

MANUAL AirOS



AirOS by Ubiquiti Networks UBIQUITI NETWORKS PowerStation2

Base Station SSID:

Signal Strength: ■ ■ ■ ■ ■ ■ ■ -49 dBm

TX Rate:

Frequency:

Antenna:

Security:

Transmit CCQ:

Uptime:

LAN Cable:

LAN MAC:

WLAN MAC:

Extra info:

AP MAC:

RX Rate:

Channel:

WLAN THROUGHPUT

RX: 16.7Mbps
TX: 17.2Mbps

NETWORK SPEED TEST

Select destination IP:

or specify manually:

User:

Password:

TEST RESULTS

Rx: 29.98 Mbps
Tx: 32.41 Mbps

Received:	Transmitted:	Collision:	Fragment:
41819417	45150956	37156	0
		39416	0

NETWORK PING

Select destination IP:

or specify manually:

Host	Time
192.168.1.1	1.56 ms
192.168.1.1	1.64 ms

10 of 10 packets received, 0% loss

Min: 1.34 ms Avg: 1.55 ms

FIREWALL

Interface	IP Type	Not	Source IP/mask	Not	Src Po
1. WLAN	UDP	<input type="checkbox"/>	192.168.1.44	<input type="checkbox"/>	1812

Scanned channels: 1 2 3 4 5 6 7 8 9 10 11

MAC address	ESSID	Encryption	Signal, dBm	Frequency, GHz
00:15:6D:A6:03:82	UBNT_AP2	-	-27	2.412
00:15:6D:A3:07:AE	Aee7	WEP	-29	2.412
00:15:6D:A6:03:82	UBNT_AP	WEP	-71	2.412
00:16:01:AF:A3:9C	AP123	WEP	-77	2.437
00:0B:6B:3E:3C:21	X	-	-91	2.417

IP Address	MAC address	Interface
192.168.1.201	00:15:6D:A6:03:82	BRIDGE
192.168.1.101	00:A0:D1:6A:70:A6	BRIDGE

Contents

- [1 AirOS Introduction](#)
- [2 Configuration Guide](#)
 - [2.1 Navigation](#)
 - [2.2 Main Page](#)
 - [2.2.1 Status Reporting](#)
 - [2.2.2 Statistics Reporting](#)
 - [2.2.3 Extra info](#)
 - [2.2.4 Tools](#)
 - [2.2.5 Antenna Alignment](#)
 - [2.3 Link Setup Page](#)
 - [2.3.1 Basic Wireless Settings](#)
 - [2.3.2 Wireless Security](#)
 - [2.4 Network](#)
 - [2.4.1 Bridge Mode](#)
 - [2.4.2 Router Mode](#)
 - [2.5 Advanced](#)
 - [2.5.1 Advanced Wireless Setting](#)
 - [2.5.2 Acknowledgement Timeout](#)
 - [2.5.3 Antenna Settings](#)
 - [2.5.4 Antenna Alignment LED Thresholds](#)
 - [2.5.5 Wireless Traffic Shaping](#)
 - [2.5.6 QoS](#)
 - [2.6 Services](#)
 - [2.6.1 Ping WatchDog](#)
 - [2.6.2 SNMP Agent](#)
 - [2.6.3 NTP Client, Web Server, Telnet Server](#)
 - [2.7 System](#)
 - [2.7.1 Administrative Management](#)
 - [2.7.2 Router Protocol Host Name](#)
 - [2.7.3 Logo Customization](#)
 - [2.7.4 UI Language Selection](#)
 - [2.7.5 Firmware](#)
 - [2.7.6 Configuration Management](#)
 - [2.7.7 Device Maintenance](#)

AirOS Introduction

The design goal of AirOS was simplicity and power. Unlike previous and current market-leading wireless or router operating systems that are complex and require a training investment, Ubiquiti set out to make an advanced operating system capable of powerful wireless and routing features, but was built upon a simple, clean, intuitive user interface foundation.

Our goal is to make AirOS simple enough for the operator, customer, or new technician to easily understand, configure, and deploy. At the same time, it is rapidly evolving towards a path of new powerful networking and wireless features strongly derived from customer interaction and feedback. Our goal is to make AirOs both the most advanced operating system on the market and the most intuitive, easy to deploy.

Configuration Guide

This guide presents the detailed description of the AirOS operating system which is integrated into long-range embedded systems (LiteStation2, LiteStation5), CPE (NanoStation2, NanoStation5), and outdoor wireless platforms (PowerStation2, PowerStation5) manufactured by Ubiquiti Networks, Inc.

[AirOS Quick Setup Guide](#) describes the configuration steps for the subscriber station (wireless client - bridge) use case.

All the configuration settings accessible via web management interface are described in this document.

[IEEE 802.11b/g](#) mode is supported in

- NanoStation2
- LiteStation2
- PowerStation2

[IEEE 802.11a](#) mode is supported in

- NanoStation5
- LiteStation5
- PowerStation5

All the devices support the following operating modes:

- Station (Client)
- Station [WDS](#)
- [Access Point](#)
- [Access Point](#) WDS / Repeater

All the devices support the following network modes:

- [Transparent bridge](#)
- [Router](#)

The **Main** Page displays a summary of link status information, basic configuration settings of the device (operating mode, network settings), traffic statistics of all the interfaces.

Network administration and monitoring utilities such as antenna alignment, ping test, and speed test tools are accessible via *Main* page also.

Status Reporting

Base Station SSID: The Name of the [802.11](#) Service Set (established by the Host [Access Point](#)) the device is connected to:

While operating in Station mode, displays the [BSSID](#) of the [Access Point](#) where the device has associated.

While operating in in [Access Point](#) mode, displays the [BSSID](#) of the [wireless](#) device itself.

AP MAC: displays the [MAC address](#) of the [Access Point](#) where the device has associated while operating in Station mode. [MAC](#) (Media Access Control) is unique [HW](#) identifier on each [802.11](#) radio. It consists of two parts:

An Organizationally Unique Identifier ([OUI](#))
Network Interface Controller ([NIC](#)) sequence.

The manufacturer list of a given [MAC address](#) is provided here:
<http://standards.ieee.org/regauth/oui/index.shtml>

Signal Strength: displays the received [wireless](#) signal level (client-side) while operating in Station mode. The represented value coincides with the graphical bar. Use antenna alignment tool to adjust the device antenna to get better link with the wireless device. The antenna of the wireless client has to be adjusted to get the maximum signal strength. [Signal Strength](#) is measured in dBm (the Decibels referenced to 1 miliwatt). The conversion is defined as $\text{dBm} = 10 \log_{10}(P/1\text{mW})$. So, 0dBm would be 1mW and -72dBm would be .0000006mW. A signal strength of -85dBm or better is recommended for stable links.

Antenna Alignment: This is a utility which allows the user to optimize the antenna direction for maximum link signal. More information is provided in the *Tools* sub-section.

TX Rate and RX Rate: displays the current [802.11](#) data transmission (TX) and data reception (RX) rate while operating in *Station* mode. Data rates at 1,2,5.5,11Mbps ([802.11b](#)) and 6,9,12,18,24,36,48,54Mbps ([802.11](#)) are possible. Typically, the higher the signal, the higher the data rate, and consequently the higher the throughput. For maximum throughput (54Mbps), typically a -70dBm or better signal is required.

Frequency: This is the operating frequency of the [802.11](#) Service Set (hosted by AP) the client is connected to. Device uses this [frequency](#) to transmit and receive data. For [802.11a](#) operation, the range of available frequencies are 5.1-5.9Ghz and for [802.11b/g](#) operation, 2412-2472Mhz. However, the specific frequencies that can be used will vary depending on local country regulations. For more information, please visit the [compliance section](#) of Ubiquiti Wiki.

Channel: This is the [802.11](#) channel number that corresponds to the operating [frequency](#). Device uses the selected [channel](#) to transmit and receive data. More information is provided in the *Link Setup* section.

Antenna: This shows which antenna option the AirOS device is using currently. Most of Ubiquiti Devices have 4 antenna options: vertical, horizontal, and Adaptive Antenna Polarity (AAP) options. There is also often an external antenna option.

Security: This is the current security setting. More information is provided in the *Link Setup* section.

ACK Timeout: displays the current ACK Timeout value, which is set on the device manually or adjusted automatically. The [ACK Timeout](#) (Acknowledgement Timeout) specifies how long the AirOS device should wait for an acknowledgement from partner device confirming packet reception before concluding the packet must have been in error and requires resending. ACK Timeout is very important outdoor wireless performance parameter. More information is provided in the *Advanced* settings section.

Transmit CCQ: This is an index which assesses the connection quality of the link. It takes into account transmit errors, latency, and throughput while evaluating the ratio of successfully transmitted [packets](#) against the re-transmitted ones and taking into account current rate ratio against the highest specified rate. The level is based on a percentage value where 100% corresponds to a perfect link state.

QoS Status: displays the current QoS setting. Quality of Service (QoS) can be enabled to direct link speeds to better service particular customers and/or particular applications like [VoIP](#) and video which require greater consistency, stability, and lower latency performance.

Uptime: This is the running total of time the device has been running since last power up (hard-reboot) or software upgrade. The time is expressed in days, hours, minutes and seconds.

Date: indicates the current system date and time, expressed in the form "year-month-day hours:minutes:seconds". System date and time can be retrieved from the internet services using [NTP](#) (Network Time Protocol).

LAN cable: displays the current status of the [Ethernet](#) port connection. This can alert operator/user/technician that [LAN](#) cable is plugged into device and there is an active [Ethernet](#) connection.

Host Name: displays the customizable name (ID) of the device as it will appear in popular [Router](#) Operating Systems registration screens.

LAN MAC: displays the [MAC address](#) of the AirOS device [LAN](#) ([Ethernet](#)) interface.

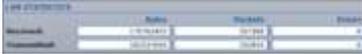
LAN IP Address: displays the current [IP address](#) of the [LAN](#) ([Ethernet](#)) interface.

WLAN MAC: displays the [MAC address](#) of the AirOS device [WLAN](#) (Wireless) interface.

WLAN IP Address: displays the current [IP address](#) of the [WLAN](#) (Wireless) interface.

Note: *LAN IP Address* and *WLAN IP Address* displays the same value - current [IP address](#) of the virtual *bridge* interface, while the device is operating in *Bridge* mode.

Statistics Reporting



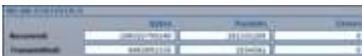
	Bytes	Packets	Errors
Received	100000000	1000000	0
Transmitted	100000000	1000000	0

LAN interface Statistics

LAN Statistics: section displays the detailed receive and transmit statistics ([Bytes](#), [Packets](#), [Errors](#)) of [LAN](#) (Ethernet) interface. This statistics represents the total amount of data and packets transferred between devices through the ethernet interface either way.

Both unicast IP traffic (conversations between two hosts using [HTTP](#), [SMTP](#), [SSH](#) and other protocols) and [broadcast traffic](#) (while addressing all hosts in a given network range with a single destination [IP address](#)) is accounted.

As long as there is some network traffic being generated or passed through the [LAN](#) interface, Received and Transmitted [Bytes](#) and [Packets](#) value will go on increasing. [Errors](#) value represents the total number of transmitted and received packets for which an error occurred.



	Bytes	Packets	Errors
Received	100000000	1000000	0
Transmitted	100000000	1000000	0

WLAN interface Statistics

WLAN Statistics: section displays the detailed receive and transmit statistics ([Bytes](#), [Packets](#), [Errors](#)) of the [wirelessinterface](#).

This statistics represents the total amount of unicast and broadcast IP data transferred between devices through the [wirelessinterface](#) either way.

As long as there is some network traffic being generated or passed through the '[wirelessinterface](#)', Received and Transmitted [Bytes](#), [Packets](#) and Errors (if any) value will go on increasing.



	Bytes	Packets	Errors
Received	100000000	1000000	0
Transmitted	100000000	1000000	0

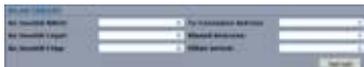
PPP interface Statistics

PPP Statistics: section displays the [IP address](#) of the [PPP](#) interface and the detailed receive and transmit statistics ([Bytes](#), [Packets](#), [Errors](#)) of the [PPP](#) interface. [PPP](#) statistics are available in *Router* mode only, while [PPPoE](#) is enabled.

This statistics represents the total amount of unicast and broadcast IP data transferred between AirOS powered device and [PPPoE](#) server through the [PPP](#) tunnel either way.

As long as there is some network traffic being passed through the [PPP](#) tunnel, Received and Transmitted Bytes, Packets and Errors (if any) value will go on increasing.

Refer to the *Network* section for more information about [PPPoE](#) setup.



WLAN Errors Statistics

WLAN Errors: section displays the counters of [802.11](#) specific errors which were registered on *wireless* interface:

Rx invalid NWID value represents the number of packets received with a different NWID or [ESSID](#) - packets which were destined for another access point. It can help to detect configuration problems or identify the adjacent wireless network existence on the same frequency.

Rx Invalid Crypt value represents the number of transmitted and received packets which were encrypted with the wrong encryption key and filed the decryption routines. It can be used to detect invalid *wireless security* settings.

Rx Invalid Frag value represents the number of packets missed during transmission and reception. These packets were dropped due to re-assembling failure as some link layer fragments of the packet were lost

Tx Excessive Retries value represents the number of packets which failed to be delivered to the destination. Undelivered packet are retransmitted a number of times before an error occurs.

Missed beacons value represents the number beacons (management packets sent at regular intervals by the Access Point) which were missed by the client. This indicates that the client is out of range.

Other errors value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

The content of the *Main* page can be updated by using the **Refresh** button.

Extra info

Extra Info: displays the current device usage statistics and status of the system components in pop-up window:



Status of the Associated Stations

- **Show Stations:** selection lists the stations which are connected to the device while operating in Access Point mode.

Statistics for all the stations (**RSSI**, **Tx Rate**, **Rx Rate** and **Idle** time) can be updated using the **Reload** button.

More statistics (**Station Uptime**, **Negotiated Rates**, **Static WDS Flag**, **Tx/Rx Frames**, **Tx/Rx Bytes**) can be retrieved while clicking on the “+” button near MAC address of the each Station entry.

IP Address	MAC address	Interface
192.168.1.101	00:0C:29:4E:11:85	BRIDGE
192.168.1.102	00:0C:29:4E:11:85	BRIDGE

Current Status of the system ARP table

- **Show ARP Table:** selection lists all the entries of the ARP (Address Resolution Protocol) table currently recorded on the device.

The list can be updated using the **Reload** button.

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

Destination	Gateway	Network	Interface
192.168.1.0	0.0.0.0	192.168.1.0	WLAN
192.168.1.0	0.0.0.0	192.168.1.0	LAN
192.168.0.0	0.0.0.0	192.168.0.0	LAN
192.168.0.0	0.0.0.0	192.168.0.0	WLAN

Current Status of the system routing tables

- **Show Routes:** selection lists all the entries in the system routing table, while the device is operating in Router mode.

The list can be updated using the **Reload** button.

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 – entries, which are registered in system routing table. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of all the AirOS interfaces.

AirOS IP configuration description is provided in the *Link Setup* section.

MAC address	Interface	Ageing timer
00:90:41:38:41:87	LAN	0:00
00:90:42:37:64:8E	LAN	0:00
00:12:78:21:79:34	LAN	0:00
00:12:77:78:0A:09	LAN	0:00
00:18:88:28:01:07	LAN	04:48
00:18:8D:89:09:08	LAN	16:04
00:18:8D:89:07:8E	LAN	0:00
00:18:8D:88:18:51	LAN	0:00
00:18:8D:84:64:8A	WLAN	0:34
00:18:8D:82:07:03	LAN	0:00
00:18:8D:84:08:92	LAN	07:21
00:18:8D:89:07:74	LAN	0:00
00:18:8D:88:08:63	LAN	0:00
00:18:8D:88:18:89	LAN	0:00
00:18:8D:7D:01:18	LAN	0:00
00:18:8D:7D:07:05	LAN	1:19
00:18:8D:85:54:5A	LAN	0:00
00:14:24:07:49:10	LAN	04:48
00:17:81:0A:82:89	LAN	07:40
00:14:8B:3D:0F:39	LAN	03:00
00:12:43:38:87:8A	LAN	00:04
00:50:00:0A:75:6A	LAN	0:00

Current Status of the system bridge table

- **Show Bridge Table:** selection lists all the entries in the system bridge table, while the device is operating in *Bridge* mode.

The list can be updated using the **Reload** button. Bridge table shows to which *bridge* port the particular station is associated to - in other words from which *interface* (ethernet or wireless) the network device (defined by *MAC address*) is reachable to AirOS system while forwarding the packets to that port only (thus saving a lot of redundant copies and transmits). *Ageing timer* shows ageing time for each address entry (in seconds) - after particular time out, not having seen a packet coming from a certain address, the bridge will delete that address from the Bridge Table.



Status of the throughput on LAN interface

- **Show Throughput** selection continuously represents the current data traffic on the LAN, WLAN and PPP interfaces in both graphical and numerical form.

The statistics is updated automatically and can be updated using the **Reload** button.

Mac Address	IP Address	Retaining Lease	Interface
00:12:00:74:74:03	192.168.1.101	00:00:00	LAN

Current Status of the DHCP leases

- **Show DHCP Leases** selection shows the current status of the leased IP addresses by the device's DHCP server.

Interface name shows from which device interface DHCP client which has specified *MAC Address* is connected.

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

The list can be updated using the **Reload** button.



Active Firewall entries in Bridge mode

- **Show Firewall** selection lists active firewall entries in the *FIREWALL chain* of the standard [ebtables](#) *filter table*, while the device is operating in *Bridge* mode.

The list can be updated using the **Reload** button.



Active Firewall entries in Router mode

Active firewall entries in the *FIREWALL chain* of the standard [iptables](#) *filter table* are listed if the device is operating in *Router* mode.

The list can be updated using the **Reload** button.

IP and MAC level access control and packet filtering in AirOS is implemented using [iptables](#) (routing) and [ebtables](#) (bridging) firewall which protects the resources of a private network from outside threats by preventing unauthorized access and filtering specified types of network communication.

More information is provided in the *Link Setup* section.



Active Port Forward entries in Router mode

- **Show Port Forward** selection lists active port forward entries in the *PORTFORWARD chain* of the standard [iptables](#) *nat table*, while the device is operating in *Router* mode.

The list can be updated using the **Reload** button.

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

More information is provided in the *Link Setup* section.

Tools

Tools: provides network utilities in pop-up window:



Wireless link throughput estimation with Network Speed Test utility

- **Speed Test:** This utility allows for testing the connection speed to and from any reachable IP address on the AirOS device network. It should be used for the preliminary throughput estimation between two network devices. If both devices are powered by AirOS, the estimation is more precise, otherwise only rough estimation is provided while using ICMP packet exchange routines.

Access credentials (administrator username - **User** and **Password**) of the remote system should be provided for the communication between two AirOS powered devices.

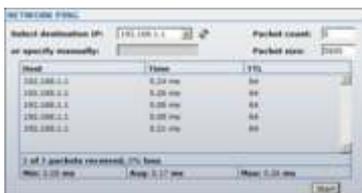
Remote system IP can be selected from the list which is generated automatically (*Select destination IP*) or can be *specified manually*.

There are 4 options available for the traffic *direction* while estimating the throughput:

- * Estimate the incoming maximal throughput (Rx) while selecting receive option;
- * Estimate the outgoing maximal throughput (Tx) while selecting transmit option;
- * First estimate the incoming (Rx) and afterwards the outgoing (Tx) maximal throughput while selecting both option;
- * Estimate the incoming (Rx) and the outgoing (Tx) maximal throughput at the same time while selecting duplex option.

Test *Duration* and *Data amount* values can be specified while defining the test execution time criteria. If both criteria are specified, the test will stop after any of the criteria is met.

The test is started using the **Run Test** button.



Wireless link quality estimation with Network Ping utility

- **Ping:** This utility will ping other devices on the network directly from the AirOS device.

Ping utility should be used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets. Remote system IP can be selected from the list which is generated automatically (*Select destination IP*) or can be *specified manually*. The size of the ICMP packets can be specified in the *Packet size* field. Estimation is done after the number of ICMP packets (specified in *Packet count* field) is transmitted/received. Packet loss statistics and latency time evaluation is provided after the test is completed. The test is started using the **Start** button.



Finding the route across the network with Traceroute utility

- **TraceRoute:** Allows tracing the hops from the AirOS device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the *Destination host*.

Resolution of the IP addresses (symbolically rather than numerically) can be enabled by selecting the **Resolve IP address** option. The test is started using the *Start* button.



Wireless Site Survey utility

- **Site Survey:** utility will search for wireless networks in range on all the supported channels while device is operating as *Access Point* or *Station*. In Station mode channel list can be modified. Refer to the section Link Setup for the details on channel list customization.

Site Survey will report *MAC Address*, *SSID*, *Encryption* type (if any), *Signal Strength*, *Frequency* and wireless *channel* used for each Access Point which is found.

The Site Survey can be updated using the **Scan** button.

Antenna Alignment



Antenna alignment Tool

Antenna Alignment utility allows the installer to point and optimize the antenna in the direction of maximum link signal. The "RSSI Range" slider bar allows the range of the meter to be either increased or reduced. If the range is reduced, the color change will be more sensitive to signal fluctuations.

Click the **Align Antenna** button and the new pop-up window with signal strength indicator will appear.

RSSI Range slider can be used to change an offset of the maximum indicator value. Window reloads every second displaying current value of the signal strength.

The content of the *Main* page can be updated by using the **Refresh** button.

Link Setup Page

The Link Setup Page contains everything needed by the operator to setup the wireless part of the link. This includes regulatory requirements, channel and frequency settings, device mode, data rates, and wireless security.

Basic Wireless Settings



Station Basic Wireless Settings

The general wireless settings, such as wireless device BSSID, country code, output power, 802.11 mode and data rates can be configured in this section.

Wireless Mode: specify the operating mode of the device. The mode depends on the network topology requirements. There are 4 operating modes supported in AirOS v3.0 software:

1. *Station*: This is a client mode, which can connect to an AP. It is common for a bridging application to an AP. In *Station* mode device acts as the Subscriber Station while connecting to the Access Point which is primary defined by the SSID and forwarding all the traffic to/from the network devices connected to the ethernet interface. The specifics of this mode is that Subscriber Station is using *arpnat* technique which may result lack of transparency while passing-through *broadcast* packets in *bridge* mode.

2. *Station WDS*: WDS stands for Wireless Distribution System. Station WDS should be used while connecting to the Access Point which is operating in WDS mode.

Station WDS mode enables packet forwarding at layer 2 level.

The benefit of *Station WDS* is improved performance and faster throughput.

Station WDS - Bridge mode is fully transparent for all the Layer2 protocols.

Refer to the section Network Settings for detailed Bridge network mode configuration information.

3. *Access Point*: This is an 802.11 Access Point mode.



AP WDS Basic Wireless Settings

4. *Access Point WDS*: This is an 802.11 Access Point which allows for layer 2 bridging with Station WDS devices using the WDS protocol.

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

It is very important that network loops should not be created with either WDS bridges or combinations of wired (Ethernet) connections and WDS bridges. Tree or Star shape network topology should be used in all WDS use-cases (i.e. if AP2 and AP3 are specified as the WDS peers of AP1, AP2 should not be specified as the WDS peer of AP3 and AP3 should not be specified as the WDS peer of AP2 in any case). Mesh and Ring network topologies are not supported by WDS and should be avoided in all the use cases.

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

MAC Clone option makes the Station fully transparent while acting as the laptop or PC which is connected to the AirOS device LAN port (Ethernet interface). MAC of the client computer is cloned and copied on top of the AirOS device, so it can be made to connect to the same device and maintain any MAC ID security based privileges from the server.

MAC Cloning option is effective for one and the only PC connected to the subscriber station's LAN port as the station will authenticate and associate to the chosen Access Point using the MAC address of the PC.

WDS Peers: WDS Stations and/or WDS Access Points connected to the AirOS powered Access Point should be specified in this list in order to create a wireless network infrastructure - Wireless Distribution System (applicable for AP WDS mode only).

Enter the MAC address of the paired WDS device in the WDS Peer entry field. One MAC address should be specified for Point-to-Point connection use case, up to six WDS Peers can be specified for Point-to-Multi-Point connection use case.

Auto option should be enabled in order to establish WDS connection between Access Points if *WDS Peers* are not specified (applicable for AP WDS mode only). If *Auto* option is enabled AirOS powered Access Point will choose WDS Peers according to the SSID setting.

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

SSID: Service Set Identifier used to identify your 802.11 wireless LAN should be specified while operating in *Access Point* mode. All the client devices within range will receive broadcast messages from the access point advertising this SSID. **ESSID:** – specify the ESSID of the Access Point which the the AirOS should associate to while operating in *Station* or *Station WDS* mode. There can be several Access Points with the same ESSID. If the ESSID is set to "Any" the *station* will connect to any available AP.



Site Survey tool for the Access Point selection

The list of the available Access Points can be retrieved using the *Select* button, which activates *Site Survey* tool with the AP selection functionality. Site Survey will search for the available wireless networks in range on all the supported channels and will allow you to select one for association. In case the selected network uses encryption, you'll need to set security parameters in wireless security section. Select the Access Point from the list and click **Select** button for association.

Click **Scan** button to refresh the list of available wireless networks.

Close this window button closes Site Survey tool window.

Site Survey channel scan list can be modified using the *Channel Scan List* control.



Channel Scan list selection on Nanostation5

Channel Scan List: This will confine scanning only to frequencies selected (applicable for Station and Station WDS modes only). The benefits of this are faster scanning as well as filtering out unwanted AP's in the results. Site Survey tool will look for the Access Points in selected channels only.

Channel list management for the selected IEEE 802.11 mode and specified Channel Spectrum Width can be enabled by selecting the **Enabled** option. There are two ways to set the Channel Scan List - enumerating the required channels (separated by comma) in the input field or using the selection window which is activated using the **Edit** button.

Hide SSID control will disable advertising the SSID of the access point in broadcast messages to wireless stations. Unselected control will make SSID visible during

network scans on the wireless stations. Control is available while operating in *Access Point* mode only.

Lock to AP MAC: This allows the station to always maintain connection to a specific AP with a specific MAC (applicable for Station and Station WDS modes only). This is useful as sometimes there can be few identically named SSID's (AP's) with different MAC addresses. With AP lock on, the station will lock to MAC address and not roam between several Access Points with the same ESSID.

Country Code: Different countries will have different power levels and possible frequency selections. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where device will be used. The channel list, output power limits, IEEE 802.11 and Channel Spectrum Width modes will be tuned according to the regulations of the selected country. Additionally, please consult [compliance guide](#) for further explanation of international compliance requirements.

IEEE 802.11 Mode: This is the radio standard used for operation of your AirOS powered device. 802.11b is an older 2.4GHz mode while the 802.11g (2.4GHz) and 802.11a (5GHz) are newer standards based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. For more information, please consult [802.11 compliance guide](#).

- PowerStation2/LiteStation2/Nano Station2 supported IEEE 802.11 modes:

B only – connect to a 802.11b only network.

B/G Mixed – connect to a 802.11b or 802.11g network (selected by default).

G only – connect to a 802.11g only network.

- PowerStation5/LiteStation5/Nano Station5 supported IEEE 802.11 modes:

A – connect to a 802.11a network (selected by default).

Channel Spectrum Width: This is spectral width of the radio channel. Supported wireless channel spectrum widths:

5MHz – is the channel spectrum with the width of 5 MHz (known as Quarter-Rate mode).

10MHz – is the channel spectrum with the width of 10 MHz (known as Half-Rate mode).

20MHz – is the standard channel spectrum width (selected by default).

40MHz – the widest channel spectrum width required to connect to a 802.11a network which supports Static Turbo feature (applicable for PowerStation5/LiteStation5/Nano Station5 only).

Reducing spectral width provides 2 benefits and 1 drawback.

Benefit 1: It will increase the amount of non-overlapping channels. This can allow networks to scale better

Benefit 2: It will increase the PSD (power spectral Density) of the channel and enable the link distance to be increased

Drawback: It will reduce throughput proportional to the channel size reduction. So just as turbo mode (40MHz) increases possible speeds by 2x, half spectrum channel (10MHz), will decrease possible speeds by 2x.

Channel Shifting: option enables the special channels which have the frequency offset from the standard 802.11b/g and 802.11a channels. This is a proprietary Ubiquiti developed feature. While 802.11 networks have standard channels such as Channel 1 (2412MHz), Channel 2 (2417MHz), etc. spaced every 5MHz apart; channel shifting will allow operation of new non-802.11 channels offset from the standard channels. The benefits of this are private networking and inherent security. Using channel-shifting, networks can instantly become invisible to the millions of wifi devices in the world.

Channel: select the wireless channel while operating in *Access Point* mode. Multiple frequency channels are available to avoid interference between nearby access points. The channel list varies depending on the selected country code, IEEE 802.11 mode, Channel Spectrum Width and Channel Shifting option.

Output Power: This will configure the maximum average transmit output power (in dBm) of the wireless device. The output power at which wireless module transmits data can be specified using the slider. When entering output power value manually, the slider position will change according to the entered value. The transmit power level that is actually used is limited to the maximum value allowed by your country's regulatory agency. Note: In case of NanoStation, this is the output power delivered to the internal Antennas.

Obey regulatory power box must be always checked. While checked transmit output power will be tuned according to the regulations of the selected country.

Data Rate: This defines the data rate (in Mbps) at which the device should transmit wireless packets. If the **Auto** check box is enabled, then the *rate algorithm* will select the best data rate depending on the link quality conditions. If a data rate below 54Mbps is selected while the *Auto* rate selection is enabled, then the selected data rate will become the maximum data rate that can be used. Use *Auto* option if you are having trouble getting connected or losing data at a higher rate. In this case the lower data rates will be used by device automatically.

Refer to the section *Advanced Wireless Settings* for the detailed information about *rate algorithms*.

Wireless Security

This section enables you to set parameters that control how the subscriber station associates to a wireless device and encrypts/decrypts data.



Station Wireless Security Settings

Choose the security method according to the Access Point security policy. Subscriber station should be authorized by Access Point in order to get access to the network and all the user data transferred between subscriber station and Access Point will be encrypted if the wireless security methods are used.

Security: AirOS supports all the popular 802.11 security options such as WEP, WPA, and WPA2. Select the security mode of your wireless network:

WEP – enable WEP encryption. WEP (Wired Equivalent Privacy) is based on the IEEE 802.11 standard and uses the RC4 encryption algorithm. Enabling WEP allows you to increase security by encrypting data being transferred over your wireless network. WEP is the oldest security algorithm.

WPA – enable WPA™ security mode. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

WPA™ and *WPA2™* support the following ciphers for data encryption:

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.

CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm.

The device will use the strongest cipher (CCMP) in Station and Access Point wireless mode by default. If CCMP is not supported on the other side of the link the TKIP encryption will be used - like in situation when the device acts as Access Point with WPA security enabled and at least one wireless station (without CCMP support) is connected to it.

WPA-TKIP – enable WPA™ security mode with TKIP support only.

WPA-AES – enable WPA™ security mode with AES support only.

WPA2 – enable WPA2™ security mode.

WPA2-TKIP – enable WPA2™ security mode with TKIP support only.

WPA2-AES – enable WPA2™ security mode with AES support only.

Authentication Type: field relates only to the WEP security option. One of the following authentication modes should be selected if WEP security method is used:

Open Authentication – station is authenticated automatically by AP (selected by default).

Shared Authentication – station is authenticated after the challenge, generated by AP.

WEP Key Length: 64-bit (selected by default) or 128-bit WEP Key length should be selected if WEP security method is used. The *128-bit* option will provide more security.

Key Type: *HEX* (selected by default) or *ASCII* option specifies the character format for the WEP key if WEP security method is used.

WEP Key: WEP encryption key for the wireless traffic encryption and decryption should be specified if WEP security method is used:

For *64-bit* – specify WEP key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.

For *128-bit* – specify WEP key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Key Index: specify the Index of the WEP Key used.

WPA Authentication: one of the following WPA™ key selection methods should be specified if WPA™ or WPA2™ security method is used (applicable for *Station* and *Station WDS* modes only). :

PSK – WPA™ or WPA2™ with Pre-shared Key method (selected by default).

EAP – WPA™ or WPA2™ with EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in Enterprise networks.

WPA Pre-shared Key: the pass phrase for WPA™ or WPA2™ security method should be specified if the *Pre-shared Key* method is selected. The pre-shared key is an alphanumeric password between 8 and 63 characters long.



Access Point Wireless Security Settings

MAC ACL: MAC Access Control List (ACL) provides ability to allow or deny certain clients to connect to the AP (applicable for AP and AP WDS modes only).

MAC ACL can be enabled by selecting the **Enabled** option.

There are two ways to set the Access Control List:

define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients - MAC ACL **Policy** is set to *Deny*.

define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - MAC ACL **Policy** is set to *Allow*.

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

Note: MAC Access Control is the weakest security approach. WPA™ or WPA2™ security methods should be used when possible.

Click **Change** button to save the changes.

Network

The Network Page allows the administrator to setup bridge or routing functionality.

AirOS powered devices can operate in bridge or router mode. The IP configuration as described below is required for device management purposes. IP addresses can either be retrieved from a DHCP server or configured manually. Use the *Network* menu to configure the IP settings.



AirOS Network Mode selection

Network Mode: specify the operating network mode for the device.

The mode depends on the network topology requirements:

Bridge operating mode is selected by default as it is widely used by the subscriber stations, while connecting to Access Point or using WDS. In this mode the device will act as a transparent bridge and will operate in Layer 2. There will be no network segmentation while broadcast domain will be the same. Bridge mode will not block any broadcast or multicast traffic. Additional *Firewall* settings can be configured for Layer 2 packet filtering and access control in *Bridge* mode.

Router operating mode can be configured in order to operate in Layer 3 to perform routing and enable network segmentation – wireless clients will be on different IP subnet. **Router** mode will block broadcasts while it is not transparent.

AirOS supports Multicast packet pass-through in **Router** mode.

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

Bridge Mode



Bridge mode Network Settings

In bridge mode, the AirOS will simply forwards the network management and data packets to the client PC without any intelligent routing. For some applications, this can provide a more efficient and simple network solution. WLAN (wireless) and LAN (Ethernet) interfaces belong to the same network segment which has the same IP

address space. WLAN and LAN interfaces form the virtual *bridge* interface while acting as the *bridge* ports. The *bridge* has assigned IP settings for management purposes:

Bridge IP Address: The device can be set for static IP or can be set to obtain an IP address from the DHCP server it is connected to.

One of the IP assignment modes must be selected:

DHCP – choose this option to assign the dynamic IP address, Gateway and DNS address by the local DHCP server.

Static – choose this option to assign the static IP settings for the *bridge* interface.

IP Address: enter the IP address of the device while *Static Bridge IP Address* mode is selected. This IP will be used for the AirOS device management purposes.

IP Address and *Netmask* settings should consist with the address space of the network segment where AirOS device resides. If the device IP settings and administrator PC (which is connected to the device in wired or wireless way) IP settings will use different address space, the AirOS device will become unreachable.

Netmask: This is a value which when expanded into binary provides a mapping to define which portions of IP address groups can be classified as host devices and network devices. Netmask defines the address space of the network segment where AirOS device resides. 255.255.255.0 (or /24) *Netmask* is commonly used among many C Class IP networks.

Gateway IP: Typically, this is the IP address of the host router which provides the point of connection to the internet. This can be a DSL modem, Cable modem, or a WISP gateway router. AirOS device will direct the packets of data to the gateway if the destination host is not within the local network.

Gateway IP address should be from the same address space (on the same network segment) as the AirOS device.

Primary/Secondary DNS IP: The Domain Name System (DNS) is an internet "phone book" which translates domain names to IP addresses. These fields identify the server IP addresses of where the AirOS device looks for the translation source.

Primary DNS server IP address should be specified for the device management purposes.

Secondary DNS server IP address is optional. It is used as the fail-over in case the primary DNS server will become unresponsive.

DHCP Fallback IP: In case the *Bridge* is placed in Dynamic IP Address mode (DHCP) and is unable to obtain an IP address from a valid DHCP server, it will fall back to the static IP address listed here.

In case the IP settings of the AirOS powered device are unknown, they can be retrieved with the help of the [UBNT_Discovery_Utility Ubiquiti Discovery Utility]. Multi-

platform *Utility* should be started on the administrator PC which resides on the same network segment as the AirOS device.

AirOS system will return to the default IP configuration (192.168.1.20/255.255.255.0) If the *Reset to defaults* routine is initiated.

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

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

Click **Change** button to save the changes.

Router Mode

The screenshot shows the 'Router Mode' configuration page for 'Network Settings'. It is divided into three sections: 'WLAN NETWORK SETTINGS', 'LAN NETWORK SETTINGS', and 'WLAN TO WIRELESS SETTINGS'. The 'WLAN NETWORK SETTINGS' section includes fields for IP Address (192.168.1.1), Netmask (255.255.255.0), Enable NAT (checked), Enable DHCP Server (checked), Range Start (192.168.100.0), Range End (192.168.199.254), Netmask (255.255.255.0), Lease Time (1440 minutes), and Port Forwarding (disabled). The 'LAN NETWORK SETTINGS' section includes a tab for 'DHCP' and fields for LAN IP Address (192.168.1.20), IP Address (192.168.1.20), Netmask (255.255.255.0), Gateway IP (192.168.1.1), Primary DNS IP (8.8.8.8), Secondary DNS IP (8.8.4.4), Default Username, Default Password, Default IP/MAC, Default Port/Port, Enable DNS, DNS (Recursive) Path, DNS IP, and DNS fallback IP. The 'WLAN TO WIRELESS SETTINGS' section includes a checkbox for 'Enable Port Binding'.

AP-Router mode Network Settings

IP Address: This is the IP address to be represented by the wireless interface.

Netmask: This is used to define the host and device classification for the chosen IP address range. 255.255.255.0 is a typical value.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the outside world to the wireless interface IP address and then sub-routed to other client devices residing on it's local network.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients who will associate to the wireless interface.

Range Start/End: This range will determine the IP addresses given out by the DHCP server to associated client devices.

Lease Time: The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interrupt, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more slight interruptions to client while the acquire new IP addresses from the server.

Port Forwarding: Port forwarding allows specific ports of the WLAN IP address to be forwarded to different IP addresses on the same network. This is useful for applications such as FTP servers, gaming, etc. where different host systems want to be seen using a single common IP address.

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

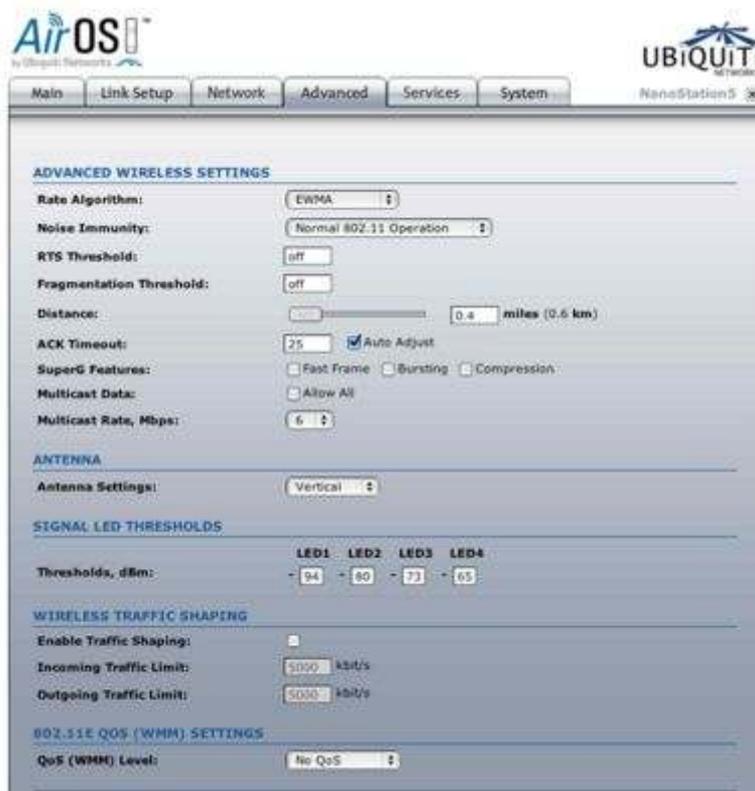
Enable DMZ: The Demilitarized zone (DMZ) can be used as a place where services can be placed such as Web Servers, Proxy Servers, and E-mail Servers such that these services can still serve the local network and are at the same time isolated from it for additional security.

MULTICAST ROUTING SETTINGS

With a multicast design, applications can send one copy of each packet and address it to the group of computers that want to receive it. This technique addresses packets to a group of receivers rather than to a single receiver, and it depends on the network to forward the packets to only the networks that need to receive them

Advanced

This page handles advanced routing and wireless settings. The Advanced options page allows you to manage advanced settings that influence on the device performance and behavior. The advanced wireless settings are dedicated for more technically advanced users who have a sufficient knowledge about wireless LAN technology. These settings should not be changed unless you know what effect the changes will have on your device.



Advanced Wireless Setting

Rate Algorithm: defines data rate algorithm convergence.

- Optimistic Algorithm is aggressive enough to move to a higher rate but yet tries to conservatively capture the fluctuations of the RSSI. It starts with the highest possible rate and then decreases till the rate can be supported while periodically transmitting packets at higher rates and computing the transmission time.
- Conservative Algorithm is less sensitive to individual packet failure as it is based on a function of number of successful and erroneous transmission/retransmission over a sampling period. It steps down to a lower rate after continuous packet failure and steps up after number of successful packets.
- EWMA Algorithm is trying to move to a higher rate but is continuously monitoring the packet failure counters.

The 802.11 data rates include 1,2,5.5,11Mbps (802.11b) and 6,9,12,18,24,36,48,54Mbps (802.11a/g). The Rate Algorithm has a critical impact on performance in outdoor links as generally lower data rates are less immune to noise while higher rates are more immune, but are capable of higher throughput. The

conservative rate algorithm provides the best case stability / robustness, but may compromise maximum throughput. The optimistic rate algorithm always looks to achieve highest throughput while sacrificing noise immunity and robustness. The EWMA algorithm is a hybrid of the two.

Noise Immunity: options define the robustness of the device to operate in the presence of noise disturbance:

For Channel Hopping Signals configuration provides robustness against Channel Hopping Signals.

For 802.11 Traffic Immunity provides robustness against external 802.11 traffic sources that are from a foreign network.

Normal 802.11 Operation (default option) provides balanced immunity between both types of interferers (Channel Hopping Signals and external 802.11 traffic).

RTS Threshold: determines the packet size of a transmission and, through the use of an access point, helps control traffic flow. The range is 0-2347bytes, or word "off". The default value is 2347 which means that RTS is disabled.

RTS/CTS (Request to Send / Clear to Send) is the mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden terminal problem. RTS/CTS packet size threshold is 0-2347 octets. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately

Fragmentation Threshold: specifies the maximum size for a packet before data is fragmented into multiple packets. The range is 256-2346 bytes, or word "off". Setting the Fragmentation Threshold too low may result in poor network performance. Only minor modifications of this value are recommended while default setting of 2346 should remain in most of the cases.

The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. The fragment size value can typically be set between 256 and 2,048 bytes.

Multicast Rate: This option allows Multicast packets to be sent in higher than usual rates.

Client Isolation: This option allows packets only to be sent from the router to the CPE. In other words, CPE's on the same network as the AP will not be able to see each other.

SuperG® /SuperAG® Features: select the checkboxes to enable the chosen SuperG® (PowerStation2 and LiteStation2) or SuperAG® (LiteStation5) features:

Fast Frame – utilizes frame aggregation and timing modifications.

Bursting – more data frames per given time period are transmitted.

Compression – real-time hardware data compression is enabled.

Acknowledgement Timeout

AirOS has an auto-acknowledgement timeout algorithm which dynamically optimizes the acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user also has the ability to enter the value manually, but this is not recommended.

Distance: specify the distance value in miles using slider or enter the value manually. The signal strength and throughput falls off with range. Changing the distance value will change the ACK Timeout to the appropriate value of the distance.

ACK Timeout: specify the ACK Timeout. This is the amount of time the subscriber station will wait to hear a acknowledgement response from the wireless device after the data packet is transmitted. If the timeout is set too short or too long, it will result poor connection and throughput performance.

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

Auto Adjust control will enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above.

Antenna Settings

AirOS based devices have a possibility to switch the antenna polarities with a single web management control. This is achieved by using Ubiquiti's patent-pending Adaptive Antenna Polarity (AAP) technology.

AirOS devices often have multiple antenna options. In the case of the NanoStation, there are 4 antenna modes:

1. Vertical Polarity
2. Horizontal Polairty
3. Adaptive: This mode chooses the best polarity dynamically. Adaptive – switches adaptive antenna polarity mode which allows for the beam polarities to be switched dynamically on the fly for improved performance in heavy noise environments.
4. External: This allows a connection to an external port / higher gain antenna

Antenna Alignment LED Thresholds

The LED's on the back of the AirOS Device can be made to light on when received signal levels reach the values defined in the following fields. This allows a technician to easily deploy an AirOS CPE without logging into the unit.

RSSI LED Thresholds specify the marginal value of RSSI which will switch on LEDs indicating signal strength:

LED 1 (Red) will switch on if the RSSI reach the value set in an entry field next to it.

LED 2 (Yellow) will switch on if the RSSI reach the value set in an entry field next to it.

LED 3 (Green) will switch on if the RSSI reach the value set in an entry field next to it.

LED 4 (Green) will switch on if the RSSI reach the value set in an entry field next to it.

Wireless Traffic Shaping

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

Traffic Shaping: The traffic can be limited at the AirOS based device in the upload and download direction based on a user defined rate limit. This is layer 3 QoS.

Enable Traffic Shaping: control will enable bandwidth control on the device.

Incoming Traffic Limit: specify the maximum bandwidth value in kbps for traffic passing from wireless interface to Ethernet interface.

Outgoing Traffic Limit: specify the maximum bandwidth value in kbps for traffic passing from Ethernet interface to wireless interface.

QoS

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). The QoS assigns priority to the selected network traffic, prevents packet collisions and delays thus improving VoIP calls and watching video over WLANs. **802.11e / WMM:** This allows for improved latency performance for Voice and Video applications. This is layer 2 QoS and happens at 802.11 frame level.

QoS (WMM) Level: choose the type of the network traffic to which the priority will be set or disable the QoS feature. No QoS – disable QoS.

Video Priority – enable priority of the video traffic.

Voice Priority – enable priority of the voice traffic.

Services

This page covers the configuration of system management services SNMP and Ping Watchdog.



Ping WatchDog

The ping watchdog sets the AirOS 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, the AirOS device will automatically reboot. This option creates a kind of "fail-proof" mechanism.

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

Enable Ping Watchdog: control will enable Ping Watchdog Tool.

IP Address To Ping: specify an IP address of the target host which will be monitored by Ping Watchdog Tool.

Ping Interval: specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool.

Startup Delay: specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted.

Failure Count To Reboot: specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device.

SNMP Agent

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

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

Enable SNMP Agent: control will enable SNMP Agent.

SNMP Community: specify SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management stations to all the objects in the MIB except the community strings, but does not allow write access.

Contact: specify the identity or the contact who should be contacted in case a emergency situation arise.

Location: specify the physical location of the device.

NTP Client, Web Server, Telnet Server

NTP Client: The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It can be used to set the AirOS internal clock.

Web Server: the following AirOS Device Web Server parameters can be set there:

Use Secure Connection (HTTPS): If checked Web server will use secure HTTPS mode. HTTP mode is selected by default.

Secure Server Port: Web Server TCP/IP port setting while using HTTPS mode.

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

Telnet Server: the following AirOs Device Telnet Server parameters can be set there:

Enable Telnet Server: Enables Telnet access to the AirOS Device.

Server Port: Telnet service TCP/IP port setting.

System

The System Page contains Administrative options. This page enables administrator to customize, reboot the device, set it to factory defaults, upload a new firmware, backup or update the configuration and configure administrator's credentials.



The screenshot shows the 'System' configuration page in the AirOS web interface. The page is titled 'AirOS' and 'UBIQUITI NETWORKS NanoStation S'. It features a navigation menu with tabs for 'Main', 'Link Setup', 'Network', 'Advanced', 'Services', and 'System'. The 'System' tab is selected. The page is divided into several sections:

- FIRMWARE:** Shows 'Firmware Version: X55.ar2313.v3.0.2927.080424.2058' with an 'Upgrade...' button.
- HOST NAME:** Shows 'Host Name: ubnt' with a 'Change' button.
- ADMINISTRATIVE ACCOUNT:** Shows 'Administrator Username: ubnt', 'Current Password', 'New Password', and 'Verify New Password' fields, with a 'Change' button.
- INTERFACE LANGUAGE:** Shows 'Language: English' with a 'Set as default' button.
- LOGO CUSTOMIZATION:** Shows 'Enable Custom Logo' (checked), 'Logo Target URL' (http://), and 'Logo File' (no file selected) with a 'Change' button.
- CONFIGURATION MANAGEMENT:** (Section header, partially visible)

Administrative Management

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

Administrator Username: displays name of the system user. The username is not configurable parameter, so it cannot be changed.

Current Password: enter a current password value. Default administrator login credentials:

User Name: ubnt

Password: ubnt

New Password: enter a new password value used for administrator authentication.

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

Click Change button to save the changes.

Router Protocol Host Name

Host Name is the system wide device identifier. It is reported by SNMP Agent to authorized management stations.

Host Name: specify the system identity. Click Change button to save the changes.

Logo Customization

Use this section to enable and upload your custom logo on the device user interface. The logo must conform to these limitations:

- The size limit of the logo is 50Kb.
- The maximum height of logo should be 70 pixels.
- Only .gif format images are accepted.

To upload new logo, enable logo customization and specify the location of logo file:



Enable Custom Logo: control will enable logo customization. Deselecting this option the custom logo will be removed and the default Ubiquiti logo will be restored. Logo Target URL: specify the target URL of custom logo. Target URL is opened when clicking on custom logo. Logo File: click Browse... button to navigate to and select the logo file or specify the full path and click the Upload button.

UI Language Selection

Use this section to change the language setting of the web management interface.

Firmware

Use this section to find out current software version and update the device with the new firmware. The device firmware update is compatible with all configuration settings. When the device is updated with a newer version or the same version firmware builds, system configuration will be preserved.

Firmware version: displays version of the current firmware. Upgrade...: click to load the device firmware upgrade window. After the Upgrade... button is clicked the new Firmware Upload pop-up window will be displayed:

Current Firmware: displays version of the current firmware. Firmware File: click the Browse... button to specify the new firmware image location or specify the full path

and click the Upload button. Close this window – cancel the upload process. After the new firmware image is uploaded into the system, use Upgrade button to upgrade a device:

[Image:System5.jpg](#)

Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as this can damage the device!

After clicking the Upgrade button the upgrade process starts immediately:

Close this window – close firmware upgrade window. This action will not cancel the firmware upgrade process.

Configuration Management

PowerStation2/LiteStation2/LiteStation5 configuration is stored in plain text file. Use the Configuration Management section controls to manage (backup, restore/update) system configuration file:

[Image:System7.jpg](#) Backup Configuration: click Download... button to download the current system configuration file. Upload Configuration: click Browse... button to navigate to and select the new configuration file or specify the full path and click the Upload button.

Use only configuration backups of the same type device - configuration backed up from PowerStation2 suits only PowerStation2, but not LiteStation2 or LiteStation5! Behavior may be unpredictable when mixing configurations from different type devices.

Device Maintenance

Use this section to reboot device or reset all the system parameters to factory default values:

[Image:System8.jpg](#) Reboot: click to hard-reboot the device in the current configuration. Any non-applied changes will be lost. Reset to Defaults: click to reset the device to factory defaults.

Retrieved from "<http://wiki.ubnt.com/wiki/index.php/AirOS>"

This page was last modified 11:25, 25 July 2008. This page has been accessed 43,722 times.

- [Privacy policy](#)
- [About Ubiquiti Wiki](#)
- [Disclaimers](#)
- [Powered by MediaWiki](#)