Log in / create account

UBIQUITI NETWORKS wiki

Main Page | Community portal | Current events | Recent changes | Random page | Help

ht hcraeS

Go Search

Page View source

modified on 3 February 2010 at 10:15 ••• 70,629 view s

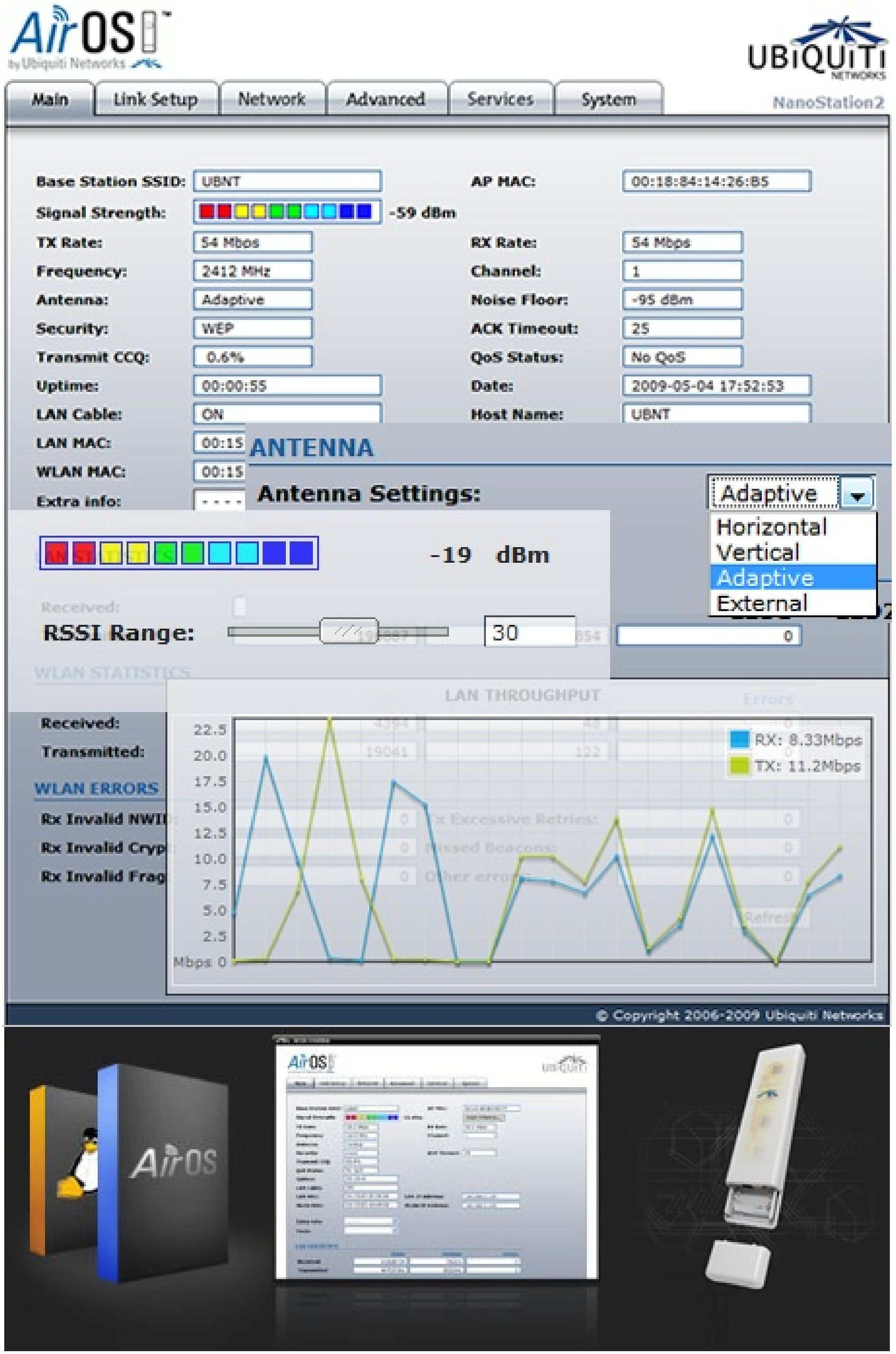
AirOS 3.4

AirOS™ by Ubiquiti Networks

User's Guide v3.4

UBIQUITI NETWORKS

Contents [hide]



Base Station SSID: UBNT
Signal Strength: -59 dBm
TX Rate: 54 Mbps
Frequency: 2412 MHz
Antenna: Adaptive
Security: WEP
Transmit CCQ: 0.6%
Uptime: 00:00:55
LAN Cable: ON
LAN MAC: 00:15
WLAN MAC: 00:15
Extra info: - - - -

AP MAC: 00:18:84:14:26:B5
RX Rate: 54 Mbps
Channel: 1
Noise Floor: -95 dBm
ACK Timeout: 25
QoS Status: No QoS
Date: 2009-05-04 17:52:53
Host Name: UBNT

ANTENNA
Antenna Settings: Adaptive

-19 dBm
RSSI Range: 30

AirOS v3.4 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.

AirOS v3.4 Configuration Guide

This guide presents the detailed description of the AirOS operating system version 3.4 which is integrated into long-range embedded systems and wireless ISP (WISP) solutions provided by Ubiquiti Networks, Inc.

2.4GHz products

2.4 GHz *(IEEE 802.11b/g)* products:

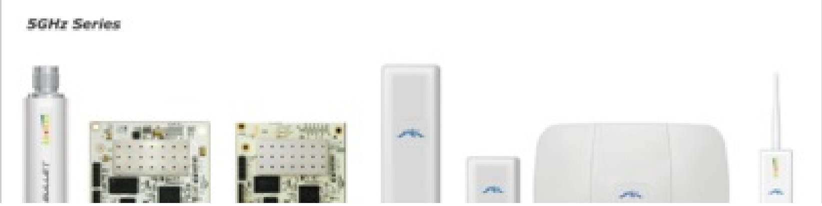
- Bullet2/2HP;
- LiteStation2;
- MiniStation;
- NanoStation2/Loco2;
- PowerStation2;
- PicoStation2/2HP.

3 GHz products (licensed bands):

- NanoStation3.

5 GHz *(IEEE 802.11a)* products:

- Bullet5/5HP;
- LiteStation5;
- NanoStation5/Loco5;
- PowerStation5;
- PicoStation5;



- WispStation5.

11n *(IEEE 802.11n)* products:

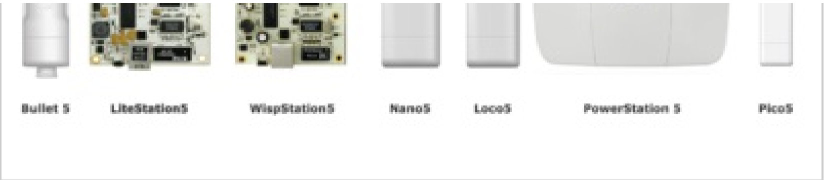
- LiteStation-SR71.

All the AirOS based devices support the following infrastructure operating modes:

- Station (Client);
- Station WDS;
- Access Point;
- Access Point WDS (Repeater).

All the AirOS based devices support the following network modes:

- Transparent bridge;
- Router.



5GHz products

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

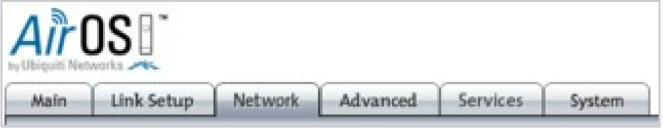
All the configuration settings accessible via web management interface are described in this document (device specific elements are described individually).

Note: the examples and pictures in this document represent NanoStation2/PowerStation5 graphical user interface which is consistent between all the AirOS based devices.

[Content]

Navigation

Each of the web management pages (listed below) contains parameters that affect a specific aspect of the device:



Configuration Management Menu

[Main] page displays current status of the device and the statistical information. There are useful network administration and monitoring tools available in Main page also (i.e. antenna alignment tool, speed test utility, site survey tool while operating in AP mode).

[Link Setup] page contains the controls for a wireless network configuration, while covering basic wireless settings which define operating mode, output power, associating details and data security options.

[Network] page covers the configuration of network operating mode, IP settings, packet filtering routines and network services (i.e. DHCP Server).

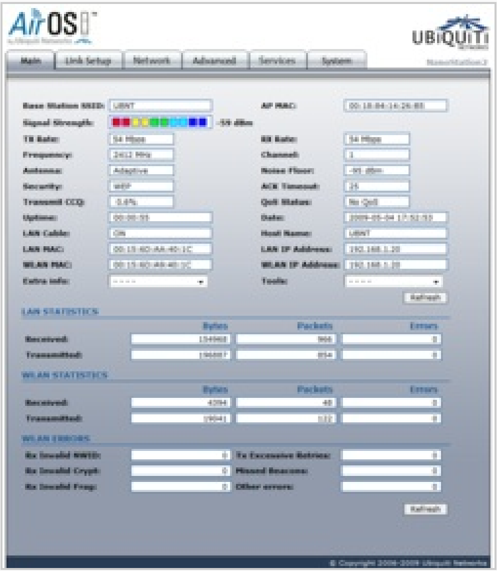
[Advanced] page settings are dedicated for more precise wireless interface control. It also includes antenna polarity, traffic shaping and QoS settings.

[Services] page covers the configuration of system management services (i.e. SNMP, NTP, System Log, Ping Watchdog and SSH/Telnet server).

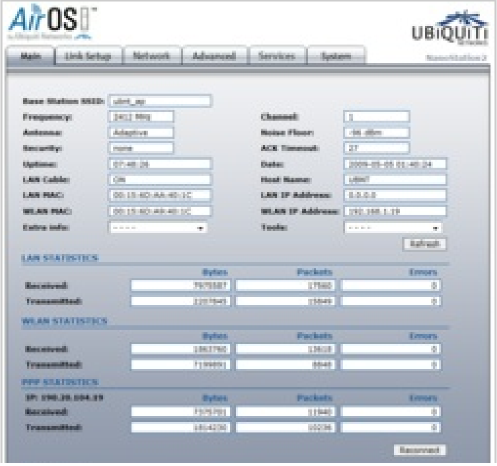
[System] page contains controls for system maintenance routines, administrator account management, device customization, interface language, firmware upgrade and configuration backup.

[Content]

Main Page



Current Status of the AirOS powered device in Client mode



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

Network administration and monitoring utilities such as antenna alignment tool, ping and traceroute utilities, 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:

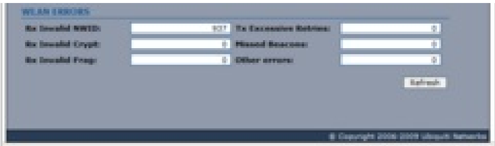
An Organizationally Unique Identifier (OUI)
Network Interface Controller (NIC) sequence.

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 dBm=10log10(P/1mW). So, 0dBm would be 1mW and –72dBm would be .0000006mW. A signal strength of –85dBm or better is recommended for stable links.

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,108Mbps (using 40MHz channel width, only available for some devices)

(802.11g, 802.11a) are possible. Typically, the higher the signal, the higher the data rate and consequently the higher the data throughput. For the maximum data throughput (54Mbps) a –70dBm or better signal is required typically.



WLAN ERRORS

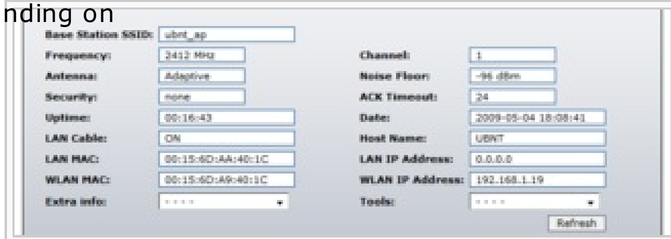
Rx Invalid NWID: 927
Tx Excessive Retries: 0
Rx Invalid Crypt: 0
Missed Beacons: 0
Rx Invalid Frag: 0
Other errors: 0

Refresh

© Copyright 2006-2009 Ubiquiti Networks

Current Status of the AirOS powered device in Access Point mode

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, for NanoStation 3, 3400-3650MHz (licensed in the US) and for 802.11b/g operation, 2412-2472MHz. However, the valid frequency range will vary depending on local country regulations. For more information regarding frequency support please visit the compliance section of Ubiquiti Wiki.

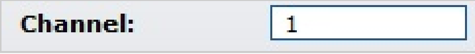


Base Station SSID: ubnt_ap
Frequency: 2412 MHz
Channel: 1
Antenna: Adaptive
Noise Floor: -96 dBm
Security: none
ACK Timeout: 24
Uptime: 00:16:43
Date: 2009-05-04 18:08:41
LAN Cable: ON
Host Name: UBNT
LAN MAC: 00:15:6D:AA:40:1C
LAN IP Address: 0.0.0.0
WLAN MAC: 00:15:6D:A9:40:1C
WLAN IP Address: 192.168.1.19
Extra info: - - - -
Tools: - - - -

Refresh

Status Reporting in AP mode

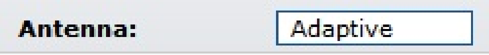
Channel: This is the 802.11 channel number that corresponds to the operating frequency. Device uses the selected channel to transmit and receive data. More information is provided in the *Link Setup* section.



Channel: 1

Current Channel used by the device

Antenna: This shows which antenna option the AirOS device is using currently. Most of Ubiquiti devices have 3 antenna options: vertical, horizontal, and Adaptive Antenna Polarity (AAP) options. External antenna option is available on several models as well. More information is provided in the *Advanced* settings section.



Antenna: Adaptive

Current Antenna used by the device

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

Security: This is the current security setting. "None" value is displayed if wireless security is disabled, WEP, WPA or WPA2 value is displayed if the corresponding wireless security method is used. More information is provided in the *Link Setup* section.

ACK Timeout: displays the current timeout value for ACK frames. ACK Timeout can be set manually or self-adjusted automatically. The **ACK Timeout** (Acknowledgement frame Timeout) specifies how long the 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.

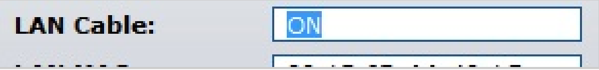
Transmit CCQ: This is an index of which evaluates the wireless Client Connection Quality. It takes into account transmit errors, latency, and throughput while evaluating the ratio of successfully transmitted packets against the re-transmitted ones and taking into account current rate ratio against the 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”. Accurate system date and time is retrieved from the internet services using NTP (Network Time Protocol). System date and time will be set to inaccurate default values after each reboot cycle if NTP is not enabled as most of the AirOS based devices have no autonomous power system for the internal clock.

LAN cable: displays the current status of the Ethernet port connection. This can alert system operator-technician that LAN cable is not plugged into device and there is no active Ethernet connection.


LAN Cable: ON

Current Status of LAN Cable

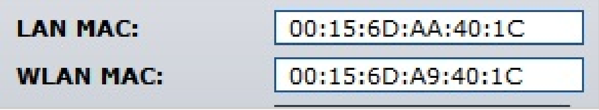
Host Name: displays the customizable name (ID) of the AirOS based device. Host Name will be represented in popular Router Operating Systems registration screens and discovery tools.

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.

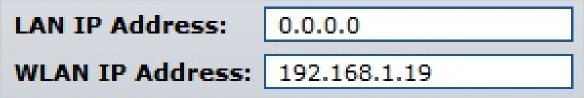
WLAN MAC: displays the MAC address of the AirOS device WLAN (Wireless) interface.

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


LAN MAC: 00:15:6D:AA:40:1C

WLAN MAC: 00:15:6D:A9:40:1C

LAN and WLAN MAC


LAN IP Address: 0.0.0.0

WLAN IP Address: 192.168.1.19

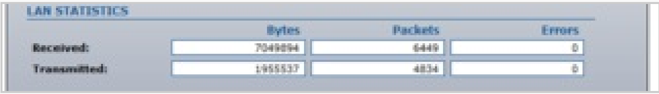
LAN and WLAN IP Addresses

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.

[Content]

Statistics Reporting

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.


LAN STATISTICS

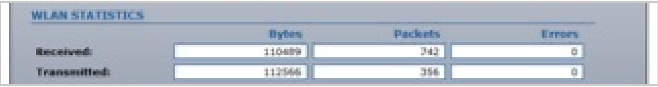
	Bytes	Packets	Errors
Received:	7049894	6449	0
Transmitted:	1955537	4834	0

LAN interface Statistics

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 in the link layer. High value of the Errors may indicate network hardware faults or misconfiguration.

WLAN Statistics: section displays the detailed receive and transmit statistics (*Bytes*, *Packets*, and "Errors") of the *wireless interface*.


WLAN STATISTICS

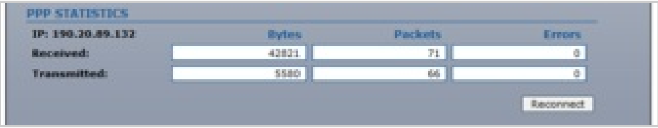
	Bytes	Packets	Errors
Received:	110489	742	0
Transmitted:	112566	356	0

WLAN interface Statistics

This statistics represents the total amount of unicast and broadcast IP data transferred between devices through the *wireless interface* either way.

As long as there is some network traffic being generated or passed through the *wireless interface*, Received and Transmitted Bytes, Packets and Errors (if any) value will go on increasing.

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 while AirOS based device operates in *Router* mode with the *PPPoE* option enabled.


PPP STATISTICS

IP: 190.20.89.132	Bytes	Packets	Errors
Received:	42821	71	0
Transmitted:	5580	66	0

PPP interface Statistics

IP address of the PPP *interface* will be displayed if it is obtained through the established

PPPoE connection, otherwise "Not Connected" message will be displayed.

Activating the **Reconnect** button will initialize the PPPoE reconnection routine which should require system reboot sequence otherwise. This control should be used for troubleshooting purposes only when PPPoE tunnel is established but the IP connection is idle.

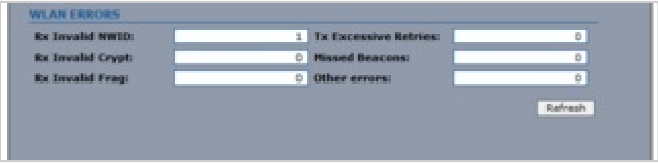
This statistics represents the total amount of unicast and broadcast IP data transferred between AirOS powered device and PPPoE server through the *PPP* tunnel either way.

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 aboutPPPoE setup.

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.



WLAN ERRORS

Rx Invalid NWID: 1
Rx Invalid Crypt: 0
Rx Invalid Frag: 0
Tx Excessive Retries: 0
Missed Beacons: 0
Other errors: 0

WLAN Errors Statistics

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

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 can indicate that the wireless client is out of range.

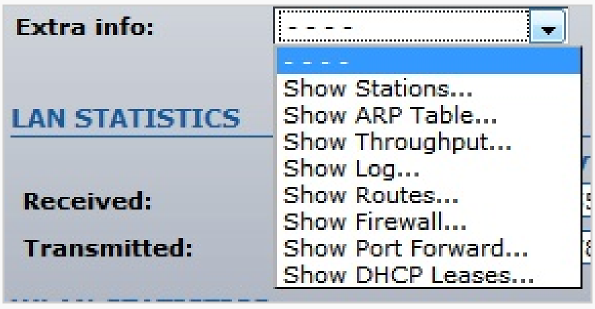
Other errors value represents the total number of transmitted and received packets that were lost or discarded for other reasons.

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

[Content]

Extra info

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



Extra info: - - - -

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

The following statistics for every station associated is represented in the station statistics window:

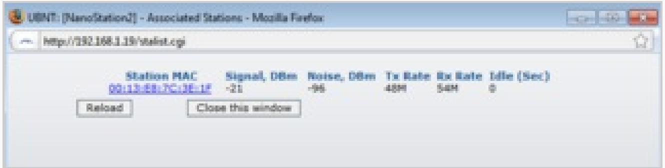
Station MAC of the station which is associated;

Signal (dBm) value represents the last received wireless signal level:

Signal (dBm) value represents the last received wireless signal level;
Noise (dBm) value displays the value of the noise level wireless signal was received;
Tx/Rx Rate value represents the data rates of the last transmitted and received packets;
Idle (sec) value represents the time (in seconds) since last packet was received from the particular station.

Extra Info Menu

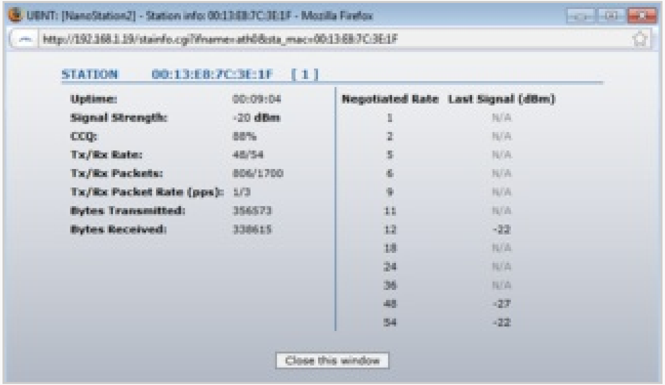
The information in the station statistics window can be updated using the **Reload** button. Window can be closed with the **Close this window** button.


UBNT: [NanoStation2] - Associated Stations - Mozilla Firefox
http://192.168.1.19/stalist.cgi
Reload
Close this window

Station MAC	Signal, DBm	Noise, DBm	Tx Rate	Rx Rate	Idle (Sec)
00:13:E8:7C:3E:1F	-21	-96	48M	54M	0

Status of the Associated Stations

Detailed information can be retrieved while selecting the particular *MAC* of the associated station:
Uptime value represents the running total of time the station is associated. The time is expressed in days, hours, minutes and seconds;
Signal Strength value represents the last received wireless signal level;
CCQ value represents the quality of the connection to the Station;
Tx/Rx Rate represents the data rates of the last transmitted and received packets;
Tx/Rx Packets value represents the total amount of packets transmitted to and received from the Station during the connection uptime;
Tx/Rx Packet Rate (packets per second) represents the mean value of the transmitted and received packet rate;
Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;
Negotiated Rate/Last Signal (dBm) table values represent the received wireless signal level along with the all data rates of recently received packets. "N/A" value is represented as the *Last Signal* if no packets were received on that particular data rate.


UBNT: [NanoStation2] - Station info: 00:13:E8:7C:3E:1F - Mozilla Firefox
http://192.168.1.19/stainfo.cgi?ifname=ath0&sta_mac=00:13:E8:7C:3E:1F
Close this window

STATION 00:13:E8:7C:3E:1F [1]

Uptime:	00:09:04
Signal Strength:	-20 dBm
CCQ:	88%
Tx/Rx Rate:	48/54
Tx/Rx Packets:	806/1700
Tx/Rx Packet Rate (pps):	1/3
Bytes Transmitted:	356573
Bytes Received:	338615

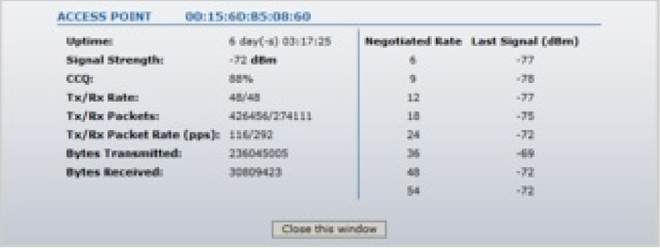
Negotiated Rate	Last Signal (dBm)
1	N/A
2	N/A
5	N/A
6	N/A
9	N/A
11	N/A
12	-22
18	N/A
24	N/A
36	N/A
48	-27
54	-22

Statistics of the Associated Station

The information in the statistic window is updated automatically. Window can be closed with the **Close this window** button.

Show AP Info: selection opens the connection statistics window while operating in Station mode.

The following link statistics is provided:
MAC of the Access Point station is associated to;
Uptime value represents the running total of time the stations is associated to the AP. The time is expressed in days, hours, minutes and seconds;
Signal Strength value represents the last received wireless signal level;
CCQ value represents the quality of the connection to the AP;
Tx/Rx Rate represents the data rates of the last transmitted and received packets;
Tx/Rx Packets value represents the total amount of packets transmitted and received during the connection;
Tx/Rx Packet Rate (packets per second) represents the mean value of the transmitted and received packet rate;
Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;



ACCESS POINT 00:15:6D:85:08:60

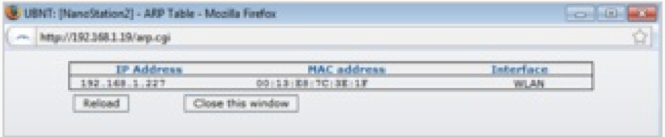
Uptime:	6 day(-s) 03:17:25
Signal Strength:	-72 dBm
CCQ:	88%
Tx/Rx Rate:	48/48
Tx/Rx Packets:	426456/274111
Tx/Rx Packet Rate (pps):	116/292
Bytes Transmitted:	236045005
Bytes Received:	30809423

Negotiated Rate	Last Signal (dBm)
6	-77
9	-78
12	-77
18	-75
24	-72
36	-69
48	-72
54	-72

Details of the connection with the associated Access Point

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

The information in the statistic window is updated automatically. Window can be closed with the **Close this window** button.


UBNT: [NanoStation2] - ARP Table - Mozilla Firefox

http://192.168.1.19/arp.cgi

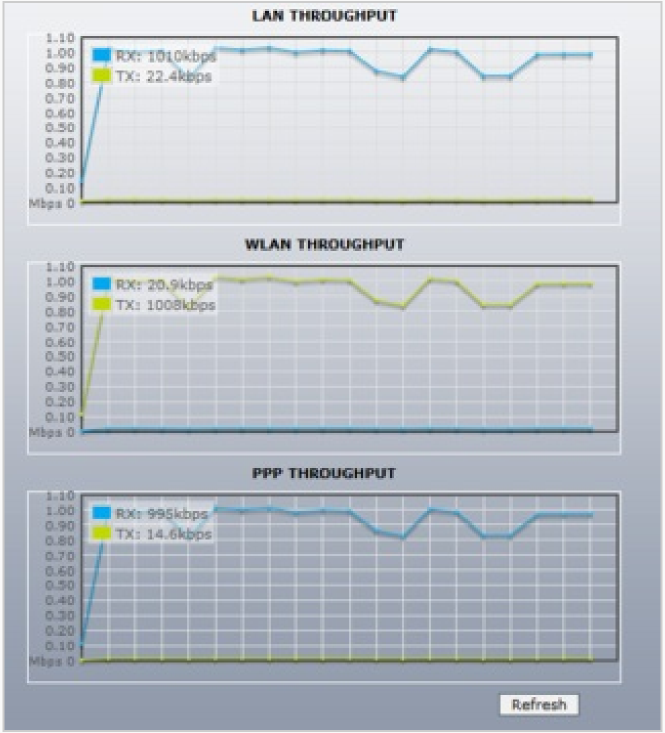
IP Address	MAC address	Interface
192.168.1.227	00:13:E8:7C:3E:1F	WLAN

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.



Status of the throughput on LAN/WLAN/PPP interface

Show Throughput selection opens statistics window which continuously represents the current data traffic on the LAN, WLAN and PPP interfaces in both graphical and numerical form. The chart scale and throughput dimension (Bps, Kbps, Mbps) changes dynamically according to the mean throughput value.

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

Show Log selection opens system log window which lists all the registered system events.

All the entries in the system log will be deleted if the **Clear** button is activated. The *System Log* content is updated if **Reload** button is activated. Window can be closed with the **Close this window** button.

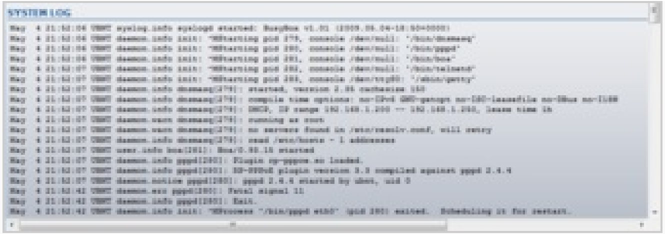
Message "Syslog is disabled, unable to show system messages" is displayed if the *System Log* is not enabled. *System Log* configuration description is provided in the *Services* section.

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

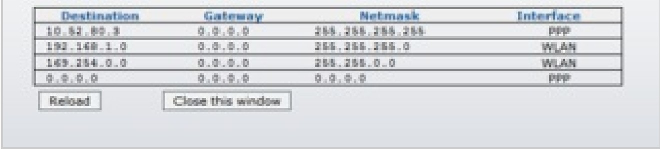
system and chooses the appropriate interface to forward the packet to. The system choice depends on static routing rules – entries, which are registered in system routing table. Static routes to specific hosts, networks or default gateway are set up automatically according to the IP configuration of all the AirOS interfaces.

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



```
SYSTEM LOG
May  4 21:52:04 UBNT syslog.info syslogd started: BusyBox v1.01 (2009.05.04-18:50+0000)
May  4 21:52:04 UBNT daemon.info init: "Starting pid 279, console /dev/null: '/bin/dnsmasq'
May  4 21:52:04 UBNT daemon.info init: "Starting pid 280, console /dev/null: '/bin/pppd'
May  4 21:52:04 UBNT daemon.info init: "Starting pid 281, console /dev/null: '/bin/boa'
May  4 21:52:07 UBNT daemon.info init: "Starting pid 282, console /dev/null: '/bin/telnetd'
May  4 21:52:07 UBNT daemon.info init: "Starting pid 283, console /dev/ttyS0: '/sbin/getty'
May  4 21:52:07 UBNT daemon.info dnsmasq[279]: started, version 2.35 cachesize 150
May  4 21:52:07 UBNT daemon.info dnsmasq[279]: compile time options: no-IPv6 GNU-getopt no-ISC-leasefile no-DBus no-I18N
May  4 21:52:07 UBNT daemon.info dnsmasq[279]: DHCP, IP range 192.168.1.200 -- 192.168.1.250, lease time 1h
May  4 21:52:07 UBNT daemon.warn dnsmasq[279]: running as root
May  4 21:52:07 UBNT daemon.warn dnsmasq[279]: no servers found in /etc/resolv.conf, will retry
May  4 21:52:07 UBNT daemon.info dnsmasq[279]: read /etc/hosts - 1 addresses
May  4 21:52:07 UBNT user.info boa[281]: Boa/0.93.15 started
May  4 21:52:07 UBNT daemon.info pppd[280]: Plugin rp-pppoe.so loaded.
May  4 21:52:07 UBNT daemon.info pppd[280]: RP-PPPoE plugin version 3.3 compiled against pppd 2.4.4
May  4 21:52:07 UBNT daemon.notice pppd[280]: pppd 2.4.4 started by ubnt, uid 0
May  4 21:52:42 UBNT daemon.err pppd[280]: Fatal signal 11
May  4 21:52:42 UBNT daemon.info pppd[280]: Exit.
May  4 21:52:42 UBNT daemon.info init: "Process '/bin/pppd eth0' (pid 280) exited.  Scheduling it for restart.
```

System Log



Destination	Gateway	Netmask	Interface
10.52.80.3	0.0.0.0	255.255.255.255	PPP
192.168.1.0	0.0.0.0	255.255.255.0	WLAN
169.254.0.0	0.0.0.0	255.255.0.0	WLAN
0.0.0.0	0.0.0.0	0.0.0.0	PPP

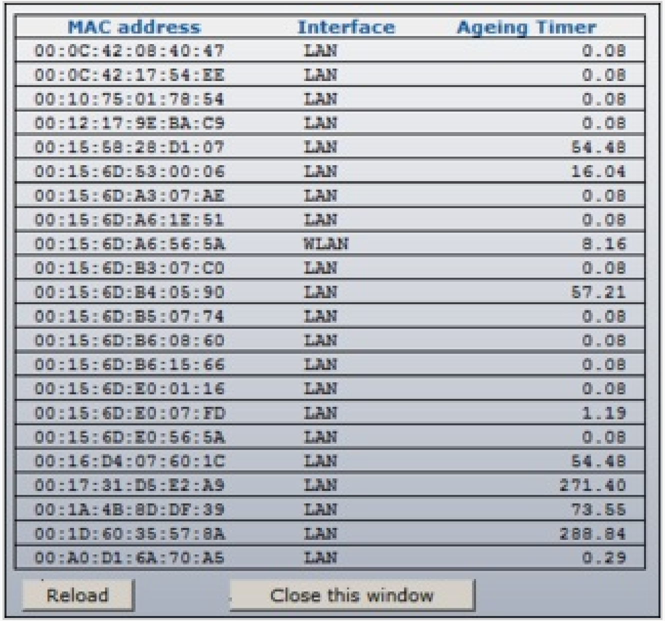
Current Status of the system routing tables

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.



MAC address	Interface	Ageing Timer
00:0C:42:08:40:47	LAN	0.08
00:0C:42:17:54:EE	LAN	0.08
00:10:75:01:78:54	LAN	0.08
00:12:17:9E:BA:C9	LAN	0.08
00:15:58:28:D1:07	LAN	54.48
00:15:6D:53:00:06	LAN	16.04
00:15:6D:A3:07:AE	LAN	0.08
00:15:6D:A6:1E:51	LAN	0.08
00:15:6D:A6:56:5A	WLAN	8.16
00:15:6D:B3:07:C0	LAN	0.08
00:15:6D:B4:05:90	LAN	57.21
00:15:6D:B5:07:74	LAN	0.08
00:15:6D:B6:08:60	LAN	0.08
00:15:6D:B6:15:66	LAN	0.08
00:15:6D:E0:01:16	LAN	0.08
00:15:6D:E0:07:FD	LAN	1.19
00:15:6D:E0:56:5A	LAN	0.08
00:16:D4:07:60:1C	LAN	54.48
00:17:31:D5:E2:A9	LAN	271.40
00:1A:4B:8D:DF:39	LAN	73.55
00:1D:60:35:57:8A	LAN	288.84
00:A0:D1:6A:70:A5	LAN	0.29

Current Status of the system bridge table

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.

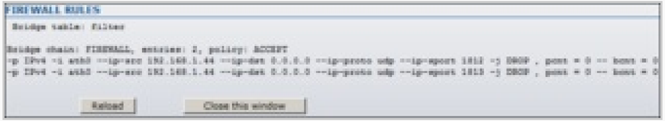
The list can be updated using the **Reload** button.

Active firewall entries in 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.



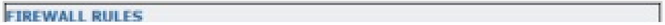
```
FIREWALL RULES
Bridge table: filter

Bridge chain: FIREWALL, entries: 2, policy: ACCEPT
-p IPv4 -i ath0 --ip-src 192.168.1.44 --ip-dst 0.0.0.0 --ip-proto udp --ip-sport 1812 -j DROP , pcnt = 0 -- bcnt = 0
-p IPv4 -i ath0 --ip-src 192.168.1.44 --ip-dst 0.0.0.0 --ip-proto udp --ip-sport 1813 -j DROP , pcnt = 0 -- bcnt = 0
```

Active Firewall entries in Bridge 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.



FIREWALL RULES

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

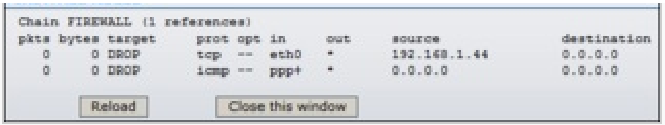
Interface name shows from which device interface DHCP client which has specified *MAC Address* is connected.

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.

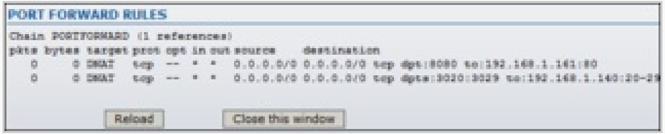
More information is provided in the *Link Setup* section.

[Content]



```
Chain FIREWALL (1 references)
pkts bytes target     prot opt in     out     source          destination
   0     0 DROP       tcp  --  eth0   *       192.168.1.44    0.0.0.0
   0     0 DROP       icmp --  ppp+   *       0.0.0.0         0.0.0.0
```

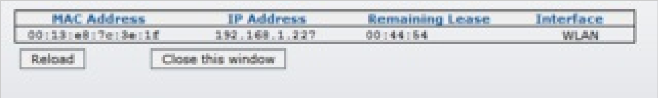
Active Firewall entries in Router mode



PORT FORWARD RULES

```
Chain PORTFORWARD (1 references)
pkts bytes target prot opt in out source    destination
   0     0 DNAT   tcp  --  *  *   0.0.0.0/0 0.0.0.0/0 tcp dpt:8080 to:192.168.1.161:80
   0     0 DNAT   tcp  --  *  *   0.0.0.0/0 0.0.0.0/0 tcp dpts:3020:3029 to:192.168.1.140:20-29
```

Active Port Forward entries in Router mode



MAC Address	IP Address	Remaining Lease	Interface
00:13:e8:7e:3e:1f	192.168.1.227	00:44:54	WLAN

Current Status of the DHCP leases

Tools

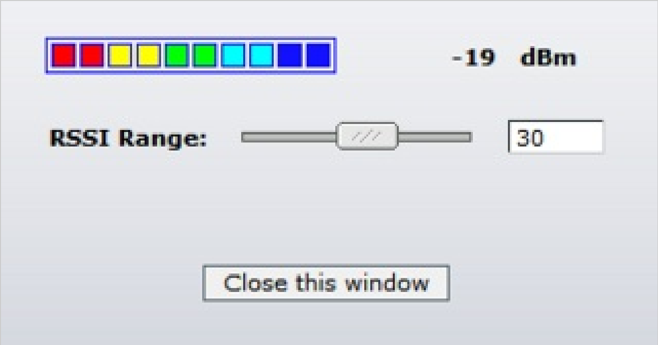
Tools: provides network utilities in pop-up window:

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

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

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 as **RSSI Range** slider actually changes an offset of the maximum indicator value thus the scale itself.

Align Antenna window can be closed with the **Close this window button**.



-19 dBm

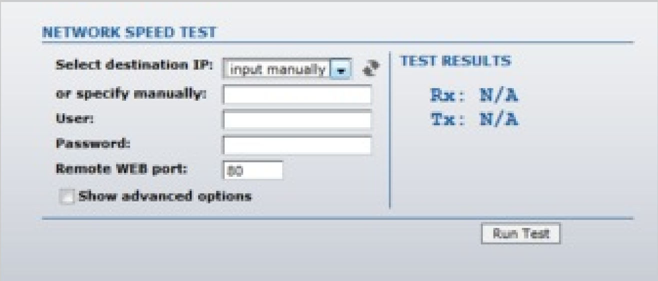
RSSI Range: 30

Antenna alignment Tool

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.

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

Access credentials (administrator username - **User** and **Password**) of the remote system should be provided for the communication between two AirOS powered devices. This is required in order to establish TCP/IP based throughput test. ICMP throughput measurement routine will be initiated if the access credentials are incorrect or not supplied.



NETWORK SPEED TEST

Select destination IP: input manually

or specify manually:

User:

Password:

Remote WEB port: 80

□ Show advanced options

TEST RESULTS

Rx: N/A

Tx: N/A

Wireless link throughput estimation

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

Show advanced options control will enable additional *Speed Test* utility options. 4 options available for the traffic *direction* while estimating the throughput maximum:
* Estimate the incoming (Rx) throughput while selecting **receive** option;
* Estimate the outgoing (Tx) throughput while selecting **transmit** option;
* First estimate the incoming (Rx) and afterwards the outgoing (Tx) throughput while selecting option **both**;
* Estimate the incoming (Rx) and the outgoing (Tx) throughput at the same time while selecting option **duplex**.
Test **Duration** and **Data amount** settings specify the test execution time:
* throughput test will stop after the specified time frame (in seconds) if the *Duration* value is set;
* throughput test will stop after the specified volume of data (in bytes) if sent/received if the *Data amount* value is set;
* the test will stop after any of the criteria is met if both (*Duration* and *Data amount*) values are specified.

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

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

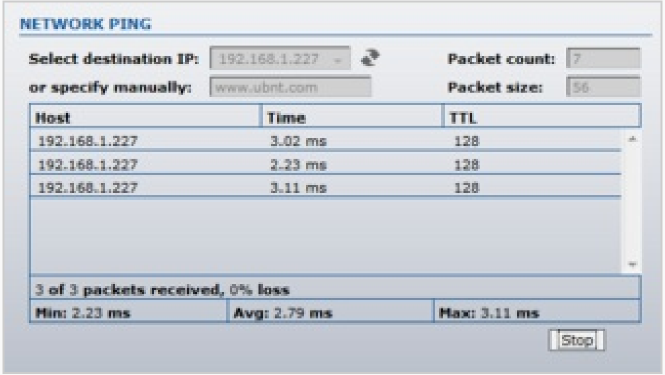
Ping utility should be used for the preliminary link quality and packet latency estimation between two network devices using the ICMP packets.

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.



NETWORK PING

Select destination IP: 192.168.1.227

or specify manually: www.ubnt.com

Packet count: 7

Packet size: 56

Host	Time	TTL
192.168.1.227	3.02 ms	128
192.168.1.227	2.23 ms	128
192.168.1.227	3.11 ms	128

3 of 3 packets received, 0% loss

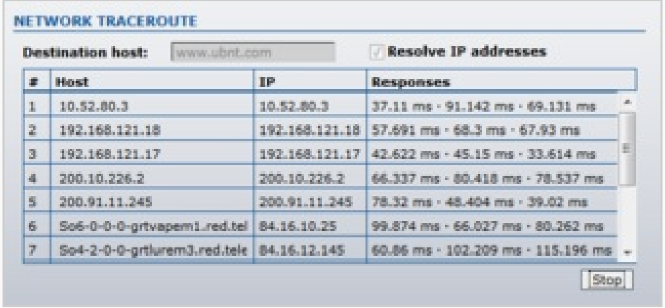
Min: 2.23 ms Avg: 2.79 ms Max: 3.11 ms

Wireless link quality estimation with Network Ping 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.



NETWORK TRACEROUTE

Destination host: www.ubnt.com

☑ Resolve IP addresses

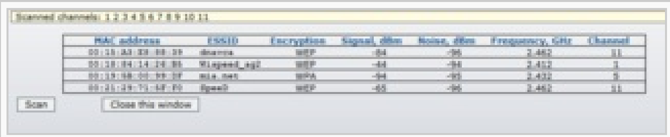
#	Host	IP	Responses
1	10.52.80.3	10.52.80.3	37.11 ms - 91.142 ms - 69.131 ms
2	192.168.121.18	192.168.121.18	57.691 ms - 68.3 ms - 67.93 ms
3	192.168.121.17	192.168.121.17	42.622 ms - 45.15 ms - 33.614 ms
4	200.10.226.2	200.10.226.2	66.337 ms - 80.418 ms - 78.537 ms
5	200.91.11.245	200.91.11.245	78.32 ms - 48.404 ms - 39.02 ms
6	So6-0-0-0-grtvapem1.red.tel	84.16.10.25	99.874 ms - 66.027 ms - 80.262 ms
7	So4-2-0-0-grtlurem3.red.tele	84.16.12.145	60.86 ms - 102.209 ms - 115.196 ms

Finding the route across the network with Traceroute utility

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

Site Survey reports *MAC Address*, "ESSID", *Encryption* type (if any), *Signal Strength* (dBm), *Frequency* (GHz) and wireless *channel* of all the surrounding Access Points which can be found by the AirOs based device.

The *Site Survey* can be updated using the **Scan** button. *Site Survey* window can be closed with the **Close this window button**.


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

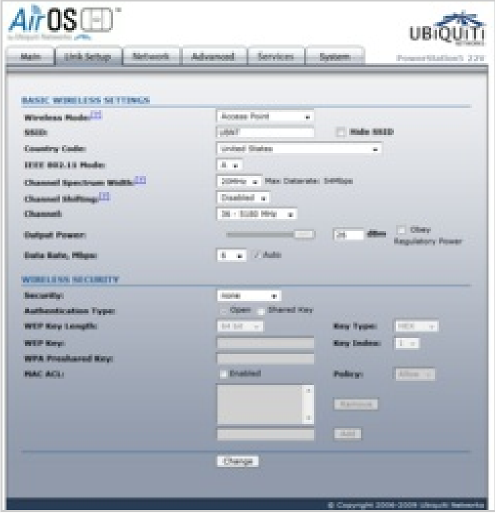
MAC address	ESSID	Encryption	Signal, dBm	Noise, dBm	Frequency, GHz	Channel
00:15:A3:33:08:39	dharma	WEP	-84	-95	2.462	11
00:18:84:14:24:B5	Wlagend_ag2	WEP	-44	-94	2.412	1
00:19:5B:00:99:DF	mia_net	WPA	-94	-95	2.432	5
00:21:29:71:6F:F0	Spee3	WEP	-65	-96	2.462	11

Wireless Site Survey utility

[Content]

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

Wireless Mode:[?] Access Point
SSID: ubnt ☐ Hide SSID
Country Code: United States
IEEE 802.11 Mode: A
Channel Spectrum Width:[?] 20MHz Max Datarate: 54Mbps
Channel Shifting:[?] Disabled
Channel: 36 - 5180 MHz
Output Power: 26 dBm ☐ Obey Regulatory Power
Data Rate, Mbps: 6 ☑ Auto

WIRELESS SECURITY

Security: none
Authentication Type: ○ Open ○ Shared Key
WEP Key Length: 64 bit Key Type: HEX
WEP Key: Key Index: 1
WPA Preshared Key:
MAC ACL: ☐ Enabled Policy: Allow

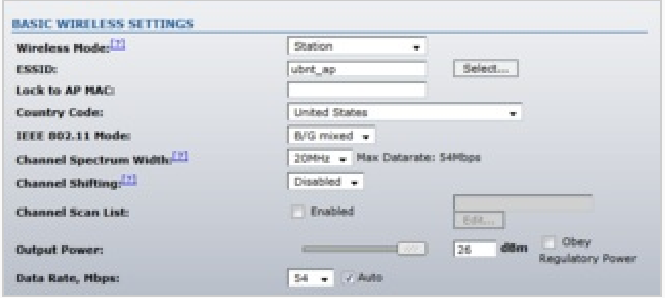
Link Setup Page - PowerStation5

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 v3.4 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.

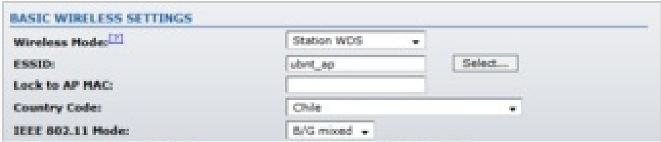

BASIC WIRELESS SETTINGS

Wireless Mode:[?] Station
ESSID: ubnt_ap Select...
Lock to AP MAC:
Country Code: United States
IEEE 802.11 Mode: B/G mixed
Channel Spectrum Width:[?] 20MHz Max Datarate: 54Mbps
Channel Shifting:[?] Disabled
Channel Scan List: ☐ Enabled Edit...
Output Power: 26 dBm ☐ Obey Regulatory Power
Data Rate, Mbps: 54 ☑ Auto

Station Basic Wireless Settings

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.

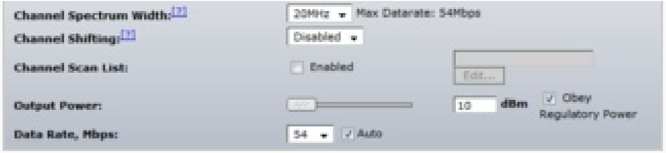
3. **Access Point**: This is an 802.11 Access Point


BASIC WIRELESS SETTINGS

Wireless Mode:[?] Station WDS
ESSID: ubnt_ap Select...
Lock to AP MAC:
Country Code: Chile
IEEE 802.11 Mode: B/G mixed

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.

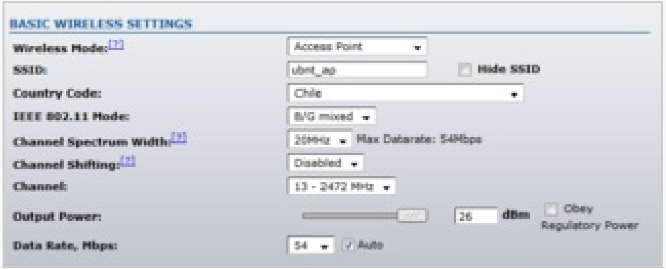


Channel Spectrum Width:[?] 20MHz ▾ Max Datarate: 54Mbps
Channel Shifting:[?] Disabled ▾
Channel Scan List: □ Enabled Edit...
Output Power: 10 dBm ☑ Obey Regulatory Power
Data Rate, Mbps: 54 ▾ ☑ Auto

Station WDS Basic Wireless Settings

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.

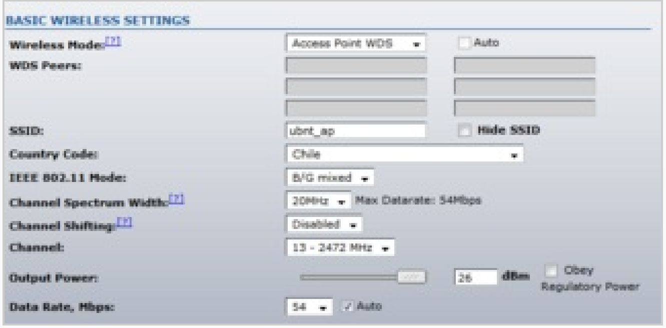


BASIC WIRELESS SETTINGS
Wireless Mode:[?] Access Point ▾
SSID: ubnt_ap □ Hide SSID
Country Code: Chile ▾
IEEE 802.11 Mode: B/G mixed ▾
Channel Spectrum Width:[?] 20MHz ▾ Max Datarate: 54Mbps
Channel Shifting:[?] Disabled ▾
Channel: 13 - 2472 MHz ▾
Output Power: 26 dBm □ Obey Regulatory Power
Data Rate, Mbps: 54 ▾ ☑ Auto

Access Point Basic Wireless Settings

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).

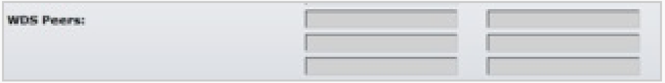
Enter the MAC address of the paired WDS device in the WDS Peer entry field. One MAC address should be specified for Point-to-Point connection use case, up to six WDS Peers can be specified for Point-to-Multi-Point connection use case.



BASIC WIRELESS SETTINGS
Wireless Mode:[?] Access Point WDS ▾ □ Auto
WDS Peers:
SSID: ubnt_ap □ Hide SSID
Country Code: Chile ▾
IEEE 802.11 Mode: B/G mixed ▾
Channel Spectrum Width:[?] 20MHz ▾ Max Datarate: 54Mbps
Channel Shifting:[?] Disabled ▾
Channel: 13 - 2472 MHz ▾
Output Power: 26 dBm □ Obey Regulatory Power
Data Rate, Mbps: 54 ▾ ☑ Auto

Access Point WDS Basic Wireless Settings

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 (Access Points) according to the SSID setting. Access Point operating in WDS mode should have the same SSID as the WDS Peer in order to establish the connection automatically while **Auto** option is enabled. This configuration is also known as the *repeater* mode. AP WDS **Auto** option can not be selected if any type of WPA or WPA2 security is used as WPA requires different roles on AP configuration (authenticator or supplicant).



WDS Peers:

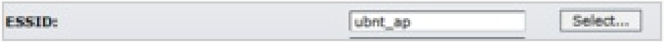
WDS Peers

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*.

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 (applicable for STA mode only) 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.

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.

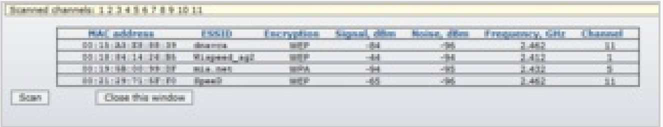


ESSID: ubnt_ap Select...

ESSID

ESSID: – specify the ESSID of the Access Point which 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.

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.



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

MAC address	ESSID	Encryption	Signal, dBm	Noise, dBm	Frequency, GHz	Channel
00:15:A3:33:88:39	dharma	WEP	-84	-96	2.462	11
00:18:84:14:24:85	Wlagsed_ag2	WEP	-44	-94	2.412	1
00:19:5B:03:99:DF	mia_net	WPA	-94	-93	2.432	5
00:21:29:71:6F:F0	Spas0	WEP	-65	-96	2.462	11

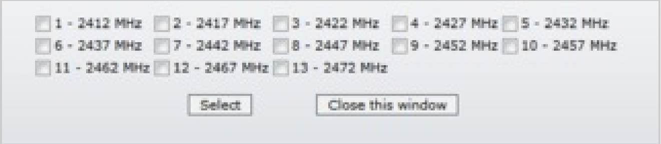
Site Survey tool for the Access Point selection

The list of the available Access Points can be retrieved using the **Select** button (not applicable to Access Point mode). This control activates *Site Survey* tool which is used for the AP selection. Site Survey will search for the available wireless networks in range on all 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.

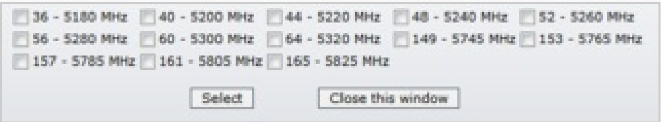
Site Survey channel scan list can be modified using the *Channel Scan List* control.



□ 1 - 2412 MHz □ 2 - 2417 MHz □ 3 - 2422 MHz □ 4 - 2427 MHz □ 5 - 2432 MHz
□ 6 - 2437 MHz □ 7 - 2442 MHz □ 8 - 2447 MHz □ 9 - 2452 MHz □ 10 - 2457 MHz
□ 11 - 2462 MHz □ 12 - 2467 MHz □ 13 - 2472 MHz

Channel Scan list selection on Nanostation2

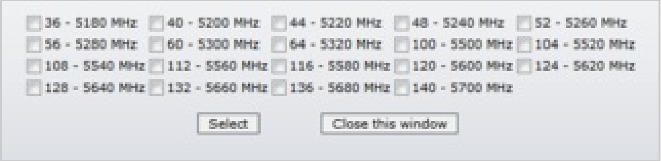
Channel Scan List: This will confine scanning only to the selected channels (applicable for Station and Station WDS mode only). The benefits of this are faster scanning as well as filtering out unwanted AP's in the results. Site Survey tool will look for the Access Points in selected channels only.



□ 36 - 5180 MHz □ 40 - 5200 MHz □ 44 - 5220 MHz □ 48 - 5240 MHz □ 52 - 5260 MHz
□ 56 - 5280 MHz □ 60 - 5300 MHz □ 64 - 5320 MHz □ 149 - 5745 MHz □ 153 - 5765 MHz
□ 157 - 5785 MHz □ 161 - 5805 MHz □ 165 - 5825 MHz

Channel Scan list selection on Powerstation5,country:USA

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 options in Channel Scan List window which is activated using the **Edit** button. *Site Survey* tool will look for the Access Points in selected channels only if the scan or site survey operation is performed in *Station* mode.



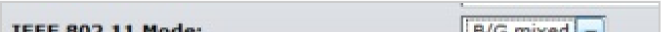
□ 36 - 5180 MHz □ 40 - 5200 MHz □ 44 - 5220 MHz □ 48 - 5240 MHz □ 52 - 5260 MHz
□ 56 - 5280 MHz □ 60 - 5300 MHz □ 64 - 5320 MHz □ 100 - 5500 MHz □ 104 - 5520 MHz
□ 108 - 5540 MHz □ 112 - 5560 MHz □ 116 - 5580 MHz □ 120 - 5600 MHz □ 124 - 5620 MHz
□ 128 - 5640 MHz □ 132 - 5660 MHz □ 136 - 5680 MHz □ 140 - 5700 MHz

Channel Scan list selection on Powerstation5,country:Spain

Lock to AP MAC: This allows the station to always maintain connection to a particular AP with a specific MAC (applicable for Station and Station WDS mode 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.

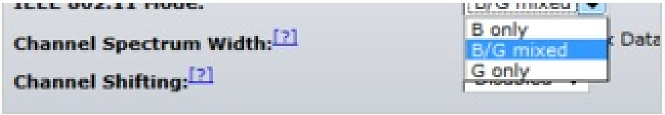
Country Code: Different countries will have different power levels and possible frequency selections. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where device will be used. The channel list, output power limits, IEEE 802.11 and Channel 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



IEEE 802.11 Mode: B/G mixed

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.

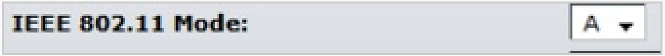


Channel Spectrum Width:[?]

Channel Shifting:[?]

IEEE 802.11 mode selection on NanoStation2

- Bullet2/2HP, LiteStation2, MiniStation, NanoStation2/loco2, PowerStation2, PicoStation2/2HP supported IEEE 802.11 modes:
  B only – connect to an 802.11b only network.
  B/G Mixed – connect to an 802.11b or 802.11g network (selected by default). This mode offers better compatibility.
  G only – connect to an 802.11g only network.



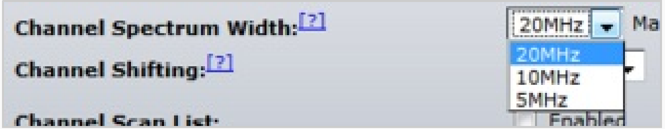
IEEE 802.11 Mode: A

IEEE 802.11 mode selection on PowerStation5

- Bullet5/HP, LiteStation5, NanoStation5/loco5, PowerStation5, PicoStation5, WispStation5 supported IEEE 802.11 modes:
  A – connect to an 802.11a network (selected by default).
- LiteStation-SR71 supported IEEE 802.11 modes:
  11n – connect to an 802.11n network (selected by default). 802.11n is compatible with 802.11b or 802.11g modes.

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 an 802.11a (or 3GHz frequency) network which supports Static Turbo feature (applicable for Bullet5/HP, LiteStation5, NanoStation5/loco5, PowerStation5, PicoStation5, WispStation5, NanoStation3 only).



Channel Spectrum Width:[?] 20MHz

Channel Shifting:[?]

Channel Scan List: Enabled

Select the Channel Spectrum Width

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. All the channels can be shifted by 5 MHz (in 802.11a mode and 3GHz) or 2 MHz (in 802.11b/g/b+g mode) from the default central channel frequency.

The benefits of this are private networking and inherent security. Using channel-shifting, networks can instantly become invisible to the millions of Wi-Fi 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 and Channel Spectrum Width and Channel Shifting option.

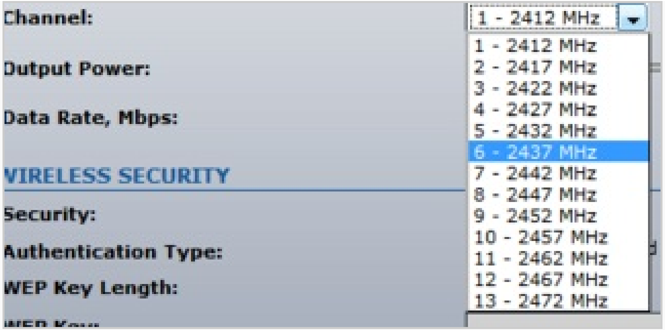
Output Power: This will configure the maximum average transmit output power (in dBm) of the wireless device. The output power at which wireless module transmits data can be specified using the slider. When entering output power value manually, the slider position will change according to the entered value. The transmit power level maximum is limited according to the country regulations. If the AirOS based device has an internal antenna (i.e. NanoStation), Output Power is the output power delivered to the internal antenna.

Obey regulatory power option must remain enabled while it will force the transmit output power to be compliant with the regulations of the selected country. In this case it will not be possible to set equivalent isotropic radiated power (EIRP) above the amount allowed per regulatory domain (different maximum output power levels and antenna gains are allowed for each IEEE 802.11a/b/g regulatory domain thus country). For more regulatory information please consult 802.11 compliance guide.

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. If you select 40MHz Channel Spectrum width the maximum data rate is 108Mbps.

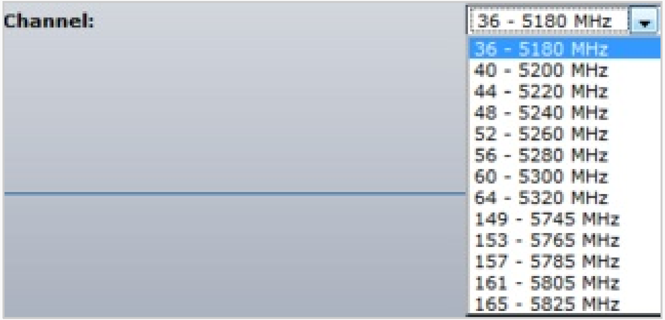
Refer to the section *Advanced Wireless Settings* for the detailed information about *rate algorithms*.

[Content]



Channel: 1 - 2412 MHz

Select a Wireless Channel on NanoStation2

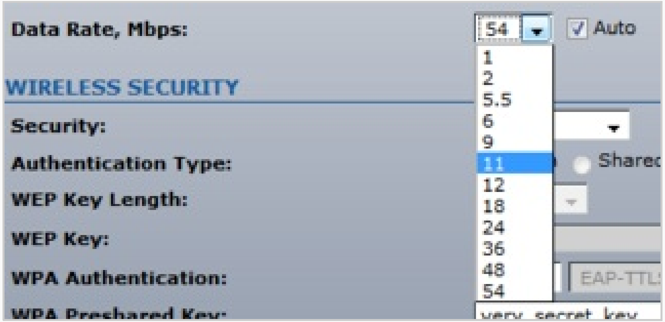


Channel: 36 - 5180 MHz

Select a Wireless Channel on PowerStation5

Output Power: 22 dBm □ Obey Regulatory Power

Output power and Obey regulatory power



Data Rate, Mbps: 54 ☑ Auto

Data rate and Auto

Wireless Security

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

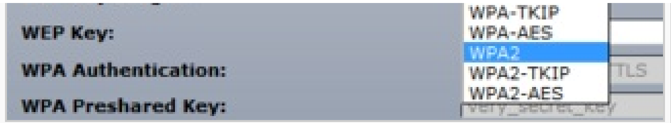
Choose the security method according to the Access Point security policy. Subscriber station should be authorized by Access Point in order to get access to the network and all the user data transferred between subscriber station and Access Point will be encrypted if the wireless security methods are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

Security: AirOS supports WEP, WPA, and WPA2 security options. Select the security mode of

WIRELESS SECURITY

Security: WEP

your wireless network:



WEP Key:
WPA Authentication:
WPA Preshared Key: very_secret_key

Wireless Security Settings

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, and there are few applications that can decrypt the WEP key in less than 10 minutes. WPA™/WPA2™ security methods should be used when possible.

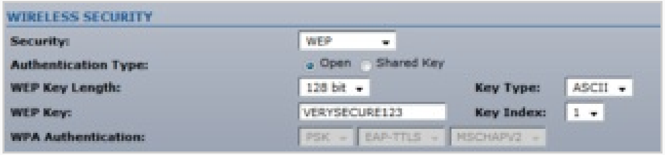
WPA – enable WPA™ security mode. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods as they are new protocols that were created under the 802.11i standard to address weaknesses in the WEP approach.

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

TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.
CCMP (commonly known as AES) - 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 – enable WPA™ security mode.
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.



WIRELESS SECURITY
Security: WEP
Authentication Type: ● Open ○ Shared Key
WEP Key Length: 128 bit   Key Type: ASCII
WEP Key: VERYSECURE123   Key Index: 1
WPA Authentication: PSK EAP-TTLS MSCHAPV2

WEP security

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 a bit higher level of wireless 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:

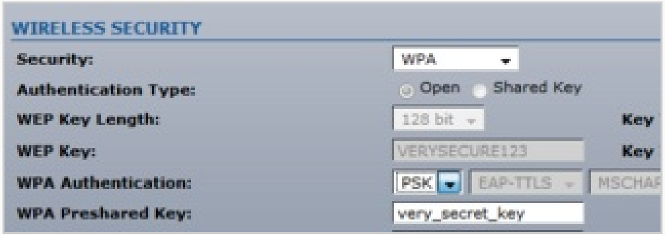
For **64-bit** – specify WEP key as 10 HEX (0-9, A-F or a-f) characters (e.g. 00112233AA) or 5 ASCII characters.
For **128-bit** – specify WEP key as 26 HEX (0-9, A-F or a-f) characters (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

Key Index: allows to specify the Index of the WEP Key used. 4 different WEP keys can be configured at the same time, but only one is used.

Effective key is set with a choice of 1, 2, 3 or 4.

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). :

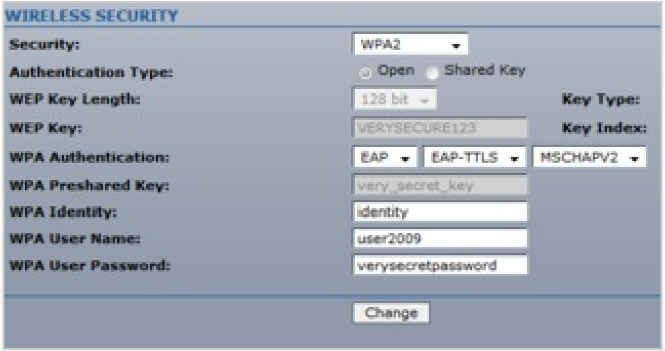
PSK – WPA™ or WPA2™ with Pre-shared Key method (selected by default).
EAP – WPA™ or WPA2™ with EAP (Extensible Authentication Protocol) IEEE 802.1x authentication method. This method is commonly used in Enterprise networks. Note: AirOS Web Management GUI supports only EAP-TTLS authentication method.



WIRELESS SECURITY
Security: WPA
Authentication Type: ○ Open ○ Shared Key
WEP Key Length: 128 bit
WEP Key: VERYSECURE123
WPA Authentication: PSK EAP-TTLS MSCHAP
WPA Preshared Key: very_secret_key

WPA/WPA2 PSK security

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 alpha-numeric password between 8 and 63 characters long.



WIRELESS SECURITY
Security: WPA2
Authentication Type: ○ Open ○ Shared Key
WEP Key Length: 128 bit
Key Type:
WEP Key: VERYSECURE123
Key Index:
WPA Authentication: EAP EAP-TTLS MSCHAPV2
WPA Preshared Key: very_secret_key
WPA Identity: identity
WPA User Name: user2009
WPA User Password: verysecretpassword

WPA/WPA2 EAP security

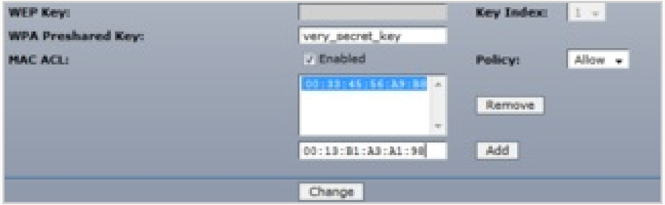
WPA Identity: identification credential (also known as *identity*) used by the supplicant for EAP authentication (applicable for STA and STA WDS modes only).

WPA User Name: identification credential (also known as *anonymous identity*) used by the supplicant for EAP tunneled authentication (EAP-TTLS) in unencrypted form (applicable for STA and STA WDS modes only).

WPA User Password: password credential used by the supplicant for EAP authentication (applicable for STA and STA WDS modes only).

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.



WEP Key:
Key Index: 1
WPA Preshared Key: very_secret_key
MAC ACL: ☑ Enabled
Policy: Allow
00:33:45:56:A9:B8
00:13:B1:A3:A1:98

MAC Address Control List

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 **Allow'**.
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 **Deny**.

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.

[Content]

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.

Network Mode: specify the operating network mode for the device. There are two modes: bridge and router.

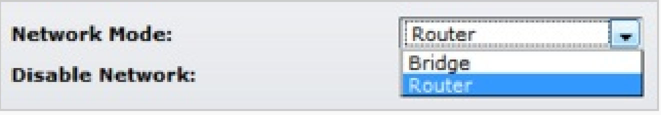
The mode depends on the network topology requirements:

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.

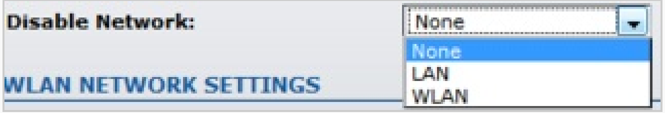
AirOS supports Multicast packet pass-through in **Router** mode.

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.


Network Mode: Router
Disable Network:

AirOS Network Mode selection

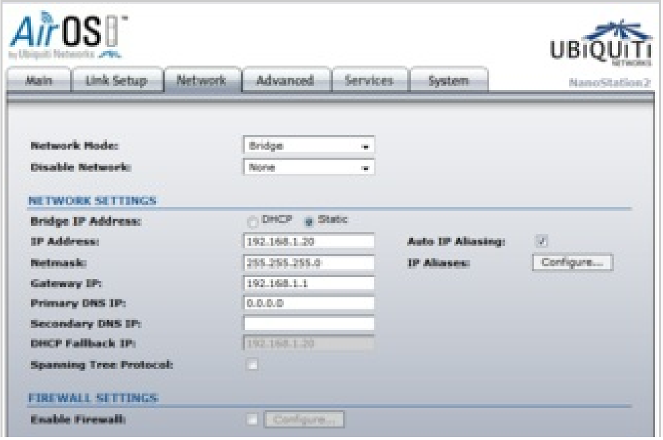
Disable Network: options can be used for disabling WLAN or LAN interface. This setting should be used with the exclusive care as no L2 or L3 connection can be established through the disabled interface. It will be impossible to access the AirOS based device from the wireless/wired network which is connected to the disabled interface.


Disable Network: None
WLAN NETWORK SETTINGS

Disable Network

Bridge Mode

In bridge mode the AirOS based device forwards all the network management and data packets from one network interface to the other without any intelligent routing. For simple applications this provides efficient and fully transparent 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:



Network Mode: Bridge
Disable Network: None
NETWORK SETTINGS
Bridge IP Address: ○ DHCP ● Static
IP Address: 192.168.1.20
Auto IP Aliasing: ☑
Netmask: 255.255.255.0
IP Aliases: Configure...
Gateway IP: 192.168.1.1
Primary DNS IP: 0.0.0.0
Secondary DNS IP:
DHCP Fallback IP: 192.168.1.20
Spanning Tree Protocol: □
FIREWALL SETTINGS
Enable Firewall: □ Configure...

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.

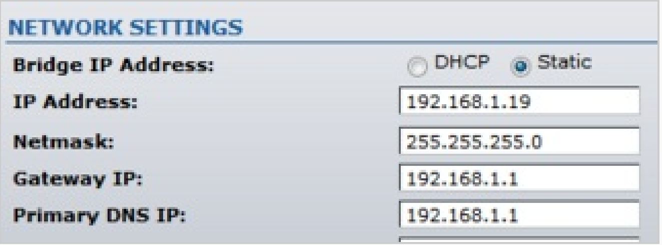
Static – choose this option to assign the static IP settings for the *bridge* interface.

Bridge mode Network Settings

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.



NETWORK SETTINGS

Bridge IP Address: ○ DHCP ● Static
IP Address: 192.168.1.19
Netmask: 255.255.255.0
Gateway IP: 192.168.1.1
Primary DNS IP: 192.168.1.1

Bridge IP Address assigned manually (Static)

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.

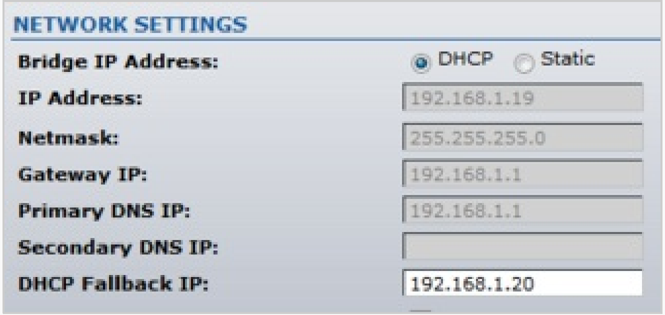
Gateway IP address should be from the same address space (on the same network segment) as the AirOS device.

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.



NETWORK SETTINGS

Bridge IP Address: ● DHCP ○ Static
IP Address: 192.168.1.19
Netmask: 255.255.255.0
Gateway IP: 192.168.1.1
Primary DNS IP: 192.168.1.1
Secondary DNS IP:
DHCP Fallback IP: 192.168.1.20

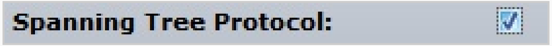
Bridge IP Address assigned automatically DHCP with IP fallback

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



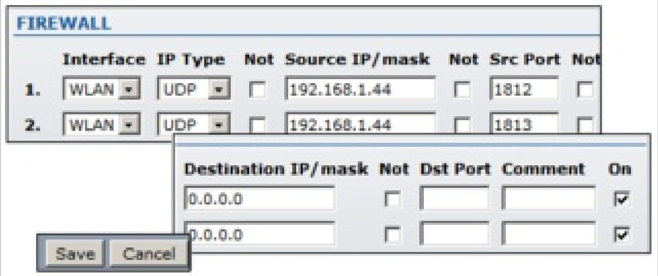
Spanning Tree Protocol: ☑

Spanning Tree Protocol enabled

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.

Spanning Tree Protocol enabled

Firewall functionality on bridge interface can be enabled using the "Enable Firewall" option. Bridge Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button.



FIREWALL

	Interface	IP Type	Not	Source IP/mask	Not	Src Port	Not
1.	WLAN	UDP	□	192.168.1.44	□	1812	□
2.	WLAN	UDP	□	192.168.1.44	□	1813	□

Destination IP/mask	Not	Dst Port	Comment	On
0.0.0.0	□			☑
0.0.0.0	□			☑

Bridge mode Firewall Configuration Settings

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN or LAN) where filtering of the incoming/passing-through packets is processed;
IP Type sets which particular L3 protocol type (IP, ICMP, TCP, UDP) should be filtered;
Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;
Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;
Destination IP/mask is 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;
Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.
Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.

On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the AirOS system operation.

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

Newly added *Firewall* entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the Firewall configuration window.

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

The list can be updated using the Reload button.

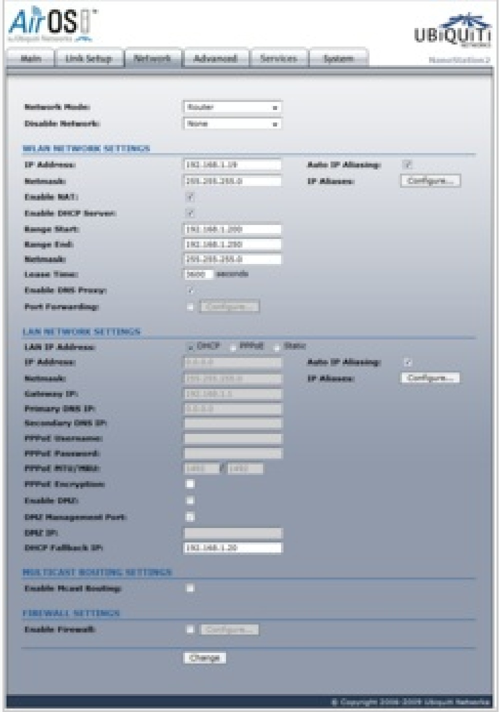
Click **Change** button to save the changes made in the *Network* page.

Router Mode

The role of the LAN and WLAN interface will change accordingly to the **Wireless Mode** while the AirOS powered device is operating in *Router* mode:

- Wireless interface and all the wireless clients connected are considered as the internal LAN and the Ethernet interface is dedicated for the connection to the external network while the AirOS powered device is operating in *AP/AP WDS* wireless mode;
- Wireless interface and all the wireless clients connected is considered as the external network and the all the network devices on LAN side as well as the Ethernet interface itself is considered as the internal network while the AirOS powered device is operating in *Station/Station WDS* mode.

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



Network Mode: Router
Disable Network: None

WLAN NETWORK SETTINGS
IP Address: 192.168.1.19
Auto IP Aliasing: ☑
Netmask: 255.255.255.0
IP Aliases: Configure...
Enable NAT: ☑
Enable DHCP Server: ☑
Range Start: 192.168.1.200
Range End: 192.168.1.250
Netmask: 255.255.255.0
Lease Time: 3600 seconds
Enable DNS Proxy: ☑
Port Forwarding: ☐ Configure...

LAN NETWORK SETTINGS
LAN IP Address: ● DHCP ○ PPPoE ○ Static
IP Address: 0.0.0.0
Auto IP Aliasing: ☑
Netmask: 255.255.255.0
IP Aliases: Configure...
Gateway IP: 192.168.1.1
Primary DNS IP: 0.0.0.0
Secondary DNS IP:
PPPoE Username:
PPPoE Password:
PPPoE MTU/MRU: 1492 / 1492
PPPoE Encryption: ☐
Enable DMZ: ☐
DMZ Management Port: ☐
DMZ IP:
DHCP Fallback IP: 192.168.1.20

MULTICAST ROUTING SETTINGS
Enable Mcast Routing: ☐

FIREWALL SETTINGS
Enable Firewall: ☐ Configure...

Change

© Copyright 2006-2009 Ubiquiti Networks

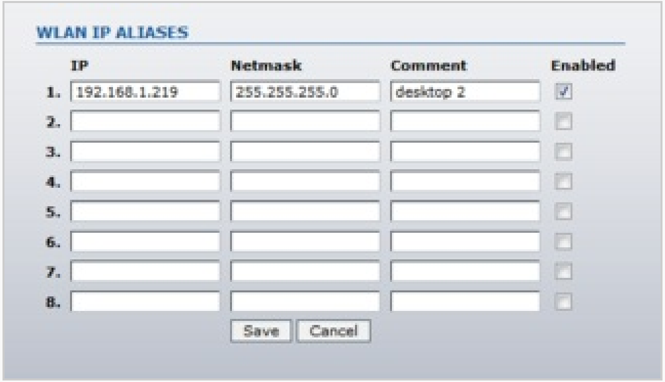
Network - Router mode

WLAN Network Settings

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

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

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



WLAN IP ALIASES

	IP	Netmask	Comment	Enabled
1.	192.168.1.219	255.255.255.0	desktop 2	☑
2.				☐
3.				☐
4.				☐
5.				☐
6.				☐
7.				☐
8.				☐

IP Aliases

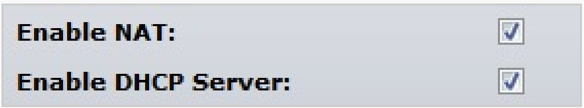
IP Aliases for internal and external network interface can be configured. *IP Aliases* can be specified using the IP Aliases configuration window which is opened while activating the "Configure" button.

IP Address is the alternative IP address for the LAN or WLAN interface, which can be used for the routing or device management purposes;
Netmask is the network address space identifier for the particular *IP Alias*;
Comments is the informal field for the comment of the particular IP Alias. Few words about the alias purpose are saved there usually;
Enabled flag enables or disables the particular IP Alias. All the added IP Aliases are saved in system configuration file, however only the enabled IP Aliases will be active during the AirOS system operation.

Newly added *IP Aliases* can be saved by activating **Save** button or discarded by activating

Cancel button in the Aliases configuration window.

Enable NAT: Network Address Translation (NAT) enables packets to be sent from the wired network (LAN) to the wireless interface IP address and then sub-routed to other client devices residing on it's local network while the AirOS powered device is operating in *AP/AP WDS* wireless mode and in the contrariwise direction in "Station/Station WDS" mode.



Enable NAT: ☑

Enable DHCP Server: ☑

Enable NAT and DHCP Server

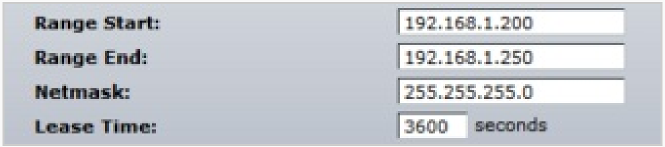
NAT is implemented using the **masquerade** type firewall rules. NAT firewall entries are stored in the iptables *nat* table, while the device is operating in Router mode. Please refer to the iptables tutorial for detailed description of the NAT functionality in *Router* mode.

Static routes should be specified in order the packets should pass-through the AirOs based device if the *NAT* is disabled in while operating in *Router* network mode.

Enable DHCP Server: Dynamic Host Configuration Protocol (DHCP) Server assigns IP addresses to clients which will associate to the wireless interface while the AirOS powered device is operating in *AP/AP WDS* wireless mode and assigns IP addresses to clients which will connect to the LAN interface while the AirOS powered device is operating in *Station/Station WDS* mode.

Range Start/End: This range determines the IP addresses given out by the DHCP server to client devices on the internal network which use dynamic IP configuration.

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



Range Start: 192.168.1.200

Range End: 192.168.1.250

Netmask: 255.255.255.0

Lease Time: 3600 seconds

DHCP Server range and lease time

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 the client while it will acquire new IP addresses from the DHCP server.

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

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

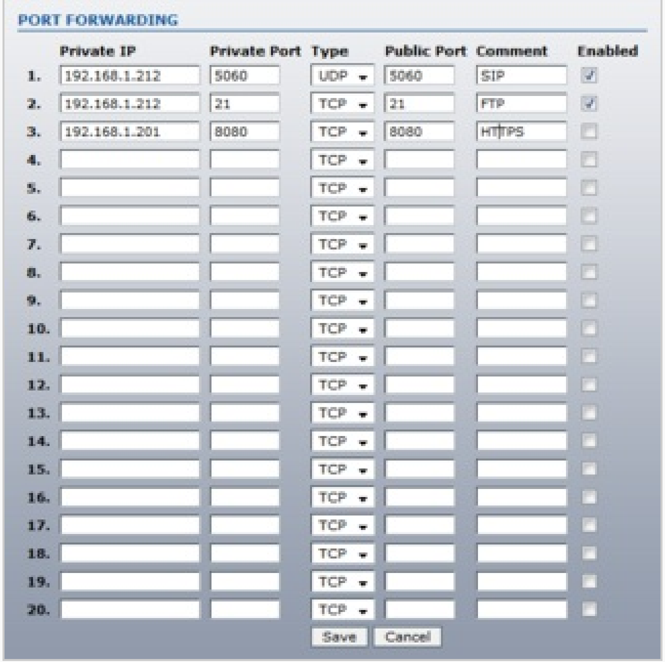
Port Forwarding rules can be set in Port Forwarding window, which is opened by enabling the **Port Forwarding** option and activating the **Configure** button.

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

Private IP is the IP of the host which is connected to the internal network and needs to be accessible from the external network;
Private Port is the TCP/UDP port of the application running on the host which is connected to the internal network. The specified port will be accessible from the external network;
Type is the L3 protocol (IP) type which need to be forwarded from the internal network.
Public Port is the TCP/UDP port of the AirOS based device which will accept and forward the connections from the external network to the host connected to the internal network.
Comments is the informal field for the comment of the particular port forwarding entry. Few words about the particular port forwarding entry purpose are saved there usually.

Enabled flag enables or disables the effect of the particular port forwarding entry. All the added firewall entries are saved in system configuration file, however only the enabled port forwarding entries will be active during the AirOS system operation.

Newly added port forwarding entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the *Port Forwarding* configuration window.



PORT FORWARDING

	Private IP	Private Port	Type	Public Port	Comment	Enabled
1.	192.168.1.212	5060	UDP	5060	SIP	☑
2.	192.168.1.212	21	TCP	21	FTP	☑
3.	192.168.1.201	8080	TCP	8080	HTTPS	□
4.			TCP			□
5.			TCP			□
6.			TCP			□
7.			TCP			□
8.			TCP			□
9.			TCP			□
10.			TCP			□
11.			TCP			□
12.			TCP			□
13.			TCP			□
14.			TCP			□
15.			TCP			□
16.			TCP			□
17.			TCP			□
18.			TCP			□
19.			TCP			□
20.			TCP			□

Port Forwarding example

LAN Network Settings

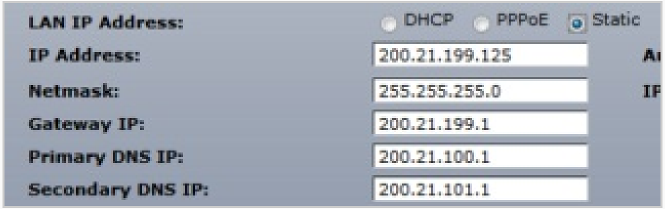
LAN IP Address: This is the IP addresses to be represented by the LAN or WLAN interface which is connected to the external network according to the wireless operation mode described above. This is the IP address can be used for the routing and the device management purposes.

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

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

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 used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the



LAN IP Address: ○ DHCP ○ PPPoE ● Static
IP Address: 200.21.199.125
Netmask: 255.255.255.0
Gateway IP: 200.21.199.1
Primary DNS IP: 200.21.100.1
Secondary DNS IP: 200.21.101.1

LAN IP Address assigned manually - Static network (alternative notation "/24") and 8 bits to identity the host.

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

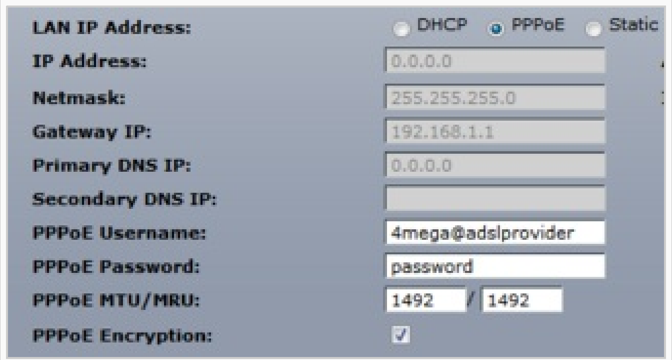
Gateway IP address should be from the same address space (on the same network segment) as the AirOS device's external network interface (Wireless interface in the *Station* case and the LAN interface in the *AP* case).

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 where the DNS requests are forwarded by the AirOS powered device.

Primary DNS server IP is mandatory. It is used by the *DNS Proxy* and for the device management purpose.

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

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.



LAN IP Address:	○ DHCP ● PPPoE ○ Static
IP Address:	0.0.0.0
Netmask:	255.255.255.0
Gateway IP:	192.168.1.1
Primary DNS IP:	0.0.0.0
Secondary DNS IP:	
PPPoE Username:	4mega@adslprovider
PPPoE Password:	password
PPPoE MTU/MRU:	1492 / 1492
PPPoE Encryption:	☑

PPPoE Internet connection (usually used by ADSL providers)

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

Valid authorization credentials are required for the PPPoE connection:

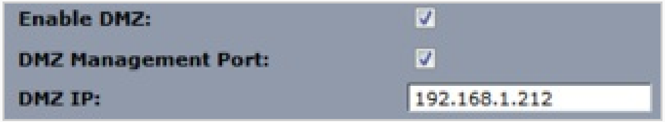
> **PPPoE Username** – username to connect to the server (must match the configured on the PPPoE server);
> **Password** – password to connect to the server (must match the configured on the PPPoE server);
> **PPPoE MTU/MRU** – the size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel;
> **PPPoE Encryption** – enables the use of MPPE encryption.

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

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

Enable DMZ: The Demilitarized zone (DMZ) can be enabled and 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. *DMZ* is commonly used with the *NAT* functionality as an alternative for the *Port Forwarding* while makes all the ports of the host network device be visible from the external network side.

DMZ Management Port: Web Management Port for the AirOS based device (TCP/IP port 80 by default) will be used for the host device if *DMZ Management Port* option is enabled. In this case AirOS device will respond to the requests from the external network as if it was the host which is specified with *DMZ IP*. It is recommended to leave *Management Port* disabled while the AirOS based device will become inaccessible from the external network if enabled.

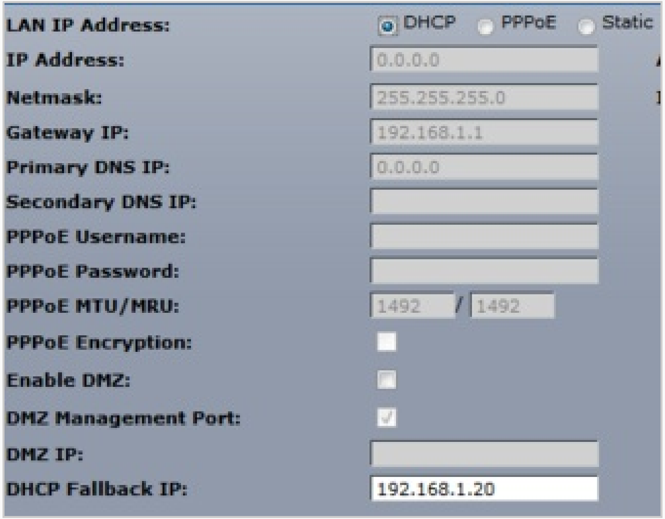


Enable DMZ:	☑
DMZ Management Port:	☑
DMZ IP:	192.168.1.212

DMZ configuration

DMZ IP: connected to the internal network host, specified with the *DMZ IP* address will be accessible from the external network.

DHCP Fallback IP: In case the external network interface of the *Router* 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.



LAN IP Address:	● DHCP ○ PPPoE ○ Static
IP Address:	0.0.0.0
Netmask:	255.255.255.0
Gateway IP:	192.168.1.1
Primary DNS IP:	0.0.0.0
Secondary DNS IP:	
PPPoE Username:	
PPPoE Password:	
PPPoE MTU/MRU:	1492 / 1492
PPPoE Encryption:	□
Enable DMZ:	□
DMZ Management Port:	☑
DMZ IP:	
DHCP Fallback IP:	192.168.1.20

LAN IP Address assigned via DHCP with IP fallback

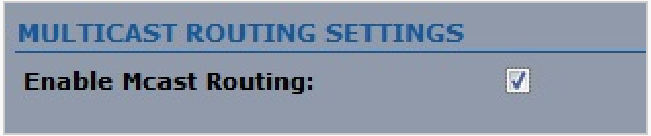
In case the IP settings of the AirOS powered device are unknown, they can be retrieved with the help of the [UBNT_Discovery_Utility Ubiquiti Discovery Utility]. Multi-platform *Utility* should be started on the administrator PC which resides on the same network segment as the AirOS device.

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.

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. It depends on the network to forward the packets to the hosts which need to receive them. Common Routers isolate all the broadcast (thus multicast) traffic between the internal and external networks, however AirOS provides the multicast traffic pass-through functionality.

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



MULTICAST ROUTING SETTINGS

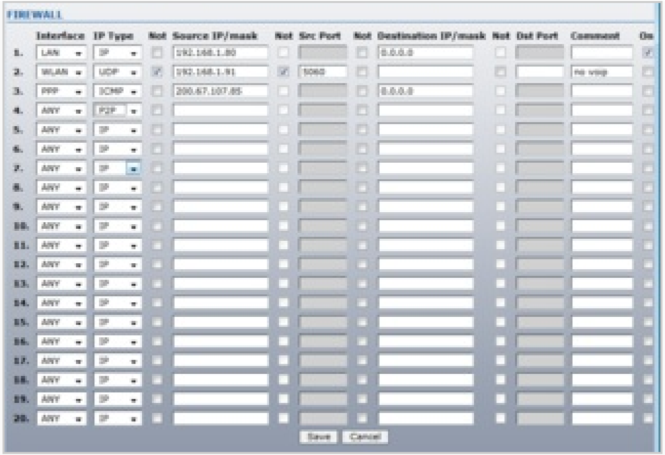
Enable Mcast Routing: ☑

Multicast routing enabled

Firewall Settings

Firewall functionality on any router interface can be enabled using the "Enable Firewall" option. Router Firewall rules can be configured, enabled or disabled while using Firewall configuration window which is opened with the "Configure" button.

Firewall entries can be specified by using the following criteria:



FIREWALL

	Interface	IP Type	Not	Source IP/mask	Not	Src Port	Not	Destination IP/mask	Not	Dst Port	Comment	On
1.	LAN	IP	□	192.168.1.80	□		□	0.0.0.0	□			☑
2.	WLAN	UDP	☑	192.168.1.91	☑	5060	□		□		no voip	□
3.	PPP	ICMP	□	200.67.107.85	□		□	0.0.0.0	□			□
4.	ANY	P2P	□		□		□		□			□
5.	ANY	IP	□		□		□		□			□
6.	ANY	IP	□		□		□		□			□
7.	ANY	IP	□		□		□		□			□
8.	ANY	IP	□		□		□		□			□
9.	ANY	IP	□		□		□		□			□
10.	ANY	IP	□		□		□		□			□
11.	ANY	IP	□		□		□		□			□
12.	ANY	IP	□		□		□		□			□
13.	ANY	IP	□		□		□		□			□
14.	ANY	IP	□		□		□		□			□
15.	ANY	IP	□		□		□		□			□
16.	ANY	IP	□		□		□		□			□
17.	ANY	IP	□		□		□		□			□
18.	ANY	IP	□		□		□		□			□
19.	ANY	IP	□		□		□		□			□
20.	ANY	IP	□		□		□		□			□

Firewall Configuration Settings

Interface the interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed;
IP Type sets which particular L3 protocol type (IP, ICMP, TCP, UDP, P2P) should be filtered;
Source IP/mask is the source IP of the packet (specified within the packet header), usually it is the IP of the host system which sends the packets;
Source Port is the source port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which sends the packets;
Destination IP/mask is 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;
Destination Port is the destination port of the TCP/UDP packet (specified within the packet header), usually it is the port of the host system application which the packet is addressed to.
Comments is the informal field for the comment of the particular firewall entry. Few words about the particular firewall entry purpose are saved there usually.
On flag enables or disables the effect of the particular firewall entry. All the added firewall entries are saved in system configuration file, however only the enabled firewall entries will be active during the AirOS system operation.
Not operators can be used for inverting the *Source IP/mask*, *Source Port*, *Destination IP/mask* and *Destination Port* filtering criteria (i.e. if *not* is enabled for the specified *Destination Port* value 443, the filtering criteria will be applied to all the packets sent to any *Destination Port* except the 443 which is commonly used by HTTPS).

Newly added *Firewall* entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the Firewall configuration window.

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

Click Change button to save the changes made in the Network page.

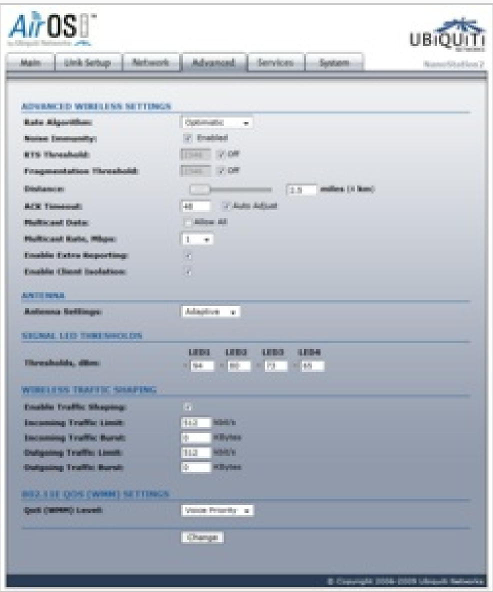
[Content]

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

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



ADVANCED WIRELESS SETTINGS

Rate Algorithm: Optimistic
Noise Immunity: ☑ Enabled
RTS Threshold: 2346 ☑ Off
Fragmentation Threshold: 2346 ☑ Off
Distance: 2.5 miles (4 km)
ACK Timeout: 48 ☑ Auto Adjust
Multicast Data: □ Allow All
Multicast Rate, Mbps: 1
Enable Extra Reporting: ☑
Enable Client Isolation: ☑

ANTENNA

Antenna Settings: Adaptive

SIGNAL LED THRESHOLDS

	LED1	LED2	LED3	LED4
Thresholds, dBm:	94	80	73	65

WIRELESS TRAFFIC SHAPING

Enable Traffic Shaping: □
Incoming Traffic Limit: 512 kbit/s
Incoming Traffic Burst: 0 kBytes
Outgoing Traffic Limit: 512 kbit/s
Outgoing Traffic Burst: 0 kBytes

802.11E QOS (WMM) SETTINGS

QoS (WMM) Level: Voice Priority

Change

© Copyright 2006-2009 Ubiquiti Networks

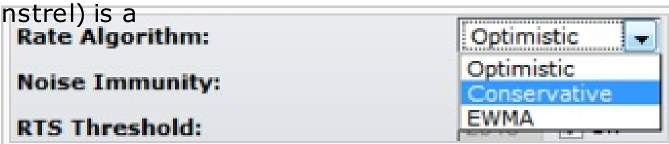
Advanced Wireless Settings in NanoStation2

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. The *optimistic rate algorithm* always looks to achieve highest throughput while sacrificing noise immunity and robustness.

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. The *conservative rate* algorithm provides the best case stability / robustness, but may compromise maximum throughput. It is recommended to select *conservative rate* algorithm when the signal strength is low due to noisy environment or link distance.

EWMA Algorithm is trying to move to a higher rate but is continuously monitoring the packet failure counters. The Exponential Weighted Moving Average (EWMA) Algorithm (also known as minstrel) is a hybrid of the Conservative and Optimistic Algorithm. It is the compromise for most of the wireless network use cases.



Rate Algorithm: Optimistic
- Optimistic
- Conservative
- EWMA

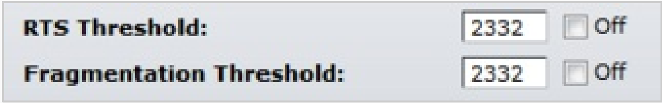
Noise Immunity:

RTS Threshold:

Rate Algorithm selection

Noise Immunity option increases the robustness of the device to operate in the presence of noise disturbance which is usually generated by external 802.11 traffic sources, channel hopping signals and other interferers.

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 Threshold: 2332 □ Off
Fragmentation Threshold: 2332 □ Off

RTS and Fragmentation Threshold

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 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

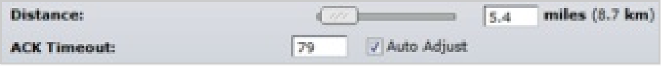
System uses Request to Send/Clear to Send frames for the handshake which provide collision reduction for access point with hidden stations. The stations are sending a RTS frame first while data is send only after handshake with an AP is completed. Stations respond with the CTS frame to the RTS which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

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

The use of fragmentation can increase the reliability of frame transmissions. Because of sending smaller frames, collisions are much less likely to occur. However lower values of the *Fragmentation Threshold* will result lower throughput as well. Minor or no modifications of the *Fragmentation Threshold* value is recommended while default setting of 2346 is optimum in most of the wireless network use cases.

AirOS has an auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance outdoor links. The user also has the ability to enter the value manually.

Distance: specify the distance value in miles (or kilometers) 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.



Distance: 5.4 miles (8.7 km)

ACK Timeout: 79 ☑ Auto Adjust

Distance and ACK Timeout

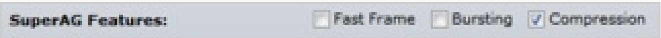
ACK Timeout: specify the *ACK Timeout*. Every time the station receives the data frame it sends an ACK frame to the AP (if transmission errors are absent). If the station receives no ACK frame from the AP within set *timeout* it re-sends the frame. The performance drops because of the too many data frames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

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

Auto Adjust control will enable the ACK Timeout Self-Configuration feature. If enabled, ACK Timeout value will be derived dynamically using an algorithm similar to the Conservative Rate Algorithm described above. It is not recommended to use *Auto Adjust* option for long range links if the signal level is low or the high level of interference is present.

If two or more stations are located at the considerably different distance from the Access Point the are associated to, the highest *ACK Timeout* for the farthest station should be set at the AP side. It is not recommended to use *Auto Adjust* option for Point-to-Multipoint connections as it will not warrant highest network performance in all the use cases.

SuperG® /SuperAG® Features: select the options to enable the chosen *SuperG®* (applicable for PowerStation2, LiteStation2) or *SuperAG®* (PowerStation5, LiteStation5) features which increase the network performance:



SuperAG Features: □ Fast Frame □ Bursting ☑ Compression

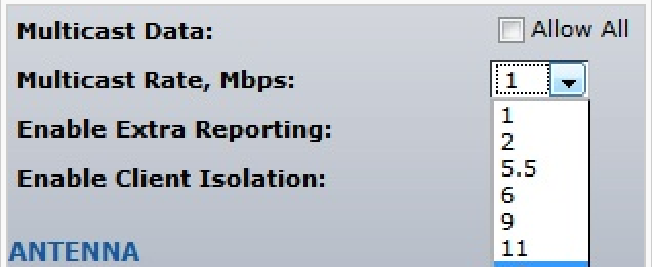
SuperAG on PowerStation5

Fast Frame – utilizes 802.11 frame aggregation and timing modifications which increases the data throughput.

Bursting – more data frames per given time period are transmitted thus the data throughput is increased.

Compression – real-time hardware data compression is enabled which allows more data sent per frame.

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



Multicast Data: □ Allow All

Multicast Rate, Mbps: 1

Enable Extra Reporting:

Enable Client Isolation:

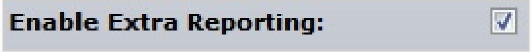
Multicast Rate: This option allows Multicast packets to be sent in higher rates (up to the 54 Mbps) than commonly used (1 Mbps at IEEE 802.11b mode, 6 Mbps at IEEE 802.11g/a mode). This is Ubiquiti's AirOS proprietary feature thus it may be incompatible with the devices from other vendors. Both AirOS based devices the sender (Station) and the receiver (Access Point) must have the same *Multicast Rate* configured in order to achieve better multicast packet throughput performance.

Antenna Settings:

SIGNAL LED THRESHOLDS

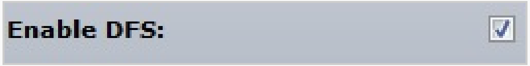
Multicast Data and Rate

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


Enable Extra Reporting: ☑

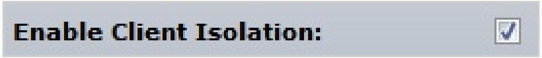
Enable Extra Reporting

Enable DFS: *DFS* is the part of the IEEE 802.11h wireless standard. *Enable DFS* option allows to enable/disable DFS support (applicable for Bullet5/5HP, LiteStation5, NanoStation5/loco5, PowerStation5, PicoStation5, WispStation5 only). DFS may be mandatory in some regulatory domains and should be tuned according to the regulations of the selected country. Please consult compliance guide and official regulations authorities for further explanation of compliance requirements for the country where AirOS based device is installed.


Enable DFS: ☑

Enable DFS

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

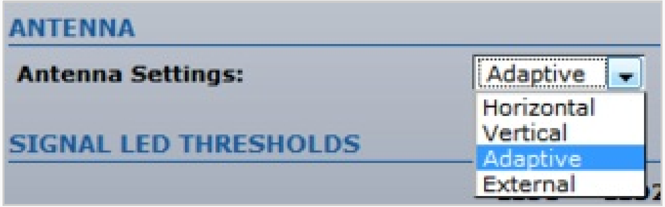

Enable Client Isolation: ☑

Enable Client Isolation

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 which can be configured using the **Antenna Settings**:


ANTENNA

Antenna Settings: Adaptive

SIGNAL LED THRESHOLDS

Antenna Polarity Configuration

Vertical and **Horizontal** antenna polarity which is the most common configuration;
Adaptive antenna mode chooses the best polarity dynamically. Adaptive antenna polarity mode which allows for the beam polarities to be switched dynamically on the fly for improved performance in heavy noise environments;
External antenna option allows a connection of the higher gain antenna to an external antenna port.

- NanoStation2, NanoStation5 has 4 antenna modes:
  1. Vertical Polarity;
  2. Horizontal Polarity;
  3. Adaptive;
  4. External.
- PowerStation5-Ext has 3 antenna modes:
  1. Antenna 1;
  2. Antenna 2;
  3. Diversity.
- PowerStation2-16D has 3 antenna modes:

1. Vertical Polarity;
2. Horizontal Polarity;
3. Adaptive;

- Loco2, Loco5 has 2 antenna modes:

1. Vertical Polarity;
2. Horizontal Polarity;

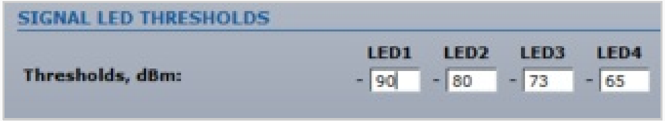
- MiniStation has 2 antenna modes:

1. Internal;
2. External.

Some AirOS devices (i.e. Bullet2/2HP, Bullet5/5HP, PicoStation 2/2HP, PicoStation 5, PowerStation2, PowerStation5) has only 1 antenna mode: Vertical, Horizontal or External. In this case *Antenna Settings* are not displayed in the *Advanced* page in this case.

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 (i.e. for antenna alignment operation).



SIGNAL LED THRESHOLDS

	LED1	LED2	LED3	LED4
Thresholds, dBm:	- 90	- 80	- 73	- 65

LED Thresholds Configuration

Signal LED Thresholds specify the marginal value of Signal Strength (dBm) which will switch on LEDs indicating signal strength:

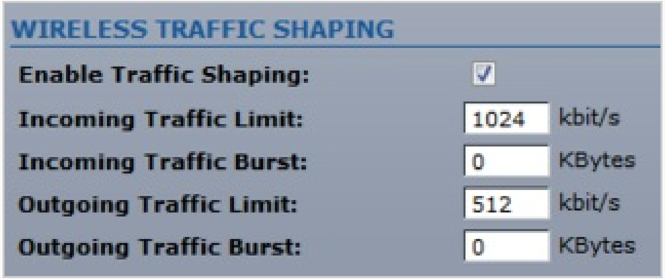
LED 1 (Red) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.
LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it.

Configuration example: if the Signal Strength (displayed in the *Main* page) fluctuates around -63 dBm, the LED Thresholds can be set to the values -70, -65, -62, -60. Note: sign "-" character should not be used for the Signal Strength value specification.

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.

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.



WIRELESS TRAFFIC SHAPING

Enable Traffic Shaping:	☑	
Incoming Traffic Limit:	1024	kbit/s
Incoming Traffic Burst:	0	KBytes
Outgoing Traffic Limit:	512	kbit/s
Outgoing Traffic Burst:	0	KBytes

Wireless Traffic Shapping

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

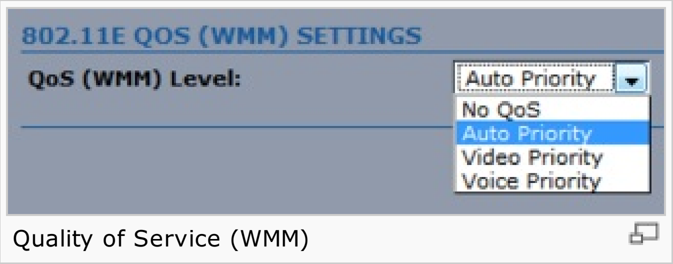
Incoming Traffic Limit: specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from wireless interface to Ethernet interface.

Incoming Traffic Burst: specify the data volume (in kilobytes) to which *Incoming Traffic Limit* will not be effective afterwards data connection is initiated.

Outgoing Traffic Limit: specify the maximum bandwidth value (in kilobits per second, Kbps) for traffic passing from Ethernet interface to wireless interface.

'*Outgoing Traffic Burst**: specify the data volume (in kilobytes) to which** Outgoing Traffic Limit* will not be effective afterwards data connection is initiated.

QoS



802.11E QOS (WMM) SETTINGS

QoS (WMM) Level: Auto Priority

Quality of Service (WMM)

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 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.

Auto Priority – priority of traffic is assigned automatically according to the type of the passing through data.

Voice Priority – enable priority of the voice traffic for all the passing through data.

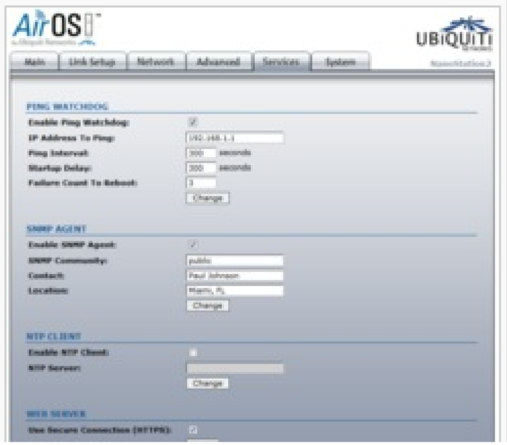
Video Priority – enable priority of the video traffic for all the passing through data.

[Content]

Services

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

Ping WatchDog



PING WATCHDOG

Enable Ping Watchdog: ☑

IP Address To Ping: 192.168.1.1

Ping Interval: 300 seconds

Startup Delay: 300 seconds

Failure Count To Reboot: 3

Change

SNMP AGENT

Enable SNMP Agent: ☑

SNMP Community: public

Contact: Paul Johnson

Location: Miami, FL

Change

NTP CLIENT

Enable NTP Client: □

NTP Server:

Change

WEB SERVER

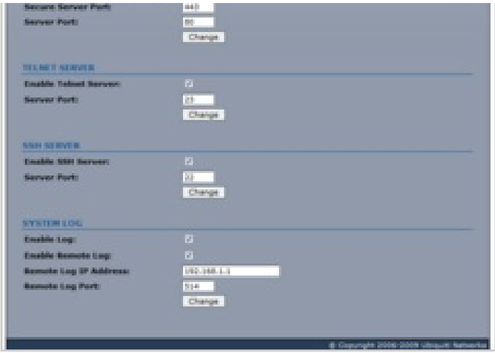
Use Secure Connection (HTTPS): ☑

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



Secure Server Port: 443
Server Port: 80
Change

TELNET SERVER
Enable Telnet Server: ☑
Server Port: 23
Change

SSH SERVER
Enable SSH Server: ☑
Server Port: 22
Change

SYSTEM LOG
Enable Log: ☑
Enable Remote Log: ☑
Remote Log IP Address: 192.168.1.1
Remote Log Port: 514
Change

© Copyright 2006-2009 Ubiquiti Networks

Services Page

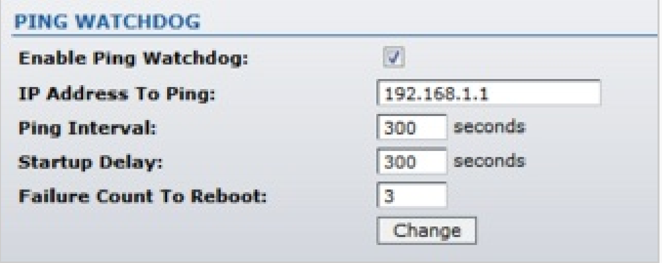
Watchdog Tool.

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.



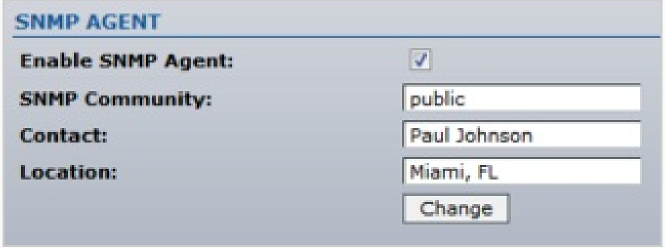
PING WATCHDOG
Enable Ping Watchdog: ☑
IP Address To Ping: 192.168.1.1
Ping Interval: 300 seconds
Startup Delay: 300 seconds
Failure Count To Reboot: 3
Change

Ping Watchdog

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:



SNMP AGENT
Enable SNMP Agent: ☑
SNMP Community: public
Contact: Paul Johnson
Location: Miami, FL
Change

SNMP Agent

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. AirOS supports SNMP v1.

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.

MIB list is provided in SNMP support section of Ubiquiti Wiki.

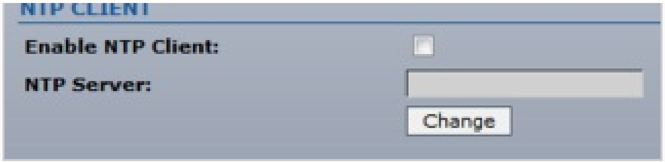
NTP Client

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 system time. *System Time* is reported next to the every *System Log* entry while registering system events if *Log* option is enabled.

Enable NTP Client: control will enable NTP client.

NTP Server: specify the IP address or domain name of the NTP Server.



NTP CLIENT

Enable NTP Client: □

NTP Server:

NTP Client

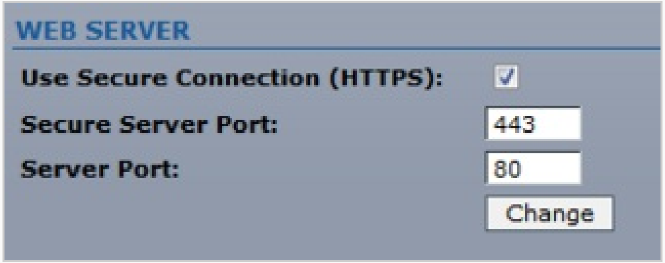
Web Server

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. HTTPS mode is unchecked 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..



WEB SERVER

Use Secure Connection (HTTPS): ☑

Secure Server Port: 443

Server Port: 80

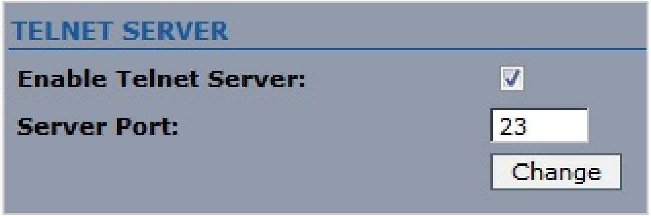
Web Server using HTTPS

Telnet Server

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

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

Server Port: Telnet service TCP/IP port setting.



TELNET SERVER

Enable Telnet Server: ☑

Server Port: 23

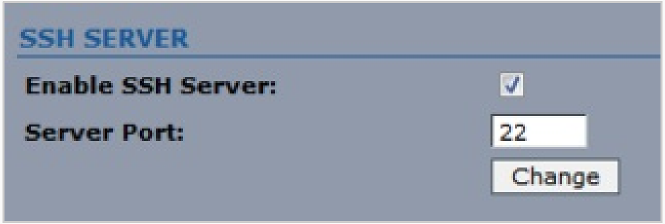
Telnet Server

SSH Server

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

Enable SSH Server: This option enables SSH access to the AirOS Device.

Server Port: SSH service TCP/IP port setting.



SSH SERVER

Enable SSH Server: ☑

Server Port: 22

SSH Server

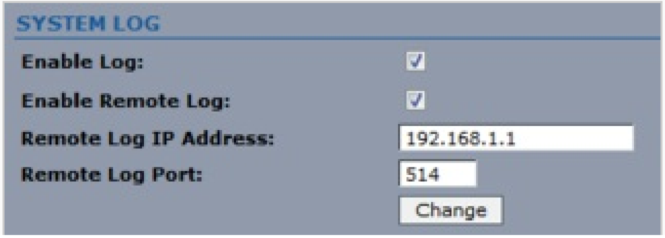
System Log

Enable Log : This option enables the registration routine of the *system log* messages.

Enable Remote Log: enables the syslog remote sending function while *System log* messages are sent to a remote server specified by the *Remote Log IP Address* and *Remote Log Port*.

Remote Log IP Address is the host IP address where syslog messages should be sent. Remote host should be configured properly to receive syslog protocol messages.

Remote Log Port: is the TCP/IP port of the host syslog messages should be sent. "514" is the default port for the commonly used system message logging utilities.



SYSTEM LOG

Enable Log: ☑

Enable Remote Log: ☑

Remote Log IP Address: 192.168.1.1

Remote Log Port: 514

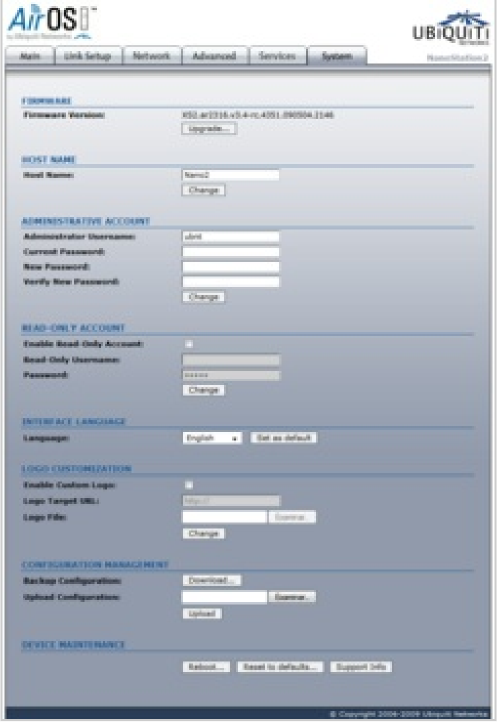
Every logged message contains at least a *System Time* and a Host Name. Usually a particular service name which generates the system event is specifies also within the message. Messages from different services have different context and different level of the details. Usually *error*, *warning* or *informational*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

System Log

[Content]

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.



FIRMWARE
Firmware Version: XS2.ar2316.v3.4-rc.4351.090504.2146

HOST NAME
Host Name: Nano2

ADMINISTRATIVE ACCOUNT
Administrator Username: ubnt
Current Password:
New Password:
Verify New Password:

READ-ONLY ACCOUNT
Enable Read-Only Account: □
Read-Only Username:
Password:

INTERFACE LANGUAGE
Language: English

LOGO CUSTOMIZATION
Enable Custom Logo: □
Logo Target URL: http://
Logo File:

CONFIGURATION MANAGEMENT
Backup Configuration:
Upload Configuration:

DEVICE MAINTENANCE

System Page

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. System configurations are preserved while the device is updated with a new firmware version.

Firmware version: displays the version of the current firmware of the AirOS system.

Upgrade: button opens the Firmware Upload window if activated.

Current Firmware: displays the version of the AirOS firmware which is currently operating.

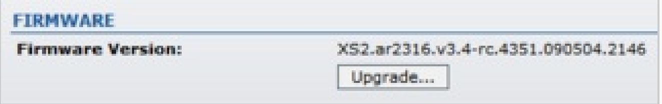
Firmware File: activate **Browse** button to navigate to and select the new firmware file. The full path to the new firmware file location can be specified there. New firmware file is transferred to the system after **Upload** button is activated.

Close this window – button cancels the new firmware upload process if activated.

Upgrade button should be activated in order to proceed with firmware upgrade routine (new firmware image should be uploaded into the system first). Please be patient, as the firmware upgrade routine can take 3-7 minutes. AirOS based device will be inaccessible until the firmware upgrade routine is completed.

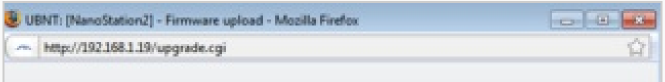
Do not switch off, do not reboot and do not disconnect the device from the power supply during the firmware upgrade process as these actions will damage the device!

It is highly recommended to backup the system configuration and the *Support Info* file before uploading the new configuration.



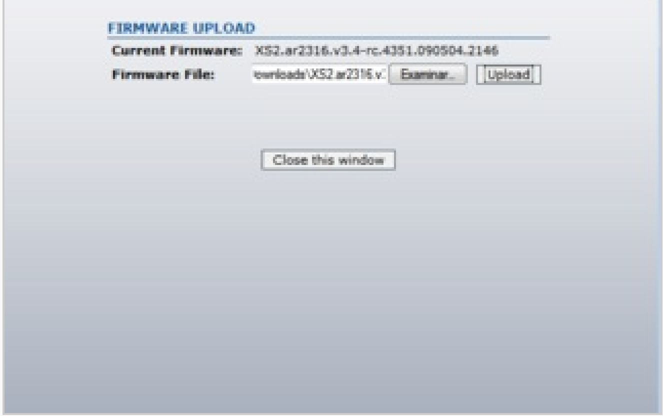
FIRMWARE
Firmware Version: XS2.ar2316.v3.4-rc.4351.090504.2146

Firmware section



UBNT: [NanoStation2] - Firmware upload - Mozilla Firefox
http://192.168.1.19/upgrade.cgi

Close this window – button closes the firmware upgrade window if activated. This action will not cancel the firmware upgrade process.



FIRMWARE UPLOAD

Current Firmware: XS2.ar2316.v3.4-rc.4351.090504.2146

Firmware File: ownloads\XS2.ar2316.v

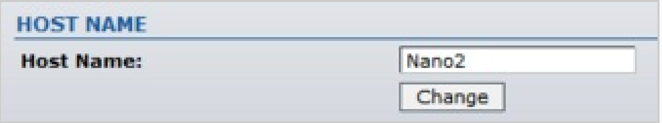
Firmware Upgrade

Host Name

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

Host Name: specifies the system identity.

Change button saves the *Host Name* if activated.



HOST NAME

Host Name: Nano2

Host Name

Administrative Account

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

Administrator Username: specifies the name of the system user.

Current Password: administrator is required to enter a current password. It is required for *Password* or *Administrator Username* change routine.

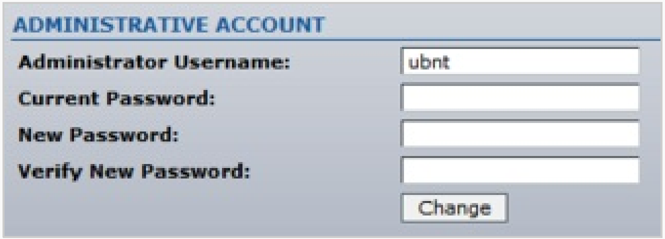
Default administrator login credentials:

* User Name: ubnt
* Password: ubnt

New Password: new password used for administrator authentication should be specified.

Verify Password: new password should be re-entered to verify its accuracy.

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



ADMINISTRATIVE ACCOUNT

Administrator Username: ubnt

Current Password:

New Password:

Verify New Password:

Administrative Account

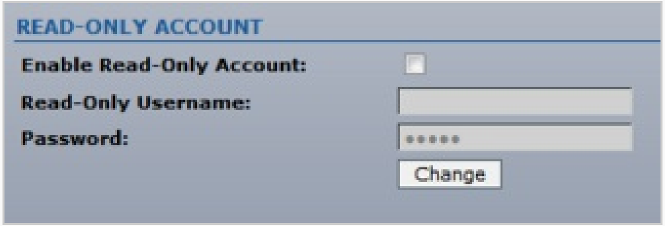
Read-only Account

In this section you can enable the read-only account, and configure the username and password to protect your device from unauthorized access. The default option is disabled.

Enable Read-Only Account: This option activates the read-only account.

Read-Only Username: specifies the name of the system user.

Password: new password used for read-only administrator authentication should be specified.



READ-ONLY ACCOUNT

Enable Read-Only Account: □

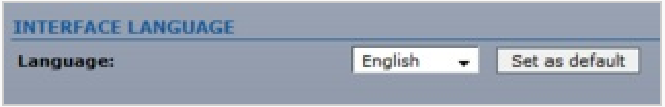
Read-Only Username:

Password: •••••

Read-only Account

Interface Language

AirOs supports multiple languages in the Web Management Interface.



Language: English

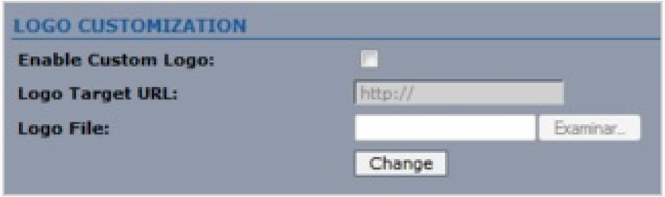
Interface Language, by default:English

Language options change the look and feel of the Web Management Interface while renaming the labels of all the configuration settings and controls according to the translation in particular language. The default language is English. The colors and the layout of all the web elements are not changed after the change of the language.

Language selection is saved by activating the **Set as default** button.

Additional language profiles may be uploaded. Please refer to this guide which describes how to import language profile used for translation of the user interface.

Logo Customization



Enable Custom Logo: □

Logo Target URL: http://

Logo File:

Logo Customization

Use the controls in this section to configure custom logo on the device web management interface. The logo must conform to these limitations:

* The volume size of the logo is 50 Kilobytes or less;

* 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. If the *Enable Custom Logo* option is not selected the default Ubiquiti logo will be set/restored and the custom logo will be removed.

Logo Target URL: the target URL of custom logo can be specified in this field. Target URL is opened when clicking on custom logo.

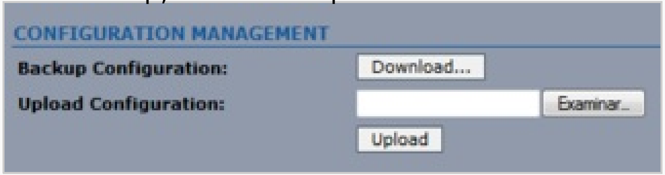
Logo File: ***activate*** *Browse'* button to navigate to and select the logo file. The full path to the logo file stored locally can be specified there. Logo file is transferred to the system after **Upload** button is activated.

If the logo file maximum volume size (50 kilobytes) is exceeded the system performance issues may occur. Default logo dimension (in pixels) is 114 (width) X 53(height).

Default Logo

Configuration Management

AirOS configuration is stored in plain text file. Use the *Configuration Management* section controls to backup, restore or update the system configuration file:



Configuration Management

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 to the configuration file location.

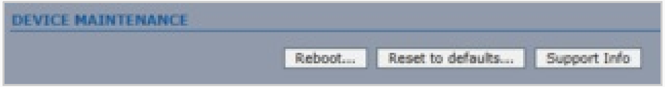
Activating the **Upload** button will transfer new configuration file to the system. The settings of the new configuration will be visible in the *Link Setup*, *Network*, *Advanced*, *Services* and *System* pages of the Web Management Interface.

New configuration will be effective after the *Apply* button is activated and system reboot cycle is completed. Previous system configuration is deleted after *Apply* button is activated. It is highly recommended to backup the system configuration before uploading the new configuration.

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

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



Device Maintenance

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

Reset to Defaults: activate *Reset to Defaults* control in order to initiate reset the device to factory defaults routine. Reset routine initiates system *Reboot* process (similar to the power off - power on cycle). The running system configuration will be deleted and the default system configuration (all the system settings with no exception) will be set.

After the *Reset to Defaults* routine is completed, AirOS system will return to the default IP configuration (192.168.1.20/255.255.255.0) and will start operating in *Station-Bridge* mode. It is highly recommended to backup the system configuration before the *Reset to Defaults* is initiated.

Support Info: activate *Support Info* button in order to get system information file. This file should be provided to Ubiquiti support engineers (upon the request) while investigating all the technical support or configuration issues if any.

[Content]