal Plug-and-Play (UPnP) network protocol for gaming, video, chat, conferencing, and other applications.

Block Management Access Select this option to block management access to the LAN.

Add LAN Select an interface, and then click **Add**.

Management Network Settings

Bridge Mode
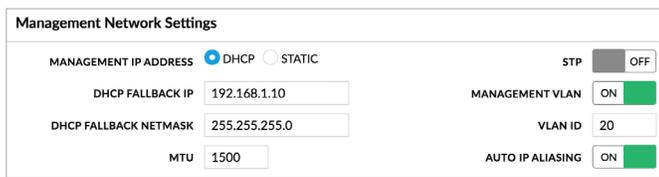
Management Network Settings

MANAGEMENT IP ADDRESS	● DHCP ○ STATIC	STP	OFF
DHCP FALLBACK IP	192.168.1.10	MANAGEMENT VLAN	ON
DHCP FALLBACK NETMASK	255.255.255.0	VLAN ID	20
MTU	1500	AUTO IP ALIASING	ON

Management Interface (Available in *Advanced* view.) Select the interface used for management.

Management IP Address Keep the default, *DHCP*, if the device obtains an IP address from its DHCP server, or click **Static** if the device uses a static IP address.

- **DHCP** The local DHCP server assigns a dynamic IP address, gateway IP address, and DNS address to the device.

MANAGEMENT IP ADDRESS	● DHCP ○ STATIC
DHCP FALLBACK IP	192.168.1.10
DHCP FALLBACK NETMASK	255.255.255.0
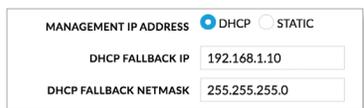
  - **DHCP Fallback IP** Enter the IP address for the device to use if a DHCP server is not found.
  - **DHCP Fallback Netmask** Enter the netmask for the device to use if a DHCP server is not found.

- **Static** Assign static IP settings to the device.

  Note: IP settings should be consistent with the address space of the device's network segment.

MANAGEMENT IP ADDRESS	○ DHCP ● STATIC
IP ADDRESS	192.168.1.20
NETMASK	255.255.255.0
GATEWAY IP	192.168.1.1
PRIMARY DNS IP	
SECONDARY DNS IP	
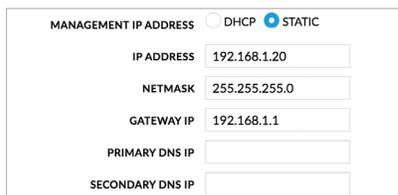
  - **IP Address** Enter the IP address of the device. This IP will be used for device management purposes.
  - **Netmask** Enter the netmask of the device. When the netmask is expanded into its binary form, it provides a mapping to define which portions of the IP address range are used for the network and which portions are used for host devices. The netmask defines the address space of the device's network segment. The 255.255.255.0 (or "/24") netmask is commonly used on many Class C IP networks.
  - **Gateway IP** Enter the IP address of the gateway device. 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 WISP gateway router. The device directs data packets to the gateway if the destination host is not within the local network.

Note: In *Bridge* mode, the gateway IP address (used for management purposes only) should be from the same address space (on the same network segment) as the device.

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

MTU (Available in *Simple* view.) Enter the desired MTU value. The default is *1500*.

STP (Available in *Simple* view.) Select this option to enable the STP feature. Multiple interconnected bridges create larger networks. Spanning Tree Protocol (STP) eliminates loops from the topology while finding the shortest path within a network.

If enabled, the device bridge communicates with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). *STP* should be disabled (default setting) when the device 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 use STP in this case.

Management VLAN (Available in *Simple* view.) Select this option to automatically create a management Virtual Local Area Network (VLAN). If this option is enabled, the device will not be accessible from other VLANs, including tagged VLANs.

- **VLAN ID** Enter a unique *VLAN ID* from 2 to 4094.

Auto IP Aliasing Select this option to automatically generate an IP address for the corresponding WLAN/LAN interface. 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. The Auto IP always starts with 169.254.X.Y, with X and Y as the last two octets from the MAC address of the device. For example, if the MAC is 00:15:6D:A3:04:FB, then the generated unique Auto IP will be 169.254.4.251.

The *Auto IP Aliasing* setting can be useful because you can still access and manage devices even if you lose, misconfigure, or forget their IP addresses. Because an Auto IP address is based on the last two octets of the MAC address, you can determine the IP address of a device if you know its MAC address.

Router Mode

Management Interface (Available in *Advanced* view.) Select the interface used for management.

Management Network Settings	
MANAGEMENT INTERFACE	LAN0 ⌄

DHCP Address Reservation

(Available in *Router* mode, *Advanced* view only.)

[Please review content below carefully; it's based on airOS 6 but modified to match airOS 8 UI functionality]

The DHCP server assigns dynamic IP addresses to its DHCP clients; however, you can map a static IP address to a specific DHCP client using its unique MAC address.

DHCP Address Reservation					
ENABLED	INTERFACE	MAC ADDRESS	IP ADDRESS	COMMENT	ACTION
No data available.					
⊕ Add					

Enabled Displays the status of the specific DHCP address reservation, Enabled (*Yes*) or Disabled (*No*).

Interface Displays the name of the interface.

MAC Address Displays the DHCP client's MAC address.

IP Address Displays the static IP address that has been assigned to the DHCP client.

Comment Displays a brief description of the purpose for the DHCP address reservation.

Action After a DHCP address reservation has been created, you have the following options:

• Click ✐ to make changes to a DHCP address reservation. Go to the *Add or Edit a DHCP Address Reservation* section below.

• Click 🗑 to remove a DHCP address reservation.

Add Click **Add** to create a new DHCP address reservation. Go to the *Add or Edit a DHCP Address Reservation* section below.

Add or Edit a DHCP Address Reservation

The *DHCP Reservation* window opens:
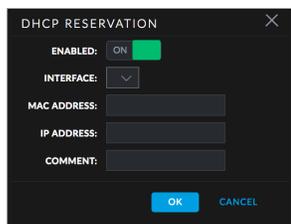
• **Enabled** Select this option to enable the DHCP address reservation. All added DHCP address reservations are saved in the system configuration file; however, only the enabled reservations are active on the device.

• **Interface** Select the appropriate interface.

• **MAC Address** Enter the MAC address of the DHCP client to which the DHCP address reservation will apply.

• **IP Address** Enter the static IP address that you want to assign to the DHCP client.

• **Comment** You can enter a brief description of the purpose for the DHCP address reservation.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

Interfaces

(Available in *Advanced* view.) You can configure a different MTU for any interface. If it is an Ethernet interface, you can also configure the speed.

Interfaces						
ENABLED	INTERFACE	MTU	SPEED	ADVERTISED LINK MODES	FLOW CONTROL	ACTION
Yes	WLAN0	1500				✐
Yes	BRIDGE0	1500				✐
Yes	LAN0	1500	Auto 10/100/1000 Mbps	10 Mbps-Half, 10 Mbps-Full, 100 Mbps-Half, 100 Mbps-Full, 1000 Mbps-Half, 1000 Mbps-Full	Disabled	✐

Enabled Displays the status of the interface, Enabled (*Yes*) or Disabled (*No*).

Interface Displays the name of the interface.

MTU Displays the MTU value.

Speed Displays the speed of the Ethernet interface.

Advertised Link Modes Displays the link modes (speed and duplex) that will be advertised.

Flow Control By using Flow Control frames (Pause requests) the device can request to stop transmitting data for a period of time. If Tx Flow Control is enabled the interface will send Pause frames when the specific interface usage threshold is met. If Rx Flow Control is enabled, the interface will process received Pause frames and will stop transmitting data for a period of time.

Action Click ✐ to change the *Enabled* status, *MTU*, *Speed*, *Advertised Link Modes*, or *Flow Control*. The *Interface* window opens:
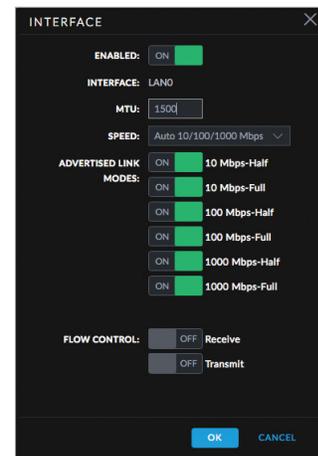
• **Enabled** Select this option to enable the interface.

• **Interface** Displays the name of the interface.

• **MTU** Enter the desired MTU value. The default is *1500*.

• **Speed** (Available only if the interface is Ethernet.) Select the appropriate option: *Auto 10/100/1000Mbps*, *100Mbps-Full*, *100Mbps-Half*, *10Mbps-Full*, or *10Mbps-Half*. We recommend using the default setting, *Auto 10/100/1000Mbps*, which is the only mode that supports gigabit (1000 Mbps) speed. In *Auto* mode, the device automatically negotiates transmission parameters, such as speed and duplex, with its counterpart. In this process, the networked devices first share their capabilities and then choose the fastest transmission mode they both support.

- **Advertised Link Modes** Select a link mode to advertise it, or deselect it to keep it from being advertised. Link modes are: *10Mbps-Half*, *10Mbps-Full*, *100Mbps-Half*, *100Mbps-Full*, *1000Mbps-Half*, and *1000Mbps-Full*.

- **Flow Control** Select *Receive* or *Transmit* to enable RX or TX flow control.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

IP Aliases

(Available in *Advanced* view.) You can configure IP aliases for the network interfaces for management purposes. For example, you may need multiple IP addresses (one private IP address and one public IP address) for a single device. If a CPE uses PPPoE, the CPE obtains a public PPPoE address, but the network administrator assigns an internal IP alias to the device. This way the network administrator can manage the device internally without going through the PPPoE server.

Enabled Displays the status of the IP alias, *Yes* or *No*.

Interface Displays the name of the interface.

IP Address Displays the alternative IP address.

Netmask Displays the network address space identifier for the IP alias.

Comment Displays a brief description of the purpose for the IP alias.

Action After an IP alias has been created, you have the following options:

- Click ✎ to make changes to an IP alias. Go to the *Add or Edit an IP Alias* section below.

- Click 🗑 to remove an IP alias.

Add Click **Add** to create an IP alias. Go to the *Add or Edit an IP Alias* section below.

Add or Edit an IP Alias

The *IP Alias* window opens:
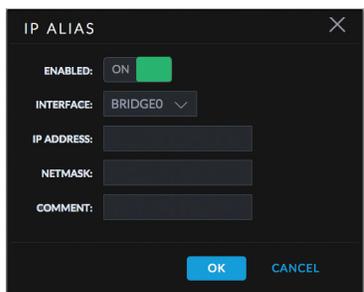
- **Enabled** Select this option to enable the specific IP alias. All the added IP aliases are saved in the system configuration file; however, only the enabled IP aliases are active on the device.

- **Interface** Select the appropriate interface.

- **IP Address** Enter the alternative IP address for the interface. This can be used for routing or device management purposes.

- **Netmask** Enter the network address space identifier for the IP alias.

- **Comment** You can enter a brief description of the purpose for the IP alias.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

VLAN Network

(Available in *Advanced* view.) You can create multiple Virtual Local Area Networks (VLANs). Click the *VLAN Network* section to display its contents.

Enabled Displays the status of the VLAN, *Yes* or *No*.

Interface Displays the name of the interface.

VLAN ID Displays the VLAN identifier.

Comment Displays a brief description of the purpose for the VLAN.

Action After a VLAN has been created, you have the following options:

- Click ✎ to make changes to a VLAN. Go to the *Add or Edit a VLAN* section below.

- Click 🗑 to remove a VLAN. (A VLAN configured as the management interface cannot be deleted.)

Add Click **Add** to create a VLAN. Go to the *Add or Edit a VLAN* section below.

Add or Edit a VLAN

The *VLAN* window opens:
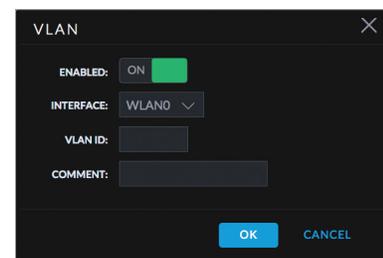
- **Enabled** Select this option to enable the specific VLAN. All the added VLANs are saved in the system configuration file; however, only the enabled VLANs are active on the device.

- **Interface** Select the appropriate interface.

- **VLAN ID** Enter the VLAN ID, a unique value assigned to each VLAN at a single device; every VLAN ID represents a different VLAN. The VLAN ID range is *2* to *4094*.

- **Comment** You can enter a brief description of the purpose for the VLAN.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

Bridge Network

(Available in *Advanced* view.) You can create one or more bridge networks if you need complete Layer 2 transparency. This is similar to using a switch – all traffic flows through a bridge, in one port and out another port, regardless of VLANs or IP addresses. For example, if you want to use the same IP subnet on both sides of a device, then you create a bridge network. Many different scenarios could require bridged interfaces, so the *Bridge Network* section is designed to allow flexibility.

Click the *Bridge Network* section to display its contents.

Bridge Network					
ENABLED	INTERFACE	STP	PORTS	COMMENT	ACTION
Yes	BRIDGE0	Disabled	LAN0, WLAN0		✏ 🗑
Yes	BRIDGE1	Disabled	WLAN0.20, LAN0.20		✏ 🗑
⊕ Add					

Enabled Displays the status of the bridge network, Enabled (*Yes*) or Disabled (*No*).

Interface Displays the name of the interface.

STP Displays the *STP* status, *Enabled* or *Disabled*.

Ports Displays the ports used for the bridge network.

Comment Displays a brief description of the purpose for the bridge network.

Action After a bridge network has been created, you have the following options:

- Click ✏ to make changes to a bridge network. Go to the *Add or Edit a Bridge Network* section below.
- Click 🗑 to remove a bridge network. (You cannot delete a bridge configured as a management interface.)

Add Click **Add** to create a bridge network. Go to the *Add or Edit a Bridge Network* section below.

Add or Edit a Bridge Network

The *Bridge* window opens:

- **Enabled** Select this option to enable the specific bridge network. All the added bridge networks are saved in the system configuration file; however, only the enabled bridge networks are active on the device.

- **Interface** Displays the name of the interface.
- **STP** Select this option to enable the STP feature. Multiple interconnected bridges create larger networks. Spanning Tree Protocol (STP) eliminates loops from the topology while finding the shortest path within a network.

  If enabled, the device bridge communicates with other network devices by sending and receiving Bridge Protocol Data Units (BPDU). *STP* should be disabled (default setting) when the device 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 use STP in this case.

- **Ports** Select the appropriate ports for your bridge network. (Virtual ports are available if you have created VLANs.)

  - **Add** Select an *Available Port* and click **Add**.
  - **Remove** Select a *Selected Port* and click *Remove*.

- **Comment** You can enter a brief description of the purpose for the bridge network.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

Static Routes

(Available in *Advanced* view.) You can manually add static routing rules to the system routing table; you can set a rule that a specific target IP address (or range of IP addresses) passes through a specific gateway. Click the *Static Routes* section to display its contents.

Static Routes					
ENABLED	TARGET NETWORK IP	NETMASK	GATEWAY IP	COMMENT	ACTION
No data available					
⊕ Add					

Enabled Displays the status of the route, Enabled (*Yes*) or Disabled (*No*).

Target Network IP Displays the IP address of the destination.

Netmask Displays the netmask of the destination.

Gateway IP Displays the IP address of the gateway.

Comment Displays a brief description of the purpose for the static route.

Action After a static route has been created, you have the following options:

- Click ✏ to make changes to a static route. Go to the *Add or Edit a Static Route* section below.
- Click 🗑 to remove a static route.

Add Click **Add** to create a static route. Go to the *Add or Edit a Static Route* section below.

Add or Edit a Static Route

The *Route* window opens:

- **Enabled** Select this option to enable the specific static route. All the added static routes are saved in the system configuration file; however, only the enabled static routes are active on the device.
- **Target Network IP** Enter the IP address of the destination.
- **Netmask** Enter the netmask of the destination.
- **Gateway IP** Enter the IP address of the gateway.
- **Comment** You can enter a brief description of the purpose for the static route.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

Firewall

(Available in *Advanced* view.) You can configure firewall rules for the network interfaces. All active firewall entries are stored in the FIREWALL chain of the ebtables filter table in *Bridge* mode, or the iptables filter table in *Router* mode. (The ebtables table is a transparent link layer filtering tool used on bridge interfaces, that allows the filtering of network traffic passing through a bridge.)

Packets are processed by sequentially traversing the firewall rules.

Click the *Firewall* section to display its contents.

Firewall Select this option to enable firewall functionality.

Enabled Displays the status of the firewall rule, Enabled (*Yes*) or Disabled (*No*).

Position Displays the order of the firewall rules.

Target Displays the firewall action for packets, *Accept* or *Drop*.

Input/Output Interface Displays the input and output interfaces specified by the firewall rule.

IP Type Displays the specific Layer 3 protocol type: *IP*, *ICMP*, *TCP*, or *UDP* being filtered.

Source IP/Mask Displays the source IP/mask of the packet that traverses the firewall rule.

Source Port Displays the source port of the packet that traverses the firewall rule.

Destination IP/Mask Displays the destination IP/mask of the packet that traverses the firewall rule.

Destination Port Displays the destination port of the packet that traverses the firewall rule.

Comment Displays a brief description of the purpose for the firewall rule.

Action After a firewall rule has been created, you have the following options:

- Click ✎ to make changes to a firewall rule. Go to the *Add or Edit a Firewall Rule* section below.
- Click ↑ or ↓ to change the order of the firewall rule entries. Order is important in the firewall rules list as packets traverse the firewall rules sequentially.
- Click 🗑 to remove a firewall rule.

Add Click **Add** to create a firewall rule. Go to the *Add or Edit a Firewall Rule* section below.

Add or Edit a Firewall Rule

The *Firewall Rule* window opens:

- **Enabled** Select this option to enable the specific firewall rule. All the added firewall rules are saved in the system configuration file; however, only the enabled firewall rules are active on the device.
- **Target** To allow packets to pass through the firewall unmodified, select **ACCEPT**. To block packets, select **DROP**.
- **Input/Output Interface** Select the appropriate input interface or output interface where the firewall rule will be applied. To apply the firewall rule to all interfaces, select **ANY**.
- **IP Type** Select which specific Layer 3 protocol type: **IP**, **ICMP**, **TCP**, or **UDP** should be filtered.
- **Source IP/Mask** Enter the source IP of the packet (specified within the packet header). Usually it is the IP of the host system that sends the packets. The mask is in slash notation (also known as CIDR format). For example, if you enter 192.168.1.0/24, you are entering the range of 192.168.1.0 to 192.168.1.255.

- **Invert** Select this option to invert the *Source IP/Mask* filtering criterion. For example, if you enable *Invert* for the specified *Source IP* a.b.c.d, then the filtering criteria will be applied to all the packets sent from any *Source IP* except a.b.c.d.

- **Source Port** Enter the source port of the packet (specified within the packet header). Usually it is the port of the host system application that sends the packets.

  - **Invert** Select this option to invert the *Source Port*. Select this option to invert the *Source Port* filtering criterion. For example, if you enable *Invert* for the specified *Source Port* 2500, then the filtering criteria will be applied to all the packets sent from any *Source Port* except 2500.

- **Destination IP/Mask** Enter 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. The mask is in slash notation (also known as CIDR format). For example, if you enter 192.168.1.0/24, you are entering the range of 192.168.1.0 to 192.168.1.255.

  - **Invert** Select this option to invert the *Destination IP/ Mask* filtering criterion. For example, if you enable *Invert* for the specified *Destination IP* a.b.c.d, then the filtering criteria will be applied to all the packets sent to any *Destination IP* except a.b.c.d.

- **Destination Port** Enter the destination port of the packet (specified within the packet header). Usually it is the port of the host system application which the packet is addressed to.

  - **Invert** Select this option to invert the *Destination Port* filtering criterion. For example, if you enable *Invert* for the specified *Destination Port* 23, then the filtering criteria will be applied to all the packets sent to any *Destination Port* except 23.

- **Comment** You can enter a brief description of the purpose for the firewall rule.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

Port Forwarding

(Available in *Router* mode only.) Port forwarding allows specific ports of the hosts on the local network to be forwarded to the external network (WAN). This is useful for a number of applications (such as FTP servers, VoIP, gaming) that require different host systems to be seen using a single common IP address/port. Click the *Port Forwarding* section to display its contents.

☑ Port Forwarding									
#	ENABLED	INTERFACE	PRIVATE IP	PRIVATE PORT	TYPE	SOURCE IP/MASK	PUBLIC IP/MASK	PUBLIC PORT	COMMENT ACTION
No data available									
⊕ Add									

Port Forwarding Select this option to enable port forwarding functionality.

Enabled Enables the specific port forwarding rule. All the added port forwarding rules are saved in the system configuration file; however, only the enabled port forwarding rules are active on the device.

Interface Displays the interface to which the port forwarding rule will be applied.

Private IP Displays the IP address of the local host that needs to be accessible from the external network.

Private Port Displays the TCP or UDP port of the application running on the local host. The specified port will be accessible from the external network.

Type Displays the Layer 3 protocol (IP) type that needs to be forwarded from the local network.

Source IP/Mask Displays the IP address and netmask of the source device.

Public IP/Mask Displays the public IP address and netmask of the device that will accept and forward the connections from the external network to the local host.

Public Port Displays the TCP or UDP port of the device that will accept and forward the connections from the external network to the local host.

Comment Displays a brief description of the port forwarding functionality, such as FTP server, web server, or game server.

Action After a port forwarding rule has been created, you have the following options:

- Click ✎ to make changes to a port forwarding rule. Go to the *Add or Edit a Port Forwarding Rule* section below.

- Click 🗑 to remove a port forwarding rule.

Add Click **Add** to create a port forwarding rule. Go to the *Add or Edit a Port Forwarding Rule* section below.

Add or Edit a Port Forwarding Rule

The *Port Forward* window opens:
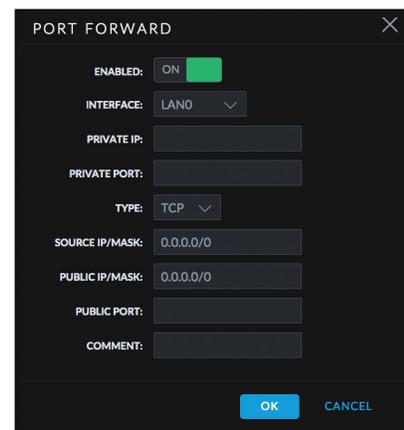
PORT FORWARD	✕
ENABLED:	ON
INTERFACE:	LAN0
PRIVATE IP:	
PRIVATE PORT:	
TYPE:	TCP
SOURCE IP/MASK:	0.0.0.0/0
PUBLIC IP/MASK:	0.0.0.0/0
PUBLIC PORT:	
COMMENT:	
	OK CANCEL

- **Enabled** Select this option to enable the specific static route. All the added static routes are saved in the system configuration file; however, only the enabled static routes are active on the device.

- **Interface** Select the interface to which the port forwarding rule will be applied.

- **Private IP** Enter the IP address of the local host that needs to be accessible from the external network.

- **Private Port** Enter the TCP or UDP port of the application running on the local host. The specified port will be accessible from the external network.

- **Type** Enter the Layer 3 protocol (IP) type that needs to be forwarded from the local network.

- **Source IP/Mask** Enter the IP address and netmask of the source device.

- **Public IP/Mask** Enter the public IP address and netmask of the device that will accept and forward the connections from the external network to the local host.

- **Public Port** Enter the TCP or UDP port of the device that will accept and forward the connections from the external network to the local host.

- **Comment** Enter a brief description of the port forwarding functionality, such as FTP server, web server, or game server.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.

Multicast Routing Settings

(Available in *Router* mode only.) 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 relies on the network to forward the packets to the hosts that need to receive them. Common routers isolate all the broadcast (thus multicast) traffic between the local and external networks; however, the device provides multicast traffic pass-through functionality. Click the *Multicast Routing Settings* section to display its contents.
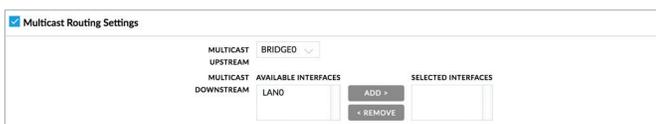
Multicast Routing Settings Select this option to enable multicast packet pass-through between local and external networks while the device is operating in *Router* mode. Multicast intercommunication is based on Internet Group Management Protocol (IGMP).

Multicast Upstream Select the source of multicast traffic.

Multicast Downstream Enter the destination(s) of multicast traffic.

- **Add** Select an *Available Interface* and click **Add**.

- **Remove** Select a *Selected Interface* and click **Remove**.

Traffic Shaping

(Available in *Advanced* view.) Traffic Shaping controls bandwidth from the perspective of the client. Bursting allows fast downloads when a user downloads small files (for example, viewing different pages of a website), but prevents a user from using excessive bandwidth when downloading large files (for example, streaming a movie).

As Layer 3 QoS, you can limit the traffic at the device at the interface level, based on a rate limit you define. Each interface has two types of traffic:

- **Ingress** traffic entering the interface

- **Egress** traffic exiting the interface

We recommend using Traffic Shaping to control egress traffic, because it is more efficient in the egress direction. When an interface accepts ingress traffic, it cannot control how quickly the traffic arrives – the sending device controls that traffic. However, when an interface sends out egress traffic, it can control how quickly the traffic exits.

Bursting allows the bandwidth to spike higher than the maximum bandwidth you configure in the *Ingress* and *Egress Rate* settings – for a short period of time. Once the *Ingress* or *Egress Burst* (volume of data) is used up, the throughput drops back down to the corresponding *Ingress* or *Egress Rate* setting (maximum bandwidth) you have set.

For example, you have the following conditions:

- *Egress Burst* is set to 2048 kBytes.

- *Egress Rate* is set to 512 kbit/s.

- Actual maximum bandwidth is 1024 kbit/s.

Bursting allows 2048 kBytes to pass at 1024 kbit/s before throttling down to 512 kbit/s.

Click the *Traffic Shaping* section to display its contents.

Traffic Shaping Select this option to enable bandwidth control on the device.

Enabled Displays the status of the rule, Enabled (*Yes*) or Disabled (*No*).

Interface Displays the name of the interface.

Ingress Displays the *Ingress* status, *Enabled* or *Disabled*.

Ingress Rate, kbps Displays the maximum ingress bandwidth.

Ingress Burst, kB Displays the maximum amount of data in kilobytes allowed to burst beyond the *Ingress Rate*.

Egress Displays the *Egress* status, *Enabled* or *Disabled*.

Egress Rate, kbps Displays the maximum egress bandwidth.

Egress Burst, kB Displays the maximum amount of data in kilobytes allowed to burst beyond the *Egress Rate*.

Action After a traffic shaper rule has been created, you have the following options:

- Click 🖉 to make changes to a traffic shaper rule. Go to the *Add or Edit a Traffic Shaper Rule* section below.

- Click 🗑 to remove a traffic shaper rule.

**Add** Click **Add** to create a traffic shaper rule. Go to the *Add or Edit a Traffic Shaper Rule* section below.

Add or Edit a Traffic Shaper Rule

The *Traffic Shaper Rule* window opens:
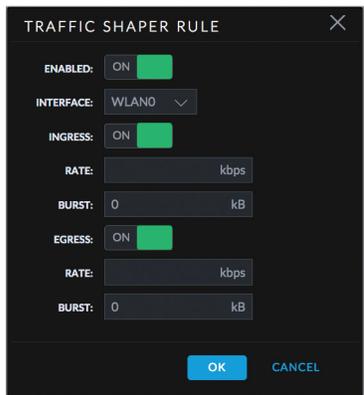
- **Enabled** Select this option to enable the specific rule. All the added rules are saved in the system configuration file; however, only the enabled rules are active on the device.

- **Interface** Select the appropriate interface.

- **Ingress** Select this option to enable the ingress values.
  - **Rate** Enter the maximum bandwidth value (in kilobits per second) for traffic entering the specified interface.
  - **Burst** Enter the data volume (in kilobytes) that is allowed before the ingress maximum bandwidth applies.

- **Egress** Select this option to enable the egress values.
  - **Rate** Enter the maximum bandwidth value (in kilobits per second) for traffic exiting the specified interface.
  - **Burst** Enter the data volume (in kilobytes) that is allowed before the egress maximum bandwidth applies.

Click **OK** to save changes, or click *Cancel* to close the window without saving changes.
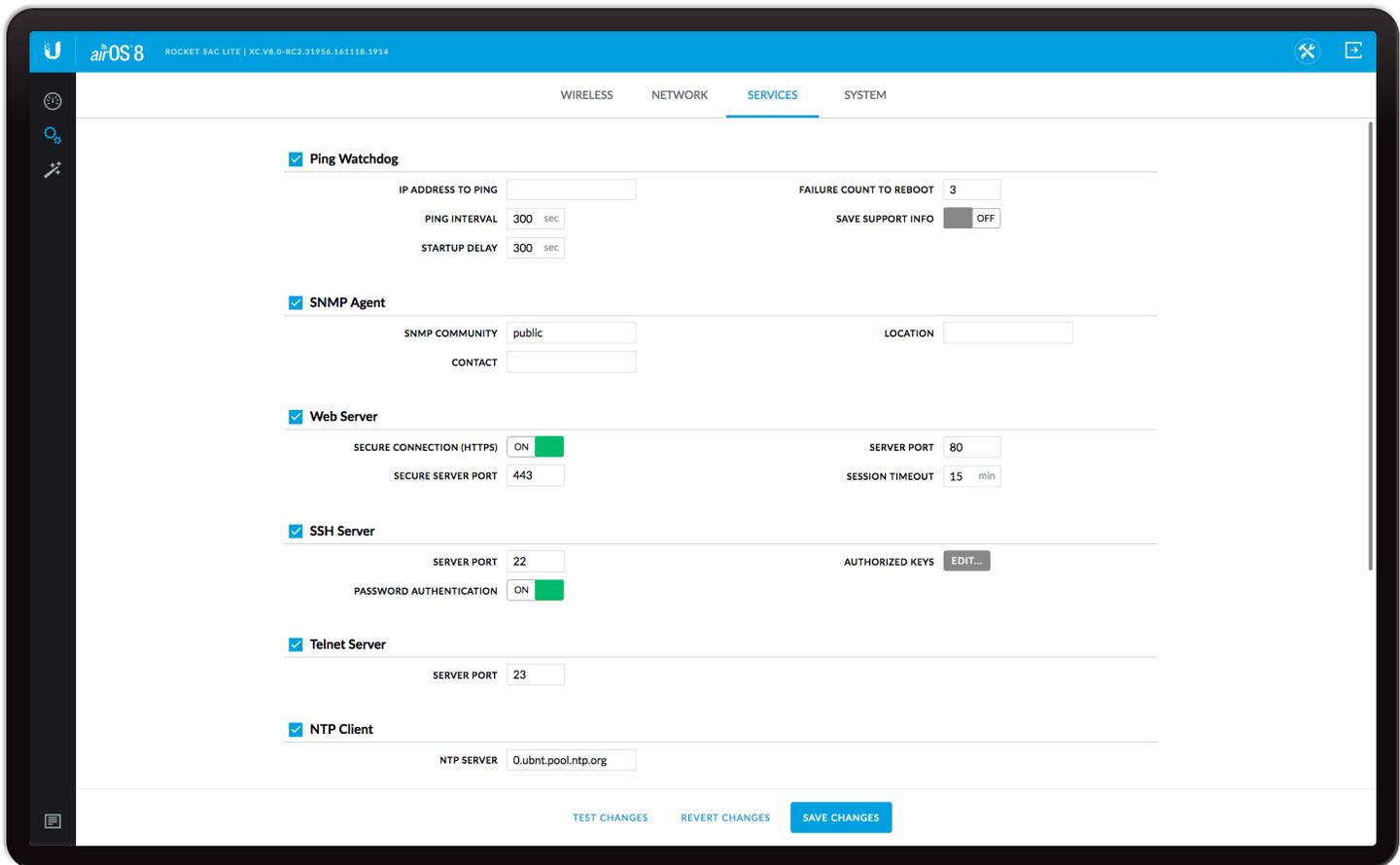
Chapter 5: Services

The *Services* page configures system management services: Ping Watchdog, SNMP, servers (web, SSH, Telnet), NTP, DDNS, system log, and device discovery.

Ping Watchdog

Ping Watchdog sets the device 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, then the device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

Ping Watchdog is dedicated to continuous monitoring of the specific connection to the remote host using the Ping tool. The Ping tool 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.

Ping Watchdog Select this option to enable use of Ping Watchdog.

IP Address To Ping Enter the IP address of the target host to be monitored by Ping Watchdog.

Ping Interval Enter the time interval (in seconds) between the ICMP echo requests that are sent by Ping Watchdog. The default value is *300* seconds.

Startup Delay Enter the initial time delay (in seconds) until the first ICMP echo request is sent by Ping Watchdog. The default value is *300* seconds.

The *Startup Delay* value 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 Enter the number of ICMP echo response replies. If the specified number of ICMP echo response packets is not received continuously, Ping Watchdog will reboot the device. The default value is *3*.

Save Support Info Select this option to generate a support information file in case the Ping Watchdog will reboot the device.

SNMP Agent

Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. Network administrators use SNMP to monitor network-attached devices for issues that warrant attention.

The device contains an SNMP agent, which does the following:

- Provides an interface for device monitoring using SNMP
- Communicates with SNMP management applications for network provisioning
- Allows network administrators to monitor network performance and troubleshoot network problems

For the purpose of equipment identification, configure the SNMP agent with contact and location information:

SNMP Agent Select this option to enable the SNMP agent.

SNMP Community Enter the SNMP community string. It is required to authenticate access to Management Information Base (MIB) objects and functions as an embedded password. The device supports a read-only community string; authorized management stations have read access to all the objects in the MIB except the community strings, but do not have write access. The device supports SNMP v1. The default is *public*.

Contact Enter the name of the contact who should be notified in case of emergency.

Location Enter the physical location of the device.

Web Server

This section manages the *Web Server* parameters.

Web Server HTTP service is enabled by default.

Secure Connection (HTTPS) Secure HTTPS mode is enabled by default.

Secure Server Port If secure HTTPS mode is enabled, enter the TCP/IP port of the web server. The default is *443*.

Server Port If HTTP mode is enabled, enter the TCP/IP port of the web server. The default is *80*.

Session Timeout Enter the maximum timeout before the session expires. Once a session expires, you must log in again using the username and password. The default is *15* minutes.

SSH Server

This section manages the *SSH Server* parameters.

SSH Server SSH access to the device is enabled by default.

Server Port Enter the TCP/IP port of the SSH server. The default is *22*.

Password Authentication Enabled by default. You must authenticate using administrator credentials to grant SSH access to the device; otherwise, an authorized key is required.

Authorized Keys Click **Edit** to import a public key file for SSH access to the device instead of using an admin password. The *SSH Authorized Keys* window opens.

- **Browse** Use this option to add a new key. Click **Browse** to locate the new key file. Select the file and click **Open** to import the file for SSH access.
- **Enabled** Select this option to enable the specific key. All of the added keys are saved in the system configuration file; however, only the enabled keys are active on the device.
- **Type** Displays the type of key.
- **Key** Displays the key.
- **Comment** You can enter a brief description of the key. You can edit this field for multiple keys at the same time.
- **Action** You have the following options:
  - **Remove** Deletes a public key file.
- **OK** Click **OK** to save changes.
- **Cancel** Click *Cancel* to discard changes.

Telnet Server

This section manages the *Telnet Server* parameters.

Telnet Server Select this option to enable Telnet access to the device.

Server Port Enter the TCP/IP port of the Telnet server. The default is *23*.

NTP Client

Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. You can use it to set the real system time on the device. If the *System Log* option is enabled, then the system time is reported next to every log entry that registers a system event.

NTP Client Select this option to enable the device to obtain the system time from a time server on the Internet.

NTP Server Enter the IP address or domain name of the NTP server. The default is: *0.ubnt.pool.ntp.org*

Dynamic DNS

Domain Name System (DNS) translates domain names to IP addresses; each DNS server on the Internet holds these mappings in its respective DNS database. Dynamic Domain Name System (DDNS) is a network service that notifies the DNS server in real time of any changes in the device's IP settings. Even if the device's IP address changes, you can still access the device through its domain name.

Dynamic DNS Select this option to enable the device to communicate with the DDNS server.

Service If available, select your DDNS service provider from the drop-down list.

Host Name Enter the host name of the device, that has to be updated on the DDNS server. For example: *sample.ddns.com*

Username Enter the user name of the DDNS account.

Password Enter the password of the DDNS account.

Show Click **Show** to display the password characters.

System Log

Every logged message contains at least a system time and specific service name that generates the system event. Messages from different services have different contexts and different levels of detail. Usually error, warning, or informational system service messages are reported; however, more detailed debug level messages can also be reported. The more detailed the system messages reported, the greater the volume of log messages generated.

System Log Enabled by default. The device runs the registration routine of system log (syslog) messages.

Remote Log Select this option to enable the syslog remote sending function. System log messages are sent to a remote server, which is specified in the *Remote Log IP Address* and *Remote Log Port* fields.

Remote Log IP Address Enter the host IP address that receives syslog messages. Properly configure the remote host to receive syslog protocol messages.

Remote Log Port Enter the TCP/IP port that receives syslog messages. *514* is the default port for commonly used system message logging utilities.

Device Discovery

This section manages the *Device Discovery* parameters.

Discovery Enabled by default. The device can be discovered by other Ubiquiti devices or by the Ubiquiti Device Discovery tool which you can download from: **http://www.ubnt.com/download/**

CDP Select this option to enable Cisco Discovery Protocol (CDP) communications, so the device can send out CDP packets to share its information.
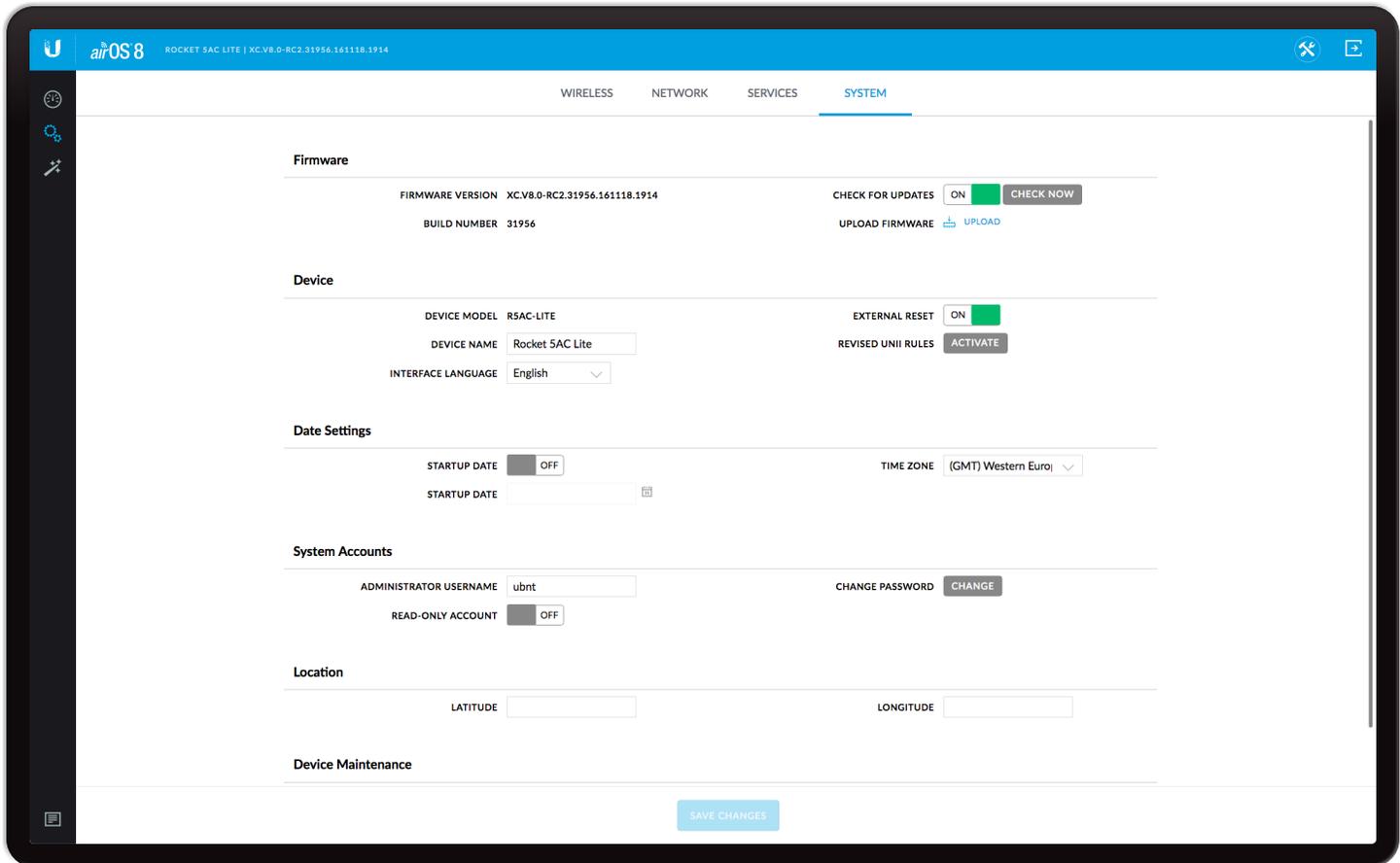
Chapter 6: System

The *System* page contains administrative options. This page enables the administrator to reboot the device, reset it to factory defaults, upload new firmware, back up or update the configuration, and configure the administrator account.

Firmware Update

This section manages the firmware maintenance.

Firmware Version Displays the current firmware version.

Build Number Displays the build number of the firmware version.

Check for Updates Enabled by default, this option automatically checks for firmware updates. To manually check for an update, click **Check Now**.

If an update is found, click **Download** to download the update. Otherwise, click **Dismiss** to cancel.

After you click *Download*, the *Ubiquiti Firmware License Agreement* window appears. Click **Agree** to accept the terms of the license agreement. On the *System* page, click **Upload** to upload the downloaded firmware to the device.

Upload Firmware Click **Upload** to locate the new firmware file. Select the file and click **Open** to upload the file.

> **Note:** The device firmware update is compatible with all configuration settings. The system configuration is preserved while the device is updated with a new firmware version. However, we recommend that you back up your current system configuration before updating the firmware

The uploaded firmware file is displayed. You have two options:

- **Update** Click **Update** to confirm. After the device reboots, the firmware update process will be completed.
- **Discard** Click *Discard* to cancel.

If the firmware update is in process, you can close the firmware update window, but this does not cancel the firmware update. Please be patient, as the firmware update routine can take three to seven minutes. You cannot access the device until the firmware update routine is completed.

> **WARNING:** Do not power off, do not reboot, and do not disconnect the device from the power supply during the firmware update process as these actions will damage the device!

Device

The *Device Name* (host name) is the system-wide device identifier. The SNMP agent reports it to authorized management stations. The *Device Name* will be used in popular router operating systems, registration screens, and discovery tools.

Device		
DEVICE MODEL	R5AC-LITE	EXTERNAL RESET ON
DEVICE NAME	Rocket 5AC Lite	REVISED UNII RULES ACTIVATE
INTERFACE LANGUAGE	English	

Device Model Displays the abbreviated model name of the device.

Device Name Enter a host name or identifier for the device.

Interface Language Select the language used in the web management interface. *English* is the default language.

External Reset Select this option to enable remote PoE reset functionality. To prevent an accidental reset to default settings, disable this option (disables the remote PoE reset functionality).

> Note: The *External Reset* option is not supported on the following models:
> - LBE-5AC-23
> - LBE-5AC-16-120
> - NBE-5AC-16
> - PBE-5AC-300
> - PBE-5AC-400
> - PBE-5AC-300-ISO
> - PBE-5AC-400-ISO

> Note: You can reset the device to default settings through *Configuration Management > Reset to Factory Defaults* on this page. You can also reset the device using the hardware reset button (it will remain functional even if the *External Reset* option is not selected).

Revised UNII Rules This option is available if DFS (Dynamic Frequency Selection) frequencies in the UNII-2 band (5.25 - 5.725 GHz) should be available for your device but are locked. To unlock the DFS frequencies, follow these instructions:

1. Visit **www.ubnt.com/fcclabelrequest** and follow the online instructions to request the activation key and FCC labels.
2. After you have received your activation key and FCC labels, click **Activate** next to *Revised UNII Rules*.
3. The Revised UNII Rules window appears.

REVISED UNII RULES

For more information about revised UNII rules activation, please visit www.ubnt.com/fcclabelrequest to request a unique activation code for your company.

⚠ **Warning**

Enabling new UNII rules will reduce EIRP limits for UNII-3 (5.8 GHz) band. Note: Activating new rules on longer-distance links may affect performance. Device will restart after activation and new rules will be in effect.

COMPANY NAME

KEY

ACTIVATE   CANCEL

4. In the *Company Name* field, enter the company name you provided when you requested the activation key.
5. In the *Key* field, enter the activation key.
6. Click **Activate**.
7. Apply the FCC labels to the appropriate device(s).

> **WARNING:** Enabling the new UNII rules will reduce EIRP limits for the UNII-3 (5.8 GHz) band. Note: Activating new rules on longer-distance links may affect performance. Device will restart after activation and new rules will be in effect.

Date Settings

Date Settings		
STARTUP DATE	OFF	TIME ZONE (GMT) Western Euro
STARTUP DATE		

Time Zone Select the appropriate time zone according to Greenwich Mean Time (GMT).

Startup Date To change the device's startup date, select this option, and then specify the date. You have two options:

- **Manual** Enter the startup date.
- **Calendar** Click the 🗓 icon to display the monthly calendar. Then, click the startup date.

‹	January 2017	›
Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

System Accounts

You can change the administrator password to protect your device from unauthorized changes. We recommend that you change the default administrator password during the very first system setup:

System Accounts

ADMINISTRATOR USERNAME	ubnt	CHANGE PASSWORD	CHANGE
READ-ONLY ACCOUNT	OFF		

Administrator Username Enter the name of the administrator.

Change Password Click **Change** to change the administrator password. The *Change Password* window opens:

CHANGE PASSWORD ✕

CURRENT PASSWORD:

NEW PASSWORD:

VERIFY NEW PASSWORD:

PASSWORD STRENGTH:

CHANGE   CANCEL

- **Current Password** Enter the current password for the administrator account. This is required to change the *Password* or *Administrator Username*.

- **New Password** Enter the new password for the administrator account. airOS will indicate that the password is *Too Short* if it has fewer than eight characters. As you enter the new password, airOS will indicate its strength: *Weak*, *Normal*, or *Strong*.

  > Note: The password length is 4 characters minimum and 63 characters maximum; we recommend using at least 8 characters.

- **Verify New Password** Re-enter the new password for the administrator account.

- **Change** Click **Change** to save the new password.

- **Cancel** Click *Cancel* to discard the new password.

Read-Only Account Select this option to create a read-only user account. Then, enter the following information:

- **Read-Only Account Name** Enter the account name.

- **Change Read-Only User Password** Click **Change** to set or change the read-only account password. Enter the new password, enter it again to verify, and click **Change** to save or *Cancel* to exit without saving.

Location

(Not available on Rocket 5ac Prism, which features built-in GPS functionality.)

Latitude and longitude define the device's coordinates.

Location

LATITUDE		LONGITUDE	

Latitude Enter the latitude of the device's location. Valid values for latitude are -90 to +90.

Longitude Enter the longitude of the device's location. Valid values for longitude are -180 to +180.

Device Maintenance

This section manages the device maintenance routines: reboot, reset the device to factory default settings, the device configuration routines, and support information reports.

Device Maintenance

⟳ REBOOT DEVICE	⬇ BACK UP CONFIGURATION	⬇ DOWNLOAD SUPPORT INFO
⬡ RESET TO FACTORY DEFAULTS	⬆ UPLOAD CONFIGURATION	

Reboot Device Click **Reboot...** to initiate a full reboot cycle of the device. Reboot is the same as the hardware reboot, which is similar to the power-off and power-on cycle. The system configuration stays the same after the reboot cycle completes. Any changes that have not been applied are lost.

Reset to Factory Defaults Click **Reset...** to reset the device to the factory default settings. This option will reboot the device, and all factory default settings will be restored. We recommend that you back up your current system configuration before resetting the device to its defaults.

Back Up Configuration Click **Back Up Configuration** to download the current system configuration file.

> Note: We strongly recommend that you save the configuration file in a secure location because the configuration file includes confidential information, such as WPA2 keys in plain text.

Upload Configuration Click **Upload Configuration** to locate the new configuration file. Select the file and click **Open** to upload the file. We recommend that you back up your current system configuration before uploading the new configuration.

> Note: Use only configuration files for the same type of the device. Behavior may be unpredictable if you mix configuration files from different types of devices. (For example, upload an R5AC-Lite configuration file to an R5AC-Lite; do NOT upload an R5AC-Lite configuration file to an R5AC-PTP.)

The uploaded configuration file is displayed. You have two options:

- **Apply** Click **Apply** to confirm. After the device reboots, the settings of the new configuration are displayed in the web management interface.

- **Discard** Click *Discard* to cancel.

Download Support Info Click **Download Support Info** to generate and download a support information file that Ubiquiti support engineers can use when providing customer support. This file only needs to be generated at their request.
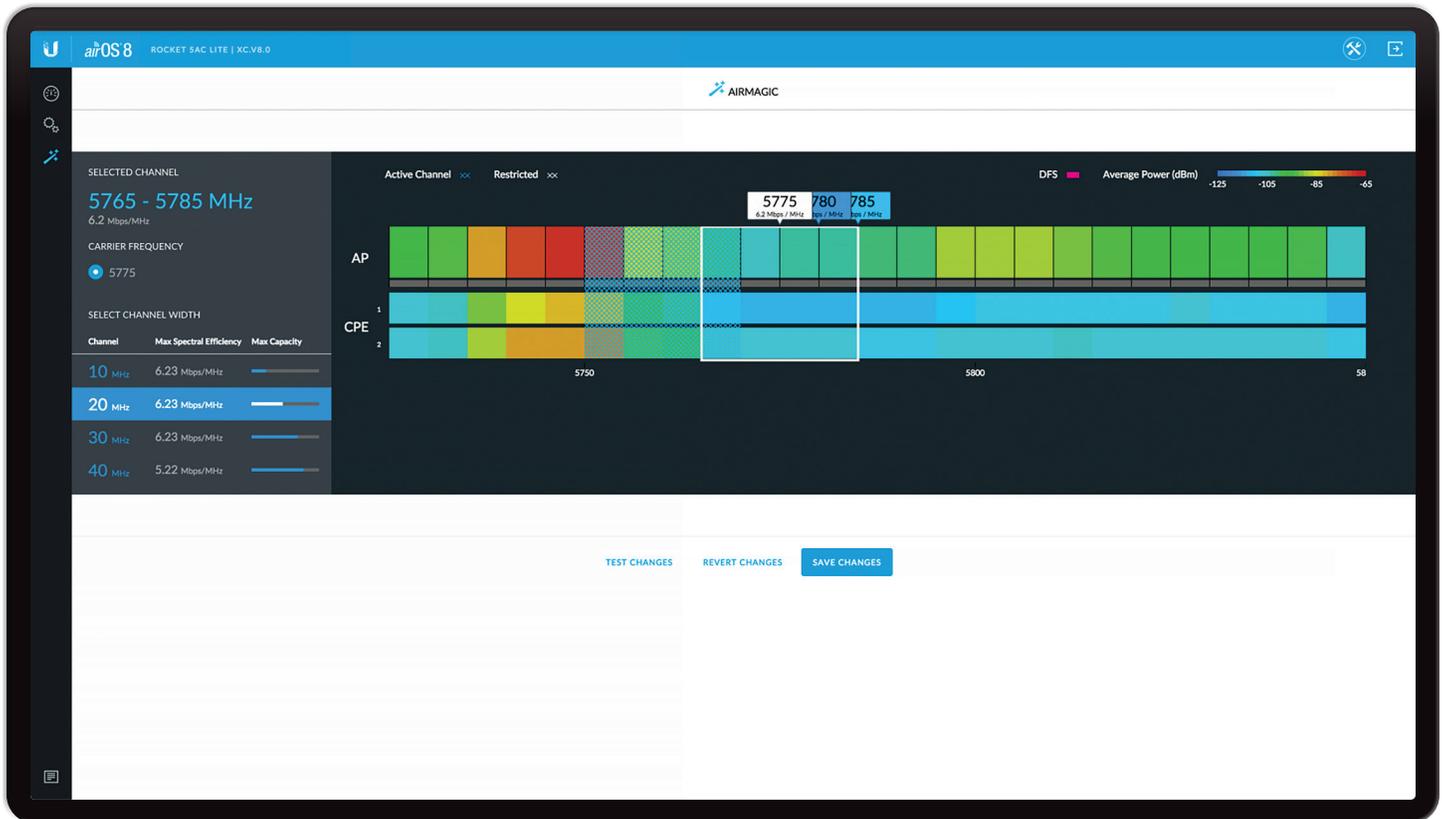
Chapter 7: airMagic

📝 **Note:** The airMagic tool is available only if the *Wireless Mode* is set to an AP mode. For information on the *Wireless Mode*, refer to **"Wireless Mode" on page 13**.

The *airMagic* page displays the airMagic tool. Using a dedicated co-processor, airOS 8 collects network-wide RF metrics to make real-time scheduling decisions. airMagic provides system-based spectrum analysis and recommends the top three channels based on spectral efficiency, capacity, and remote/local RF environment reporting.

airMagic Display

The *airMagic* page displays channel information on the left, and spectral analysis information on the right. The left side of the window displays the following:

- **Selected Channel** This is the currently selected channel.
- **Carrier Frequency** This indicates the carrier frequency of the selected channel.
- **Select Channel Width** The list of available channel widths (determined by the *Wireless Mode* setting; for details, see **"Channel Width" on page 15**). The highlight indicates the current channel width setting (specified by the *Channel Width* option in *Settings > Wireless*). The channel width information includes:
  - **Channel** The width of the channel in MHz
  - **Max Spectral Efficiency** The channel's maximum spectral efficiency expressed as Mbps/MHz.
  - **Max Capacity** A bar graph showing the maximum capacity of the channel.

The right side of the window displays the following:

- **Active Channel** Blue cross-hatching indicates the currently active channel.

- **Restricted** White cross-hatching indicates restricted channels (determined by your country code).

- **DFS** Dynamic Frequency Selection (DFS) frequencies are indicated by magenta.

DFS

- **Average Power** Shows how to interpret the colors in the display. Red indicates the highest interference levels; blue indicates the lowest interference levels.

Average Power (dBm)
-125   -105   -85   -65

- **AP** A graphical representation of the spectrum usage near the AP.

AP

- **CPE** A graphical representation of the spectrum usage near each CPE device in the network (the devices are numbered consecutively starting from 1). If you position the cursor over a particular CPE, airMagic displays the following information for the CPE: *MAC*, *Model*, *Name*, *Last IP*, *Signal TX/RX*, *Connection Time*, and *Distance*. If a CPE is disconnected, the CPE's row becomes gray.

CPE
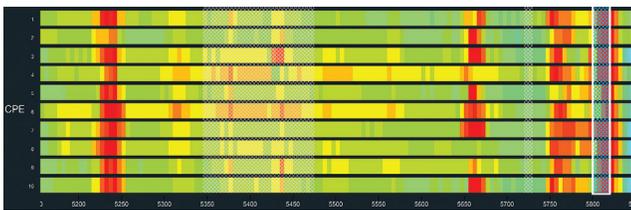
- Tags above the spectral display identify the three channels that airMagic has determined to be the best based on spectral efficiency, capacity, and remote/local RF environment reporting. Tags are labeled with the channel's carrier frequency and aggregate spectral efficiency in Mbps/MHz. Place the cursor over a tag to highlight the channel. Click the tag to select the channel (it will be displayed as the *Selected Channel* on the left side of the window).

5775   5780   5785
6.2 Mbps / M   6.2 Mbps / MHz   Mbps / MHz

Using airMagic

Follow these instructions to use airMagic:

1. If the *airMagic* page is not displayed, click the ⚡ icon in the navigation bar on the left of the interface.

2. The *airMagic* page appears. Wait for airMagic to make its calculations; when done, it displays its results.

3. If you want to change the channel width (the current channel width is highlighted on the left side of the window), select the new channel width now.

   Note: In general, a smaller channel size is preferable, since it yields better spectral efficiency for higher-capacity data networks while also scaling better, allowing for more co-located networks.

4. On the right side of the window, airMagic identifies the three channels that it has determined to be the best. To select one of these channels, click its tag and click **Save Changes**.

5. The Access Point will now have the new channel settings.

Depending on their settings, the stations may become disconnected. If this happens, modify the channel settings on the stations to allow them to reconnect to the AP.

   Note: A station will remain connected only if its *Channel Width* is set to either *Auto 20/40/80 MHz* (*Station PTP* mode) or *Auto 20/40 MHz* (*Station PTMP* mode) and the AP's new channel width is one of the *Auto* channel widths.
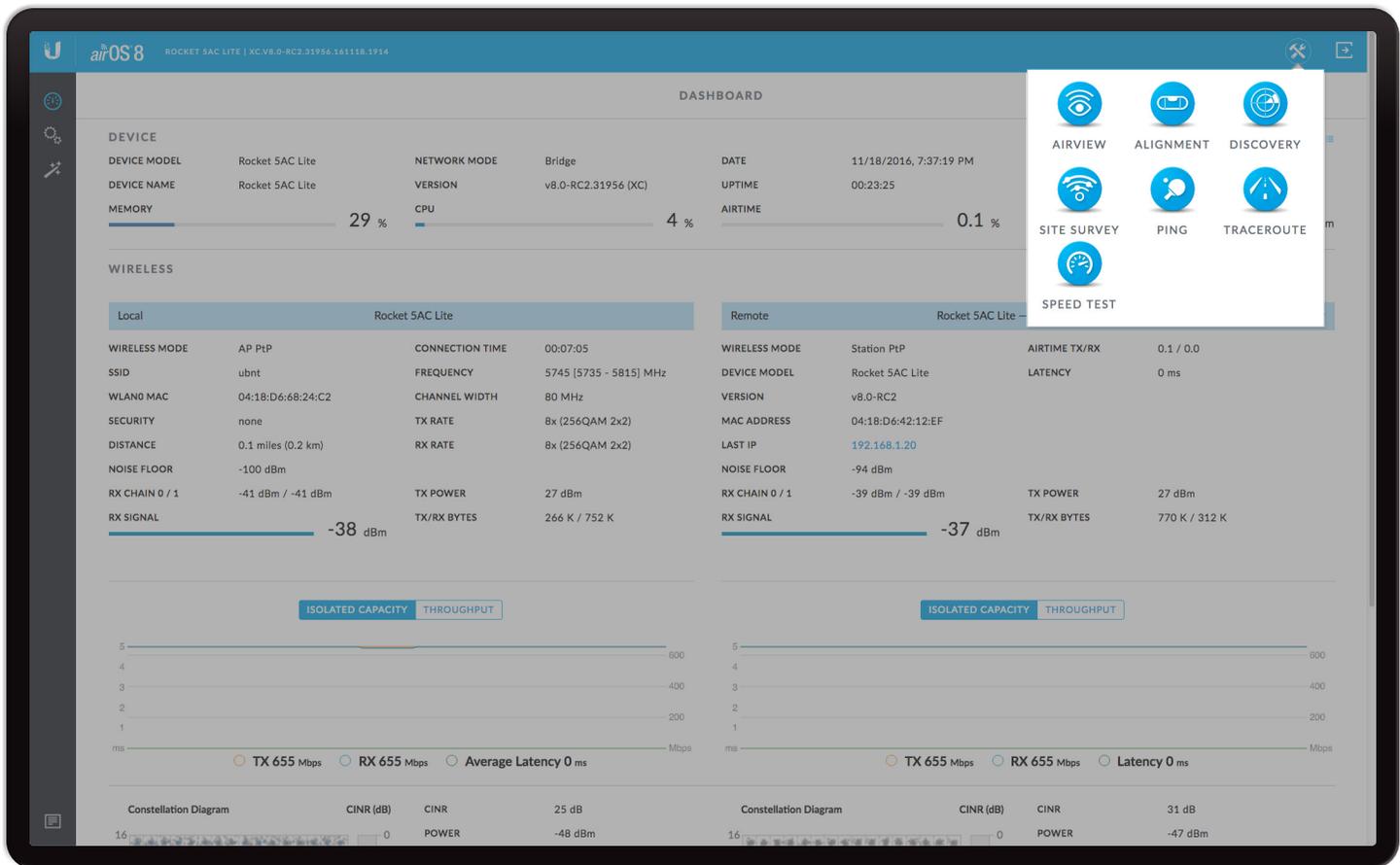
Chapter 8: Tools and Information

Each page of the airOS interface contains the ⚒ icon which provides links to tools and information. The icon is found near the upper-right corner of the window.

When you click ⚒ the following list of network administration and monitoring tools is displayed:

- **"airView" on page 45**
- **"Alignment" on page 47**
- **"Discovery" on page 47**
- **"Site Survey" on page 48**
- **"Ping" on page 48**
- **"Traceroute" on page 49**
- **"Speed Test" on page 49**

Click 🗐 near the bottom-left corner of any window to display log information (refer to **"Log" on page 50**).

airView

The airView® Spectrum Analyzer allows you to identify noise signatures so you can plan your wireless network to optimize RF performance and minimize interference.

airView constantly monitors RF environmental noise and displays energy data points in multiple spectral views at a rapid frame rate.

Powered by a second, dedicated radio, airView runs 100% in the background without disabling the wireless link.
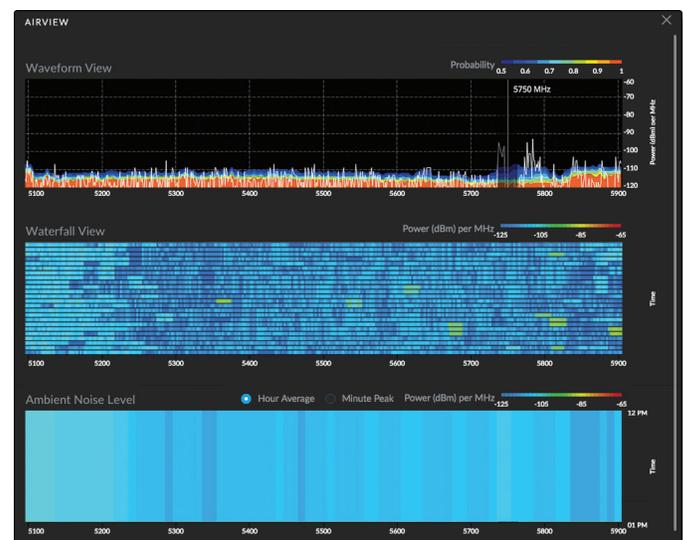
Use the controls in the upper-right corner to maximize or close the airView window.

You can place the cursor at a specific frequency to highlight that frequency across the three spectral views, each of which represents different data.
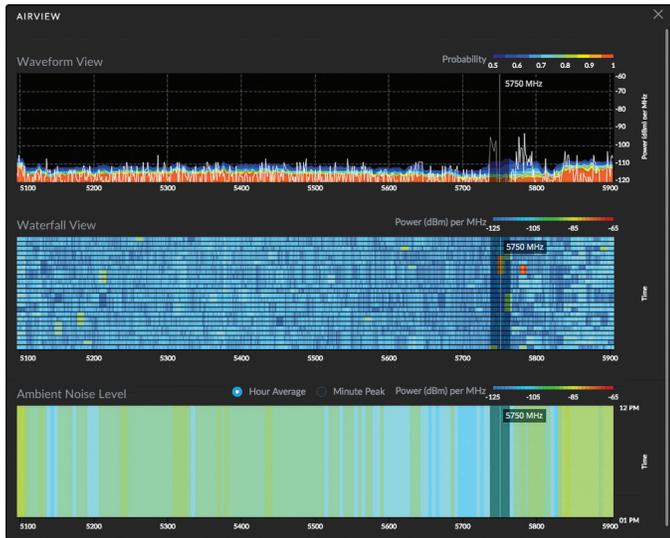
These are the three views:

- **"Waveform View" on page 46**
- **"Waterfall View" on page 46**
- **"Ambient Noise Level" on page 46**

Waveform View
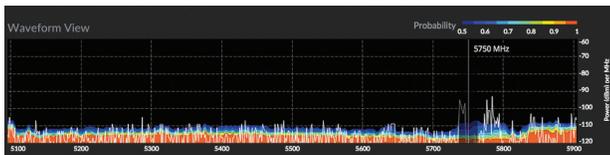
This activity-based graph shows the aggregate energy collected since the start of the airView session. The power of the energy (in dBm) is shown across the frequency span. Cooler colors (such as blue and darker colors) represent energy of a specific strength and frequency appearing at a relatively low occurrence rate, whereas increasingly warmer colors (from green to yellow to orange to red) represent energy of a specific strength and frequency appearing at a higher rate of occurrence.

> **Note:** Energy is the power ratio in decibels (dB) of the measured power referenced to one milliwatt (mW).

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

The legend at the top-right corner provides a numerical guide associating the various colors to probability levels, from 0 (least likely to occur) to 1 (most likely to occur).

Waterfall View
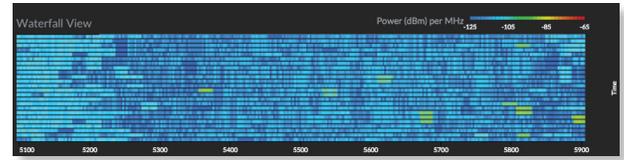
This time-based graph shows the aggregate energy collected since the start of the airView session for each frequency. The power of the energy (in dBm) is displayed across the frequency span, and a new row is inserted every few seconds.

The energy color designates the amplitude (or strength) of the signal. Cooler colors represent lower energy levels (with blue representing the lowest levels) in that frequency bin, and warmer colors (yellow, orange, or red) represent higher energy levels in that frequency bin.

The legend at the top-right corner provides a numerical guide associating the various colors to power levels (in 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 airView session.

Ambient Noise Level
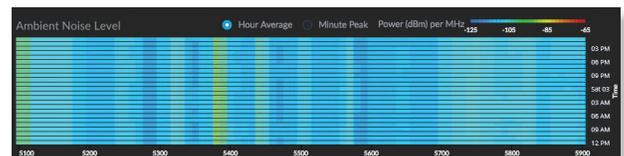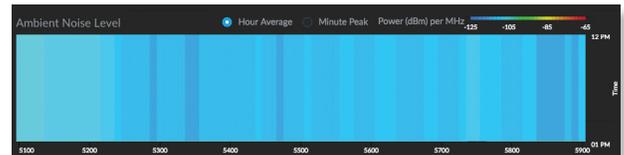
This time-based graph shows the ambient energy (in dBm) per minute or per hour as a function of frequency. Select **Minute Peak** (default) or **Hour Average** to set the time interval. The graph initially shows data for the most recent minute or hour, as shown by the first graph above. Data for each subsequent minute or hour is added to the graph until there are 24 minutes or 24 hours of data, as shown by the second graph above. After that, only the most recent 24 minutes or 24 hours are shown.

The energy color designates the amplitude (or strength) of the ambient noise. Cooler colors represent lower energy levels (with blue representing the lowest levels) in that frequency bin, and warmer colors (yellow, orange, or red) represent higher energy levels in that frequency bin.

The legend at the top-right corner provides a numerical guide associating the various colors to power levels (in dBm).

Alignment

Use this tool to point and optimize the antenna in the direction of maximum link signal. The *Antenna Align Tool* window reloads every second.

ANTENNA ALIGN TOOL   ✕

Signal Level	
Current Signal	**-40 dBm**
Max Signal Reached	**-39 dBm**
Chain 0	
Current Signal	**-45 dBm**
Max Signal Reached	**-45 dBm**
Chain 1	
Current Signal	**-41 dBm**
Max Signal Reached	**-41 dBm**
Max Signal	-66 dBm
Audio Indicator [?]	OFF
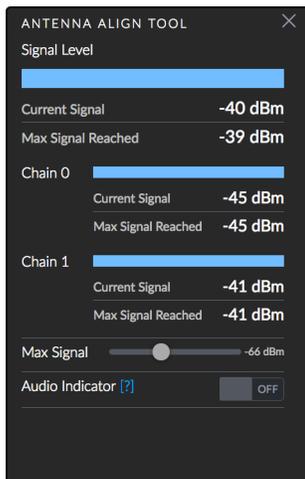
Signal Level Displays the signal strength of the last received packet.

- **Current Signal** Displays the current signal level.
- **Max Signal Reached** Displays the maximum signal level reached.

Chain Displays the wireless signal level (in dBm) of each chain, if there is more than one chain. (The number of chains is device-specific.)

- **Current Signal** Displays the current signal level of the chain.
- **Max Signal Reached** Displays the maximum signal level reached by the chain.

Max Signal Displays the maximum signal strength (in dBm). Use the slider to adjust the range of the *Signal Level* and *Chain* meters to be more sensitive to signal fluctuations (it changes an offset of the maximum indicator value).

Audio Indicator Enabling the audio option allows a technician to align the antenna of an airMAX ac device without looking at the airOS Configuration Interface. The higher the pitch, the stronger the signal strength. Each rise in pitch correlates to an increase in the received signal level.

Discovery

The *Device Discovery* tool searches for all Ubiquiti devices on your network.
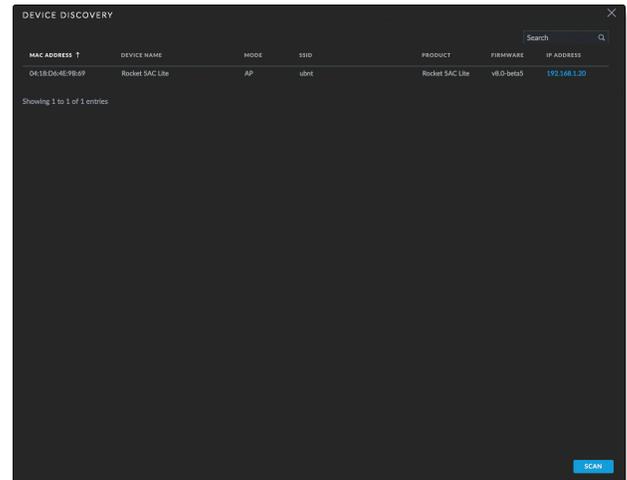
DEVICE DISCOVERY   ✕

MAC ADDRESS ↑	DEVICE NAME	MODE	SSID	PRODUCT	FIRMWARE	IP ADDRESS
04:18:D6:4E:9B:69	Rocket 5AC Lite	AP	ubnt	Rocket 5AC Lite	v8.0-beta5	192.168.1.20

Showing 1 to 1 of 1 entries

SCAN

Search As you enter keywords, the *Search* field automatically filters the device results.

The *Device Discovery* tool reports the following for each result:

MAC Address Displays the MAC address or hardware identifier of the device.

Device Name Displays the hostname or identifier of the device.

Mode Displays the operating mode of the wireless device, *AP* or *STA* (Station).

SSID Displays the wireless network name.

Product Displays the product name.

Firmware Displays the version number of the device's firmware.

IP Address Displays the IP address of the device. To access a device configuration through its web management interface, click the device's IP address.

Scan To refresh the device discovery results, click **Scan**.

Site Survey

The *Site Survey* tool searches for wireless networks in range on all supported frequencies.
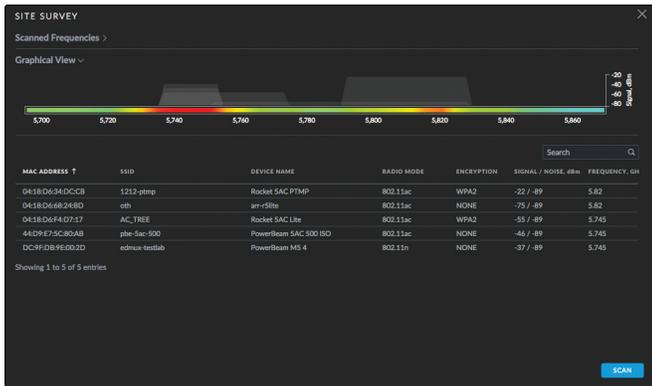
Scanned Frequencies Displays the scanned frequencies list. In *Station PTP* or *Station PTMP* mode, you can edit this list; for details, see **"Control Frequency Scan List, MHz" on page 15**.

Graphical View Displays a graphical view of the signal strength in dBm for each connected device.

Search As you enter keywords, the *Search* field automatically filters the device results.

The *Site Survey* tool reports the following for each result:

MAC Address Displays the MAC address of the wireless interface of the device.

SSID Displays the wireless network name.

Device Name Displays the hostname or identifier of the device.

Radio Mode Displays the technology used by the device, *airMAX AC* for airMAX ac devices.

Encryption Displays the encryption method, *WPA2* or *NONE*.

Signal/Noise, dBm Displays the signal strength and noise values.

Frequency, GHz Displays the frequency used by the device.

Scan To refresh the site survey results, click **Scan**.

Ping

You can ping other devices on the network directly from the device. The *Ping* tool uses Internet Control Message Protocol (ICMP) packets to check the preliminary link quality and packet latency estimation between two network devices.
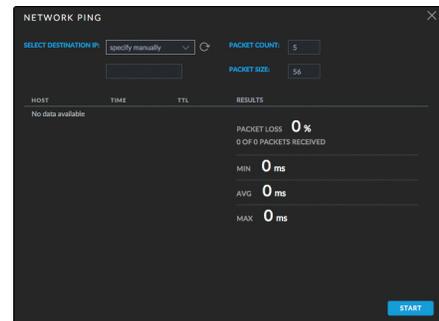
Select Destination IP You have two options:

- Select a remote system IP from the drop-down list, which is generated automatically.
- Select **specify manually** and enter the IP address in the field displayed below.

Click the ↻ icon to refresh the list of remote system IP addresses.

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

Packet Size Enter the size of the packet.

Start Click **Start** to start the test.

After the test is completed, the *Ping* tool reports the following information for each packet sent:

Host Displays the IP address of the remote host.

Time Displays the round-trip time in ms.

TTL Displays the Time To Live (TTL), the number of hops allowed before the ping test fails.

Results The *Ping* tool reports packet loss statistics and round-trip time evaluation:

- **Packet Loss** Displays the percentage of packets lost and number of packets received.
- **Min** Displays the minimum round-trip time in ms.
- **Avg** Displays the average round-trip time in ms.
- **Max** Displays the maximum round-trip time in ms.

Traceroute

The *Traceroute* tool traces the hops from the device to a specified destination host name or IP address. Use this tool to find the route taken by ICMP packets across the network to the destination host.
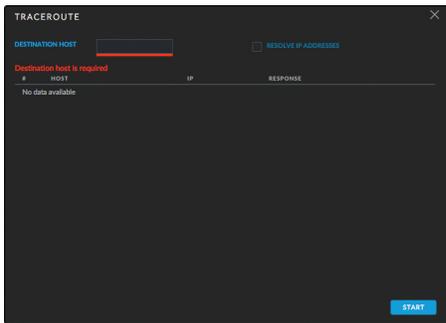
Destination Host Enter the host name or IP address of the destination host.

Resolve IP Addresses Select this option to resolve and print hop IP addresses symbolically rather than numerically.

Start Click **Start** to start the test.

After the test is completed, the *Traceroute* tool reports the following information for each hop:

Displays the hop number.

Host Displays the hostname, identifier, or IP address of the hop host.

IP Displays the IP address of the hop host.

Response Displays the round-trip times from the device to the hop host. There are three packets sent per hop, so there should be three round-trip times displayed. If there is no response from the hop host within the timeout interval of 5 seconds, "*" is displayed.

Speed Test

This utility allows you to test the connection speed between two airOS 8 devices. You can use the *Speed Test* tool to estimate a preliminary throughput between two network devices.

Note: If traffic shaping is enabled on either device, then the *Speed Test* results will be limited accordingly.
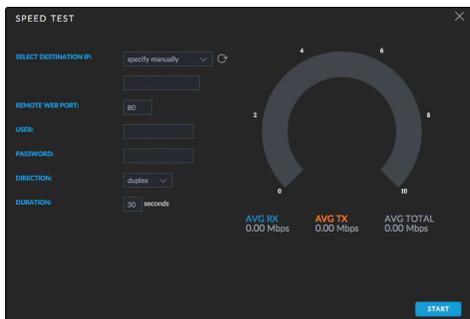
Select Destination IP You have two options:

- Select a remote system IP from the drop-down list, which is generated automatically.
- Select **specify manually** and enter the IP address in the field displayed below.

Click the ↻ icon to refresh the list of remote system IP addresses.

Remote Web Port Enter the remote web port of the airOS device to establish a TCP/IP-based throughput test (for example, specify port 443 if HTTPS is enabled on the remote device). The default is *80*.

User Enter the administrator username.

Note: Enter the remote system access credentials required for communication between two airOS devices. Administrator username and password are required to establish the TCP/IP-based throughput test.

Password Enter the administrator password.

Direction Select one of three directions:

- **duplex** Estimates the incoming (RX) and outgoing (TX) throughput at the same time.
- **receive** Estimates the incoming (RX) throughput.
- **transmit** Estimates the outgoing (TX) throughput.

Duration Enter the number of seconds the test should last. The default is *30* seconds.

Start Click **Start** to start the test.

The results are displayed on a speedometer dial and in five result categories:

Avg RX Displays the estimated average of incoming throughput.

Avg TX Displays the estimated average of outgoing throughput.

Avg Total Displays the estimated average of aggregate throughput.

Max RX Displays the maximum of incoming throughput.

Max TX Displays the maximum of outgoing throughput.

Log

Click at the bottom left corner of the page to open the *System Log* window, which provides a record of events on the system.

Click **Refresh** to update the display with the most recent information. To clear the system log, click **Clear**, and then click **Yes** to verify.

Appendix A: Contact Information

Ubiquiti Networks Support

Ubiquiti Support Engineers are located around the world 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.

Ubiquiti Networks, Inc.
685 Third Avenue, 27th Floor
New York, New York 10017
www.ubnt.com

Online Resources

Support: **ubnt.link/airMAX-Support**

Community: **ubnt.link/airMAX-ac-Blog**

Downloads: **downloads.ubnt.com/airmax-ac**

01/12/17

www.ubnt.com