Navigation

- ▶ Main Page
- ▶ Community portal
- ▶ Current events
- ▶ Recent changes
- ▶ Random page
- ▶ Help

Search the Wiki

[　　　　　　　] **Go** 　Search

AirOS 5

User's Guide v5.0

Contents

AirOS v5 Introduction

AirOS v5.0 is the latest evolution in Ubiquiti's AirOS interface. It is advanced operating system capable of powerful wireless and routing features, built upon a simple, intuitive user interface foundation. AirOS v5.0 maximizes the wireless performance of Ubiquiti M Series products which are based on *IEEE 802.11n* (http://en.wikipedia.org/wiki/IEEE_802.11n) .

AirOS v5.0 Configuration Guide

This guide presents the detailed description of the AirOS operating system version 5.0 which is integrated into all M Series products provided by Ubiquiti Networks, Inc.

AirOS v5.0 supports the new M series product versions:

M2 (2.4GHz) products:

- Bullet M2 HP (http://ubnt.com/bulletm) ;
- Nano/Loco M2 (http://ubnt.com/nanostationm) ;
- Rocket M2 (http://ubnt.com/rocketm) ;

M5 (5GHz) products:

- Bullet M5 HP (http://ubnt.com/bulletm) ;
- Nano/Loco M5 (http://ubnt.com/nanostationm) ;
- Rocket M5 (http://ubnt.com/rocketm) ;

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

- Station (http://en.wikipedia.org/wiki/Station_(networking)) (Wireless Client);
- Station WDS (http://en.wikipedia.org/wiki/Wireless_Distribution_System) (Wireless Client Repeater);
- Access Point (http://en.wikipedia.org/wiki/Access_point) ;
- Access Point WDS (http://en.wikipedia.org/wiki/Wireless_Distribution_System) (Repeater).

All the AirOS based devices support the following network modes:

- Transparent Layer2 bridge (http://en.wikipedia.org/wiki/Transparent_bridge) ;
- Router (http://en.wikipedia.org/wiki/Router) .

AirOS Quick Setup Guide describes the configuration steps for the subscriber station (wireless client - bridge) use case (AirOS v3.4 based).

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 Bullet M5 graphical user interface which is consistent between all the AirOS v5.0 based devices.

[Content]
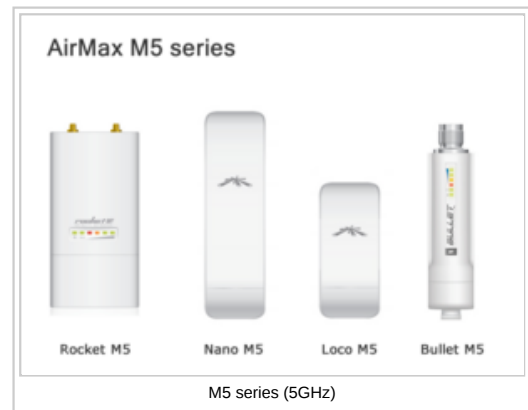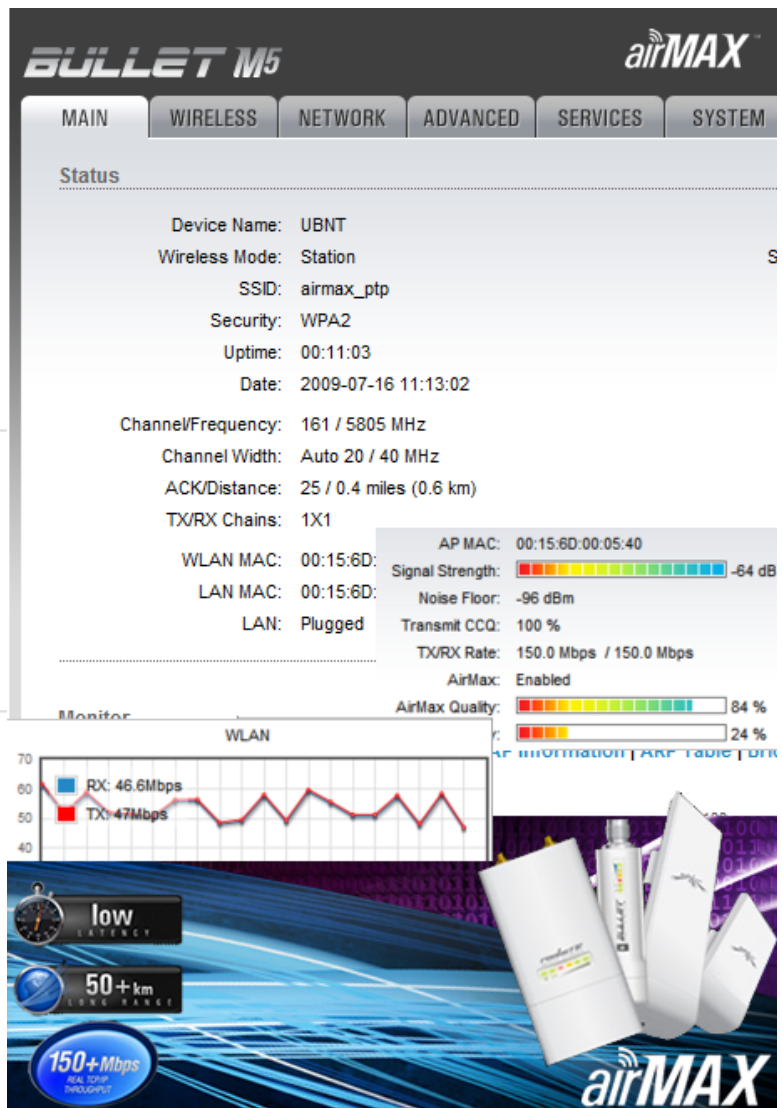
Navigation

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

[Main] page displays current status of the device and the statistical information.

[Wireless] 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 (http://en.wikipedia.org /wiki/Internet_Protocol) settings, packet (http://en.wikipedia.org /wiki/Packet_%28information_technology%29) filtering routines and network services (i.e. DHCP Server (http://en.wikipedia.org/wiki/DHCP)).

[Advanced] page settings are dedicated for more precise wireless interface control. AirMax feature and 802.11n specific parameters can be set in this page. Also advanced page includes external signal LED and traffic shaping settings.

[Services] page covers the configuration of system management services like SNMP (http://en.wikipedia.org/wiki/SNMP) , NTP (http://en.wikipedia.org/wiki/Network_Time_Protocol) , System Log, Ping Watchdog and SSH/Telnet server.

[System] page contains controls for system maintenance routines, dedicated for administrator account management, device customization, firmware upgrade and configuration backup. Web management interface language can be changed in this page also.

There are useful network administration and monitoring **[Tools]** available in every page also:

- ▶ Antenna alignment tool;
- ▶ Site survey tool (also available in AP (http://en.wikipedia.org/wiki/Access_point) mode);
- ▶ Ping (http://en.wikipedia.org/wiki/ping) ;
- ▶ Traceroute (http://en.wikipedia.org/wiki/traceroute) ;
- ▶ Speed test utility (not yet available);

[Content]

M2 series (2.4GHz)

Configuration Management Menu

Administration and monitoring tools

Main Page

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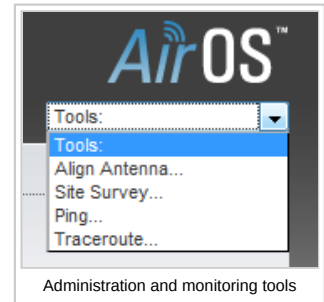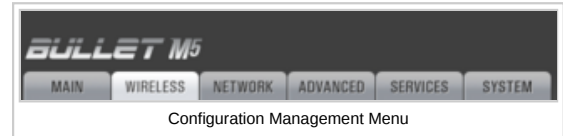
Status

Device Name: (http://en.wikipedia.org/wiki/Host_name) displays the customizable name (ID) of the AirOS v5.0 based device. Device Name (Host Name) will be represented in registration screens of the Router Operating Systems and discovery tools.

Wireless Mode: displays the radio interface operating mode. AirOS v5.0 powered device supports infrastructure wireless networking solution. Access Point (or Access Point WDS) and Station (or Station WDS) operating modes can be set depending on the network topology requirements.

SSID (http://en.wikipedia.org/wiki/BSSID#Basic_service_set_identifier) : is the Name of the 802.11 (http://en.wikipedia.org/wiki/802.11) Service Set (established by the Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) the stations are connected to):

> While operating in Station mode, displays the SSID (http://en.wikipedia.org /wiki/BSSID#Basic_service_set_identifier) of the Access Point (http://en.wikipedia.org /wiki/Wireless_access_point) where the AirOS v5.0 powered device has associated. While operating in Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) mode, displays the SSID (http://en.wikipedia.org/wiki/BSSID#Basic_service_set_identifier) of the

AirOS v5.0 Main Page
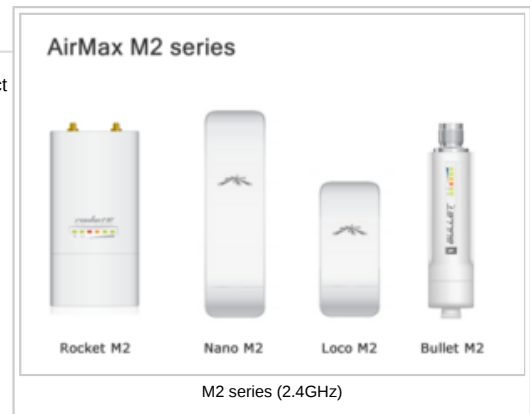
AirOS v5.0 powered device.

Current Status of the AirOS v5 powered Access Point

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

Device Name: UBNT
Wireless Mode: Access Point

Device Name and Wireless Mode

Uptime: This is the running total of time the device has been running since last power up (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 (http://en.wikipedia.org/wiki/Network_Time_Protocol) (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 supply for the internal clock.

Uptime: 00:58:22
Date: 2009-07-16 12:00:20

Total uptime and device date

Channel/Frequency: (http://en.wikipedia.org/wiki/Frequency) This is the operating frequency of the 802.11 (http://en.wikipedia.org/wiki/802.11) Service Set (hosted by AP) the client is connected to. 802.11 (http://en.wikipedia.org/wiki/802.11) Channel (http://en.wikipedia.org/wiki/Channel_%28communications%29) number corresponds to the operating frequency (http://en.wikipedia.org/wiki/Frequency) . More information about the supported channels is provided in the *Wireless* section. Device uses the radio frequency (http://en.wikipedia.org/wiki/Frequency) specified to transmit and receive data. For 5 GHz operation (M5 series), the common range of available frequencies (channels) is 5.1-5.9GHz, for 2.4 GHz operation (M2 series) - 2412-2472MHz. Valid frequency range (channels) will vary depending on local country regulations. For more information regarding frequency support please visit the compliance section (http://wiki.ubnt.com/wiki/index.php/RF_Compliance) of the Ubiquiti Wiki.

Channel Width: This is spectral width of the radio channel used by AirOS v5 powered device. 5, 10, 20 and 40 MHz channel spectrum widths are supported. In Station (or Station WDS) 20/40MHz is the value by default.

Channel/Frequency: 37 / 5185 MHz
Channel Width: 20 MHz

Current channel and channel width

ACK Timeout (http://en.wikipedia.org/wiki/802.11#Frames) : displays the current timeout value for ACK frames. ACK Timeout can be set manually or self-adjusted automatically. The **ACK Timeout** (http://en.wikipedia.org/wiki/802.11#Frames) (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. When you are using 802.11n mode, it is recommended to set "Auto adjust" for ACK Timeout. More information is provided in the *Advanced* settings section.

TX/RX Chains: displays the number of independent spatial data streams AirOS v5 powered device is transmitting/receiving simultaneously within one spectral channel of bandwidth. This ability is specific for 802.11n (http://en.wikipedia.org/wiki/IEEE_802.11n) devices which rely on multiple-input multiple-output (MIMO) (http://en.wikipedia.org/wiki/Multiple-input_multiple-output) technology. Multiple chains increase data transfer performance significantly. **The number of chains Ubiquiti device uses is hardware specific**. Every TX/RX chain requires separate antenna. Bullet M series devices use 1 chain for transmitting/receiving (1x1). Nano/Loco M series and Rocket M series uses 2 chains for transmitting/receiving (2x2).

ACK/Distance: 25 / 0.4 miles (0.6 km)
TX/RX Chains: 1X1

ACK Timeout/Distance and TX/RX Chains

WLAN MAC: displays the MAC address (http://en.wikipedia.org/wiki/MAC_Address) of the AirOS v5.0 device WLAN (http://en.wikipedia.org/wiki/Wireless_LAN) (Wireless) interface.

LAN MAC: displays the MAC address (http://en.wikipedia.org/wiki/MAC_Address) of the AirOS v5.0 device LAN (http://en.wikipedia.org/wiki/Lan) (Ethernet (http://en.wikipedia.org/wiki/Ethernet)) interface.

WLAN MAC: 00:15:6D:00:05:40
LAN MAC: 00:AA:BB:CC:DD:EE

LAN and WLAN MAC

LAN: indicates the current status of the Ethernet (http://en.wikipedia.org/wiki/Ethernet) port connection. This can alert system operator-technician that LAN (http://en.wikipedia.org/wiki/LAN) cable is not plugged into device and there is no active Ethernet (http://en.wikipedia.org/wiki/Ethernet) connection.

LAN: Plugged

Current Status of LAN Cable

AP MAC: displays the MAC address (http://en.wikipedia.org/wiki/MAC_Address) of the Access Point (http://en.wikipedia.org/wiki/Wireless_access_point) where the device has associated while operating in Station mode (or Station WDS). It is the MAC address of the AirOS v5.0 powered device's wireless interface itself if operating in Access Point mode. AP MAC is used as Basic Service Set Identifier (BSSID) (http://en.wikipedia.org/wiki/BSSID) in infrastructure type wireless networks.

MAC (http://en.wikipedia.org/wiki/Media_Access_Control) is unique HW (http://en.wikipedia.org/wiki/Hardware) identifier on each 802.11 (http://en.wikipedia.org/wiki/802.11) radio. It consists of two parts:

Signal Strength: -64 dBm
Noise Floor: -96 dBm
Transmit CCQ: 100 %
TX/RX Rate: 150.0 Mbps / 150.0 Mbps

Status information available in AirOS powered Station

An Organizationally Unique Identifier (OUI (http://en.wikipedia.org/wiki/Organizationally_Unique_Identifier))
Network Interface Controller (NIC (http://en.wikipedia.org/wiki/Network_Interface_Controller)) sequence.

The manufacturer list of a given MAC address (http://en.wikipedia.org/wiki/MAC_Address) is provided in this (http://standards.ieee.org/regauth/oui/index.shtml) page.

Signal Strength: (http://en.wikipedia.org/wiki/Signal_strength) displays the received wireless (http://en.wikipedia.org/wiki/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 (http://en.wikipedia.org/wiki/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 –80dBm or better (-50..-70) is recommended for stable links.

Connections: displays the number of associated wireless stations while the device is operating in Access Point mode. This value is not displayed while operating in Station mode.

AP MAC address and Connections (wireless stations associated)

Noise Floor: displays the current value of the noise (http://en.wikipedia.org/wiki/Electronic_noise) level in dBm. Noise Floor (http://en.wikipedia.org/wiki/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.

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

TX Rate and RX Rate: displays the current 802.11 (http://en.wikipedia.org/wiki/802.11) data transmission (TX) and data reception (RX) rate while operating in *Station* mode. Data rates up to 150 Mbps on 1 chain devices (Bullet M series) and up to 300 Mbps on 2 chain devices (NanoStation/LocoStation M and Rocket M series) can be used. Highest data rates will provide maximum data throughput while signal level is relevant.

Noise Floor and Transmit CCQ

Airmax: Indicates the current status of the AirMax (Ubiquiti's propietary TDMA polling technology) in the device while operating in AP or AP WDS mode. If AirMax is enabled, the device only accepts AirMax stations. (Disable AirMax for legacy 802.11abg devices compatibility). AirMax also features some advanced QOS AutoDetection settings.

Airmax quality: This is an index which evaluates the AirMax Connection Quality. The level is based on a percentage value where 100% corresponds to a perfect link state.

Airmax status, Airmax quality and capacity

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

[Content]

Monitor

Throughput: show graphs 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 *Refresh* button.

Stations: this selection lists the stations which are connected to the device while operating in Access Point mode (or Access Point WDS).

> 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;
> **Noise (dBm)** value displays the value of the noise level wireless signal was received;
> **Tx Rate (Mbps)** value represents the data rates, in Mbps, of the last transmitted packets;
> **Rx Rate (Mbps)** value represents the data rates, in Mbps, of the last received packets;
> **Idle (sec)** value represents the time (in seconds) since last packet was received from the particular station.
> The information in the station statistics window can be updated using the *Refresh* button.
> Detailed information can be retrieved while selecting the particular *MAC* of the associated station:

Throughput graphs and statistics

Status Reporting in AP mode

>> **Connection time** 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, in dBm, the last received wireless signal level;
>> **Noise Floor**: displays the current value of the noise (http://en.wikipedia.org/wiki/Electronic_noise) level in dBm. Noise Floor (http://en.wikipedia.org /wiki/Noise_floor) is taken into account while evaluating the signal quality (Signal-to-Noise Ratio SNR, RSSI) while value mean depends on signal strength above the noise floor.
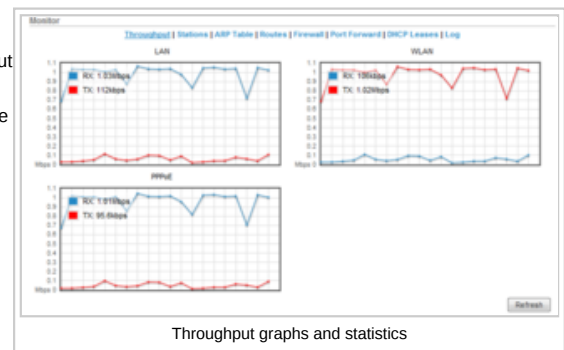>> **CCQ** value represents the quality of the connection to the Station;
>> **Tx/Rx Rate** represents the data rates, in Mbps, of the last transmitted and received packets;
>> **Tx/Rx Packets** value represents the total amount of packets transmitted to and received from the Station during the connection uptime;
>> **Tx/Rx Packet Rate** (packets per second or pps) represents the mean value of the transmitted and received packet rate;
>> **Bytes transmitted** value represents the total amount of data (in bytes) transmitted during the connection;

Bytes received value represents the total amount of data (in bytes) received during the connection;

Negotiated Rate/Last Signal (dBm) table 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. The information in the station statistics window can be updated using the *Refresh* button. Window can be closed with the **Close this window** button.

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

Station info

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;
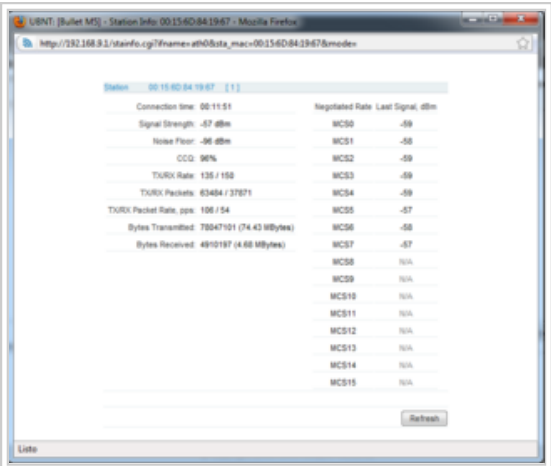
Bytes transmitted/received value represents the total amount of data (in bytes) transmitted and received during the connection;

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.

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 **Refresh** 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.

ARP table

Bridge: 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 **Refresh** 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).
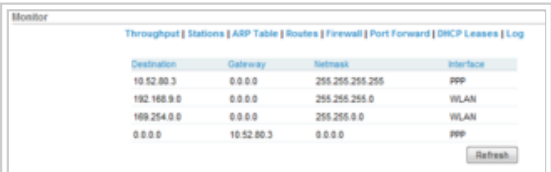
Ageing timer shows ageing time for each address entry (in seconds) - after particular time out, not having seen a packet coming from a certain address, the bridge will delete that address from the Bridge Table.

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 **Refresh** 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 *Wireless* section.

Monitor - Routes

Firewall: selection lists active firewall entries in the *FIREWALL chain* of the standard ebtables (http://ebtables.sourceforge.net/ebtables-man.html) *filter table*, while the device is operating in *Bridge* mode.

The list can be updated using the '*Refresh* button.
Active firewall entries in the *FIREWALL chain* of the standard iptables (http://security.maruhn.com/iptables-manual.html) *filter table* are listed if the device is operating in *Router* mode.

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

IP and MAC level access control and packet filtering in AirOS is implemented using iptables (http://security.maruhn.com/iptables-manual.html) (routing) and ebtables (http://ebtables.sourceforge.net/ebtables-man.html) (bridging) firewall which protects the resources of a private network from outside threats by preventing unauthorized access and filtering specified types of network communication.

Monitor - Firewall

More information is provided in the *Wireless* section.

Port Forward: selection lists active port forward entries in the *PORTFORWARD chain* of the standard iptables (http://security.maruhn.com/iptables-manual.html) *nat table*, while the device is operating in *Router* mode.

Monitor - Port forwarding

The list can be updated using the **Refresh** 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.

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.

DHCP leases

MAC address shows the client's MAC address, which is connected to the Access Point.
IP address shows the client's IP address leased by the device's DHCP server.
Remaining Lease time shows for how long the leased *IP address* will be valid and reserved for particular DHCP client.
Interface name shows from which device interface DHCP client which has specified *MAC Address* is connected.

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

More information is provided in the *Wireless* section.

Log selection shows a lists with 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 **Refresh** button is activated.

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.

[Content]

Wireless Page

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

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 Page – Bullet M5

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 v5.0 software:

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

2. **Station WDS**: WDS stands for Wireless Distribution System. Station WDS should be used while connecting to the Access Point which is operating in WDS mode. This mode is compatible with WPA/WPA2 encryption.
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 (http://en.wikipedia.org/wiki/Access_point)

4. **Access Point WDS**: This is an 802.11 Access Point (http://en.wikipedia.org/wiki/Access_point) which allows for layer 2 bridging with Station WDS devices using the WDS protocol. AP WDS is not fully compatible with WPA/WPA2 encryption.
WDS allows you to bridge wireless traffic between devices which are operating in *Access Point* mode. Access Point is usually connected to a wired network
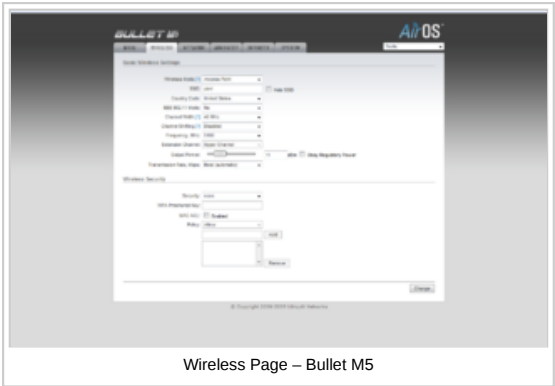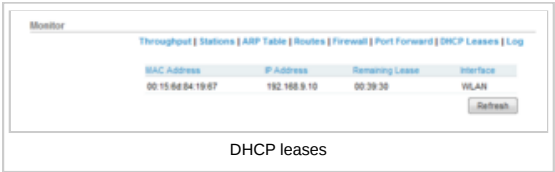
(Ethernet LAN) allowing wireless connection to the wired network. By connecting Access Points to one another in an Extended Service Set using the WDS, distant Ethernets can be bridged into a single LAN.

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

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

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

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

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

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

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

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.

ESSID: – specify the ESSID of the Access Point which the AirOS v5.0 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.

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

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 (http://wiki.ubnt.com/wiki/index.php /RF_Compliance) for further explanation of international compliance requirements.

IEEE 802.11 Mode: This is the radio standard used for operation of your AirOS powered device. 802.11b, 802.11a and 802.11g are old 2.4GHz mode while the 802.11n (2.4GHz and/or 5GHz) is newer standards based on faster Orthogonal Frequency Division Multiplexing (OFDM) modulation. For more information, please consult 802.11 compliance guide (http://wiki.ubnt.com/wiki/index.php/RF_Compliance) .
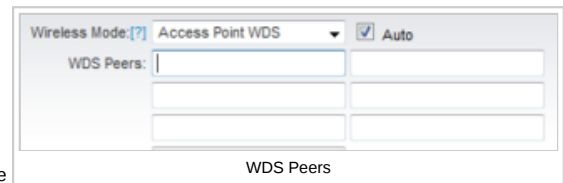

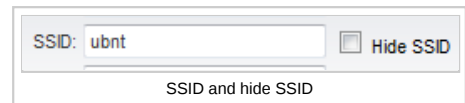Wireless Page – Station WDS Bullet M5
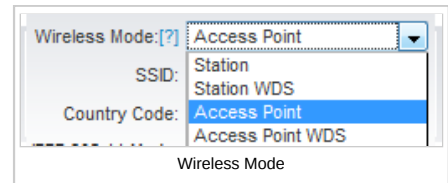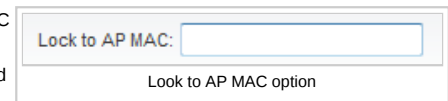

Wireless Mode
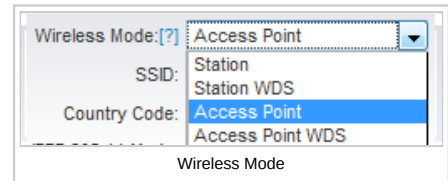
Wireless Mode

WDS Peers

SSID and hide SSID

ESSID and Site Survey (Select) tool

Look to AP MAC option

IEEE 802.11 mode and Country Code selection on Bullet

▶ Bullet M2, Rocket M2, Nano M2, Loco M2 supported IEEE 802.11 mode:

B/G/N – connect to an 802.11b, 802.11g or 802.11n network (selected by default). This mode offers better compatibility.

▶ Bullet M5, Rocket M5, Nano M5, Loco M5 supported IEEE 802.11 mode:

A/N – connect to an 802.11a or 802.11n network (selected by default). This mode offers better compatibility.

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

Select the Channel Spectrum Width

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 – is the channel spectrum with the width of 40 MHz.
20MHz/40MHz – only available in Station (or Station WDS) mode. It offers better compatibility.

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/n and 802.11a channels. This is a proprietary Ubiquiti developed feature. While 802.11 networks have standard channels such as Channel 36 (5180MHz), Channel 40 (5200MHz), 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 802.11na) or 2/3 MHz (in 802.11bgn) from the default central channel frequency.

Enable or disable Channel Shifting

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.

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

Extension Channel: (Only applicable for AP or AP WDS, and 40MHz channel width) indicates the use of channel bonding that allows the AirMax network to use two channels at once. Using two channels improves the performance of the Wi-Fi connection. It is automatically selected by the system.

Channel Scan List, MHz: 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.

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.

Select a Wireless Frequency on Bullet M5

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 v5.0 based device has an internal antenna (i.e. NanoStation M/LocoStation M), Output Power is the output power delivered to the internal antenna.

Extension Channel

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/n regulatory domain thus country). For more regulatory information please consult 802.11 compliance guide (http://wiki.ubnt.com/wiki/index.php/RF_Compliance) .

Data Rate: This defines the data rate (in Mbps) at which the device should transmit wireless packets. If the **Best (automatic)** option is selected, then the *rate algorithm* will select the best data rate depending on the link quality conditions. You can fix a specific data rate between MCS 0 and MCS 7 (or MCS15 for 2x2 chains devices) also. Use *Best (automatic)* 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 20MHz Channel Spectrum width the maximum data rate is MCS7 (65Mbps) or MCS15 (150Mbps). If you select 40MHz Channel Spectrum width the maximum data rate is MCS7 (150Mbps) or MCS15 (300Mbps).

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

[Content]

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 v5.0 supports none, WPA, and WPA2 security options. **The current AirOS v5.0 firmware doesn't support WEP security**. Select the security mode of your wireless network:

WPA - AES – enable WPA™ security mode with AES support only. Wi-Fi Protected Access - WPA™ (IEEE 802.11i/D3.0) 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.

WPA2 - AES – enable WPA2™ security mode with AES support only. Wi-Fi Protected Access 2 - 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:

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

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 v5.0 Web Management GUI supports only EAP-TTLS authentication method. (Applicable for *Station* and *Station WDS* modes only).

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.

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** checkbox.

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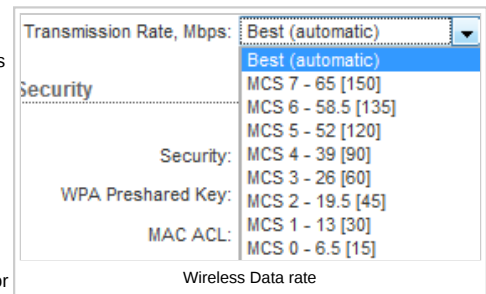
The MAC addresses of the wireless clients can be added and removed to the list using the **Add** and **Remove** buttons.
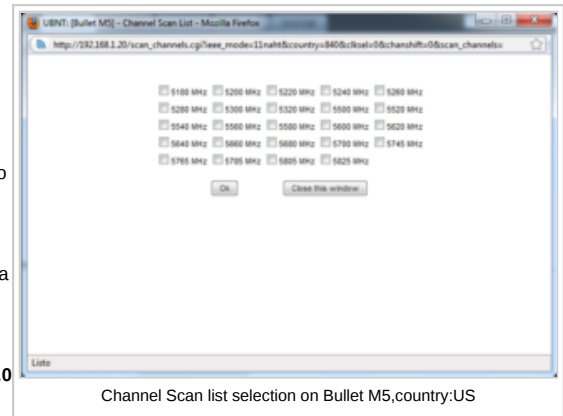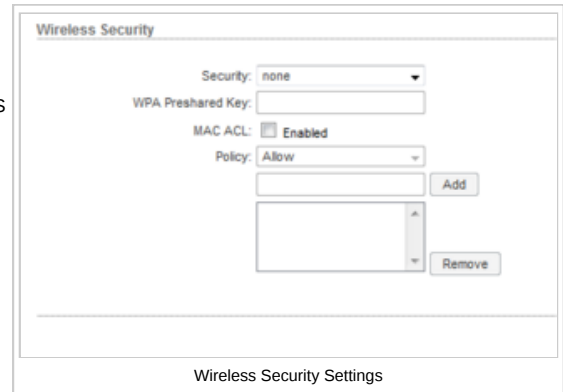

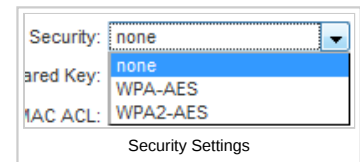Channel Scan list selection on Bullet M5,country:US
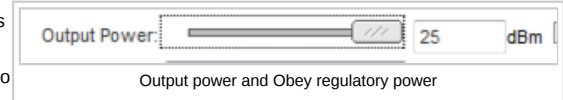
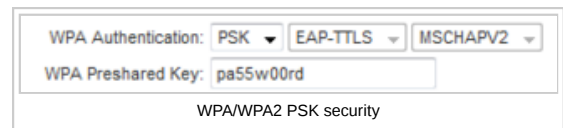
Output power and Obey regulatory power
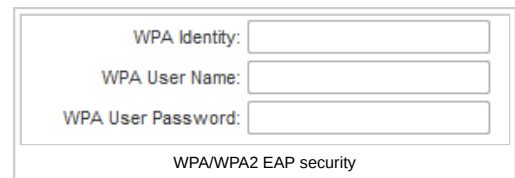

Wireless Data rate

Wireless Security Settings

Security Settings

WPA/WPA2 PSK security

WPA/WPA2 EAP security

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

MAC Address Control List

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

AirOS v5.0 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.

AirOS v5.0 Network Page

> **[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 v5.0 supports Multicast packet pass-through in **Router** mode.

> AirOS v5.0 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.

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

Network settings

Bridge Mode

In bridge mode the AirOS v5.0 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:

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 v5.0 device management purposes.

IP Address and *Netmask* settings should consist with the address space of the network segment where AirOS v5.0 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.

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 (http://en.wikipedia.org/wiki/Link-local_address) 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).

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.

Bridge IP Address assigned manually (Static)

> **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.

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.

IP Aliases

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 v5.0 device will direct the packets of data to the gateway if the destination host is not within the local network.

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

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

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

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

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

In case the IP settings of the AirOS v5.0 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 v5.0 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.

Bridge IP Address assigned automatically DHCP with IP fallback

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

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 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.

Bridge mode Firewall Configuration Settings

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 ebtables filter table, while the device is operating in Bridge mode. Please refer to the ebtables manual (http://ebtables.sourceforge.net/ebtables-man.html) 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:

Network - 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.

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 v5.0 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 (http://en.wikipedia.org/wiki/Link-local_address) 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).
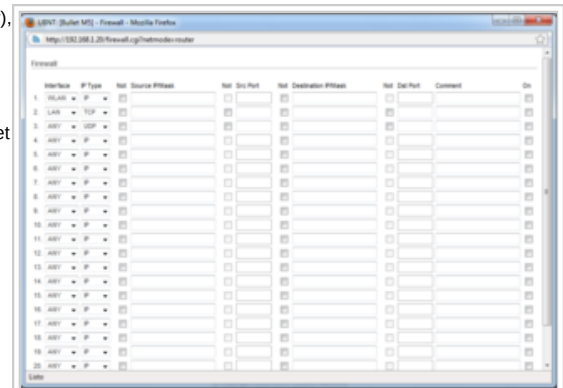
Netmask: This is used to define the device IP classification for the chosen IP address range. 255.255.255.0 is a typical netmask value for Class C networks, which support IP address range 192.0.0.x to 223.255.255.x. Class C network *Netmask* uses 24 bits to identify the network (alternative notation "/24") and 8 bits to identity the host.

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.

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 (http://iptables-tutorial.frozentux.net/iptables-tutorial.html#MASQUERADETARGET) for detailed description of the NAT functionality in *Router* mode.

IP Aliases

Static routes should be specified in order the packets should pass-through the AirOs v5.0 based device if the *NAT* is disabled in while operating in *Router* network mode.

Enable NAT and DHCP Server

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.

DHCP Server range, Netmask 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. The time is expressed in seconds.

Enable DNS Proxy: The DNS Proxy forwards the Domain Name System requests from the hosts which reside in the internal network to the DNS server while 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.

DNS Proxy and Port Forwarding settings

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 v5.0 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.
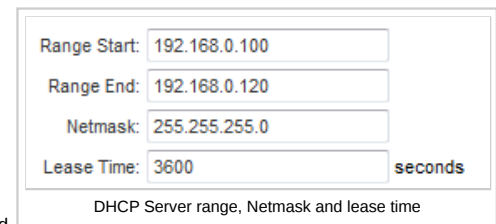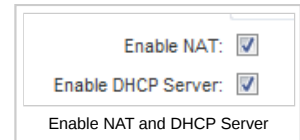
Newly added port forwarding entries can be saved by activating **Save** button or discarded by activating **Cancel** button in the *Port Forwarding* configuration window.
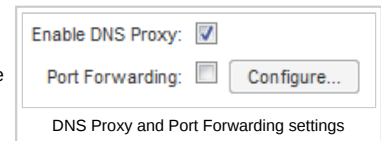
LAN Network Settings

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
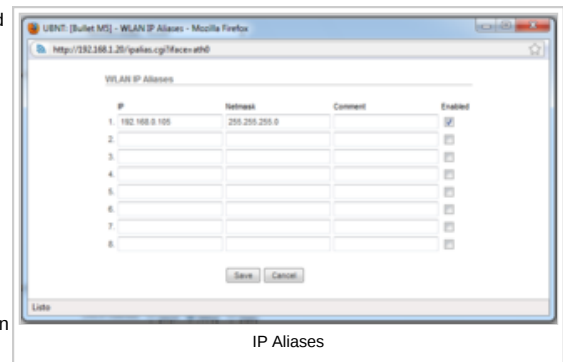
operation mode described above. This is the IP address can be used for the routing and the device management purposes.

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. (Applicable for Static mode only)

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

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. (Applicable for Static mode only)

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). (Applicable for Static mode only)

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 v5.0 powered device. (Applicable for Static mode only)

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.

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);
> **PPPoE 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 (http://en.wikipedia.org/wiki/Maximum_transmission_unit)) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP (http://tools.ietf.org/html/rfc1661) tunnel; (MTU/MRU default value: 1492)
> **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.

Port Forwarding example

LAN IP Address assigned manually - Static

PPPoE Internet connection (usually used by ADSL providers)

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 v5.0 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.

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.

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 v5.0 system will return to the default IP configuration (192.168.1.20/255.255.255.0) if the *Reset to defaults* routine is initiated (more information in System section).

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.

LAN IP Address assigned via DHCP with IP fallback

Enable Multicast 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) (http://en.wikipedia.org /wiki/Internet_Group_Management_Protocol) .

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.

Multicast routing enabled

Firewall entries can be specified by using the following criteria:

Interface the interface (WLAN, LAN or PPP) where filtering of the incoming/passing-through packets is processed;

IP Type sets which particular L3 protocol type (IP, ICMP, TCP, UDP, P2P) should be filtered;

Source IP/mask 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.

Firewall Configuration Settings

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 (http://iptables-tutorial.frozentux.net/iptables-tutorial.html) 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 802.11n data rates include MCS0, MCS1, MCS2, MCS3, MCS4, MCS5, MCS6, MCS7 for 1x1 chain devices and MCS8, MCS9, MCS10, MCS11, MCS12, MCS13, MCS, MCS15 for 2x2 chains devices. The ACK timeout has a critical impact on performance in 802.11n outdoor links.

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

Advanced Wireless Settings in Bullet M5 (AP mode)

RTS/CTS (Request to Send / Clear to Send) are 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 0-2346 bytes. If the packet size the node wants to transmit is larger than the threshold, the RTS/CTS handshake gets triggered. If the packet size is equal to or less than threshold the data frame gets sent immediately.

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.

RTS and Fragmentation Threshold

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 v5.0 has a new auto-acknowledgement timeout algorithm which dynamically optimizes the frame acknowledgement timeout value without user intervention. This is a critical feature required for stabilizing long-distance 802.11n outdoor links. The user also has the ability to enter the value manually, but it's not recommended.

Distance: specify the distance value in miles (or kilometers) using 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 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 (used in AirOS v3.4). It is very recommended to use *Auto Adjust* option for 802.11n.

If two or more stations are located at the considerably different distance from the Access Point are associated to, the highest *ACK Timeout* for the farthest station should be set at the AP side. AirOS v5.0 includes an improved ACK Timeout algorithm.

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

Enable Aggregation

    Frames – determines the number of frames combined on the new larger frame.

    Bytes – determines the size (in Bytes) of the larger frame.

AirMax: AirMax is the Ubiquiti's propietary TDMA polling technology (Applicable only for AP or AP WDS mode). If AirMax is enabled, the device only accepts AirMax stations. (Disable AirMax for legacy 802.11abg devices compatibility). AirMax also features some advanced QOS AutoDetection settings.

Enable AirMax and Multicast data

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

Enable Extra Reporting: feature will report additional information (i.e. 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 DFS: *DFS* is the part of the IEEE 802.11h wireless standard. *Enable DFS* option allows to enable/disable DFS support (applicable for M5 series 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 (http://wiki.ubnt.com/wiki/index.php/RF_Compliance) and official regulations authorities for further explanation of compliance requirements for the country where AirOS v5.0 based device is installed.

Enable DFS and Client Isolation

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.

Signal LED Thresholds

The LED's on the back of the AirOS v5.0 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).

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. The default value is -94dBm.
    LED 2 (Yellow) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -80dBm.
    LED 3 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -73dBm.
    LED 4 (Green) will switch on if the Signal Strength reaches the value set in an entry field next to it. The default value is -65dBm.

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**.

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.

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.

Wireless Traffic Shapping

    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.

[Content]

Services

This page covers the configuration of system management services SNMP, SSH, System Log and Ping Watchdog.

Ping WatchDog

The ping watchdog sets the AirOS v5.0 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.

Services Page

- **Enable Ping Watchdog**: control will enable Ping Watchdog Tool.
- **IP Address To Ping**: specify an IP address of the target host which will be monitored by Ping Watchdog Tool.
- **Ping Interval**: specify time interval (in seconds) between the ICMP "echo requests" are sent by the Ping Watchdog Tool. The default value is 300 seconds.
- **Startup Delay**: specify initial time delay (in seconds) until first ICMP "echo requests" are sent by the Ping Watchdog Tool. The default value is 300 seconds.
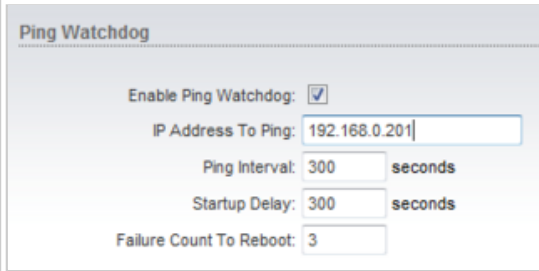
The value of Startup Delay should be at least 60 seconds as the network interface and wireless connection initialization takes considerable amount of time if the device is rebooted.

Ping Watchdog

- **Failure Count to Reboot**: specify the number of ICMP "echo response" replies. If the specified number of ICMP "echo response" packets is not received continuously, the Ping Watchdog Tool will reboot the device. The default value is 3.

SNMP Agent

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. AirOS contains an SNMP agent which allows it to communicate to SNMP manage applications for network provisioning.
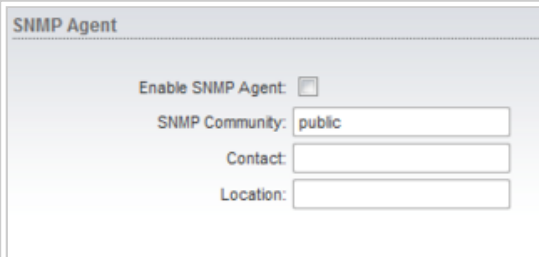
SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol (an application layer protocol that facilitates the exchange of management information between network devices). SNMP Agent allows network administrators to monitor network performance, find and solve 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**: 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. The default SNMP Community is *"public"*.
- **Contact**: specify the identity or the contact who should be contacted in case a emergency situation arise.
- **Location**: specify the physical location of the device.

NTP Client

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.

NTP Client

- **Enable NTP Client**: control will enable NTP client.
- **NTP Server**: specify the IP address or domain name of the NTP Server.

Web Server

Web Server: the following AirOS v5.0 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..

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.

SSH Server

SSH (http://en.wikipedia.org/wiki/Secure_Shell) 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.

System Log

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

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

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.

[Content]

Web Server using HTTPS

Telnet Server

SSH Server

System Log

System

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

Device Name

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

Device Name: specifies the system identity.

Change button saves the *Device Name* if activated.

Interface Language

AirOS v5.0 supports multiple languages in the Web Management Interface.

System Page

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.

Device Name

Language selection is saved by activating the **Change** 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.

Interface Language, by default:English

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.

Administrative Account

Note: password length is 8 characters maximum, characters after the 8th position will be truncated.

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.

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

Read-only Account

Configuration Management

AirOS v5.0 configuration is stored in plain text file (cfg file). Use the *Configuration Management* section controls to backup, restore or update the system configuration file:

Backup Configuration: click **Download** button to download the current system configuration file.

Configuration Management

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 *Wireless*, *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 Bullet M2 (or M5), Rocket M2 (or M5), NanoStation M2 (or M5)! Behavior may be unpredictable when mixing configurations from different type devices. AirOS v3.4 backups are not compatible with AirOS v5.0

Device Maintenance

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

Firmware Version: shows the current firmware version.

Update

Device Maintenance

Firmware section

Use this section to 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 upload

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.

Update 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 v5.0 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.

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

Firmware Upload

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.

Reboot

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]

Tools

Align Antenna

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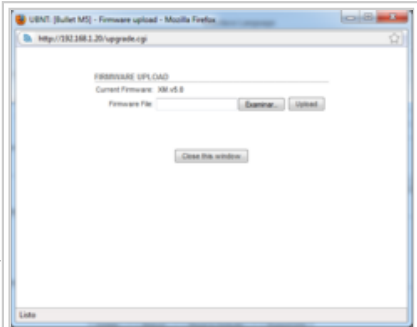

Reset to Defaults

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.
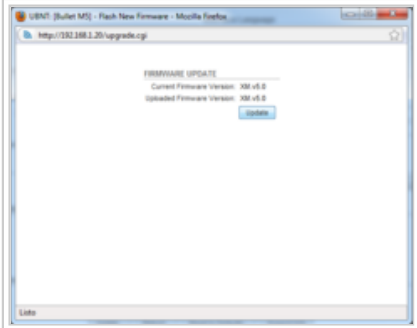
"Noise Level": value displays the value of the noise level wireless signal was received.

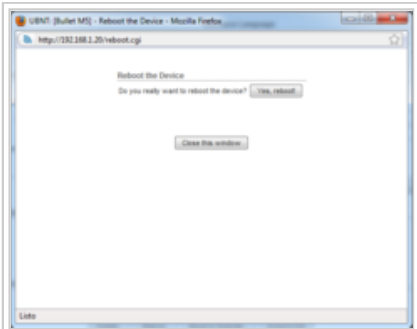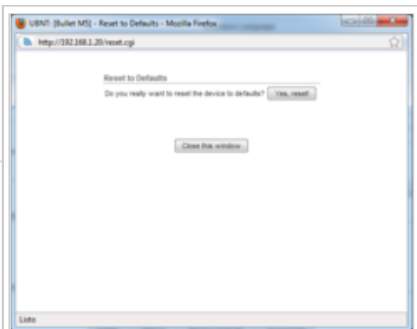*Align Antenna* window can be closed with the **Close this window button**.

Site Survey

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**.

Antenna alignment Tool

Ping

Ping (http://en.wikipedia.org/wiki/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.

Wireless Site Survey utility

Traceroute

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

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

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

Wireless link quality estimation with Network Ping utility

DHCP Client

DHCP Client: (Applicable for Router - DHCP mode only) shows WAN IP address, Netmask, DNS servers and Gateway of the device while operating in DHCP Router mode.

[Content]

Finding the route across the network with Traceroute utility

DHCP Client