PowerStation2
LiteStation2
LiteStation5

User's Guide

Contents

Introduction

This guide presents the description of the subscriber stations LiteStation2, LiteStation5 and the outdoor wireless station PowerStation2.

LiteStation2 and PowerStation2 operate in IEEE 802.11b/g modes, while the LiteStation5 operates in IEEE 802.11a mode. The devices can operate in Client (Station), Access Point and WDS modes. The screenshots in this manual are made for PowerStation2 but they are also applicable for LiteStaiton2 and LiteStaiton5.

Quick Setup Guide

This Quick Setup Guide will guide you through quick and easy configuration of the subscriber station (client bridge) including:

— Changing of the IP settings (static or dynamic),

— Defining the SSID to which the subscriber station will be associated,

— Defining the IEEE 802.11 mode,

— Defining the wireless security (None, WEP, WPA™ or WPA2™),

— Changing the administrator's password.

For detailed setup and configuration instructions, please refer to the chapter *Configuration Guide.*

Follow these steps for subscriber station quick setup via web-browser interface:

Step 1 Login to the web management

Open the web browser and type the default IP address of the PowerStation2/LiteStation2/LiteStation5 device **http://192.168.1.20/** into the browser address field. You will be prompted to enter the administrator login credentials:

User Name: **ubnt**

Password: **ubnt**

After successful administrator log on you will see the main page of the subscriber station web management interface.

Step 2 Configure network settings

The IP configuration as described below is required for PowerStation2/LiteStation2/LiteStation5 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:	Bridge ▾	
NETWORK SETTINGS		
Bridge IP Address:	○ DHCP ◉ Static	
IP Address:	192.168.1.20	
Netmask:	255.255.255.0	
Gateway IP:	192.168.1.1	
Primary DNS IP:	192.168.1.2	
	Change	

Network Mode: specify the *Bridge* operating mode (selected by default). Router operating mode configuration is described in the chapter *Configuration Guide.*

Bridge IP Address: specify the IP mode:

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

    Static – choose to assign a static IP address.

IP Address: enter IP address of the device.

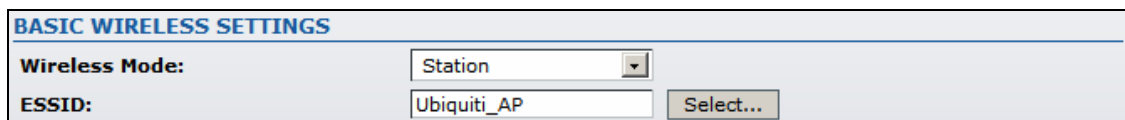**Netmask:** enter a subnet mask of the device.

Gateway IP: enter a Gateway IP address.

Primary DNS IP: enter a DNS IP address.

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

Step 3 Assign the SSID to subscriber station

Use **Link Setup** menu to specify the SSID of the wireless device (Access Point) to which the subscriber station will be associated:

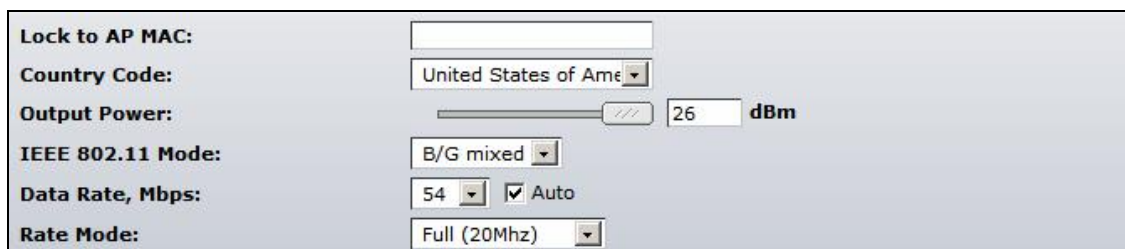| BASIC WIRELESS SETTINGS		
Wireless Mode:	Station ▾	
ESSID:	Ubiquiti_AP	Select...

Wireless Mode: specify the *Station* wireless mode (selected by default).

SSID: specify the SSID of the wireless network device which the PowerStation2/LiteStation2/LiteStation5 will associate to.

Refer to the section *Basic Wireless Settings* for detailed configuration information.

Step 4 Specify the IEEE 802.11 mode

Specify the 802.11 wireless network mode by which the subscriber station will communicate with the wireless device:

Lock to AP MAC:	
Country Code:	United States of Ame ▾
Output Power:	———▰ 26 **dBm**
IEEE 802.11 Mode:	B/G mixed ▾
Data Rate, Mbps:	54 ▾ ☑ Auto
Rate Mode:	Full (20Mhz) ▾

IEEE 802.11 Mode: select the IEEE 802.11 mode of your wireless network.

    PowerStation2/LiteStation2 supported IEEE 802.11 modes:

        B only – connect to a 802.11b only network.

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

        G only – connect to a 802.11g only network.

    LiteStation5 supported IEEE 802.11 modes:

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

A (Dynamic Turbo) – connect to a 802.11a network which supports Dynamic Turbo feature.

A (Static Turbo) – connect to a 802.11a network which supports Static Turbo feature.

Step 5 Specify the security mode

Choose the security method to protect your data that only authorized network users could access the network. You can choose **WEP**, **WPA, WPA2** or **None** security methods for your device.

If no security method will be used, choose the **None** option (selected by default):

WIRELESS SECURITY

Security:	none ▾
Authentication Type:	⦿ Open ○ Shared Key
WEP Key Length:	64 bit ▾ **Key Type:** HEX ▾
WEP Key:	[ ] **Key Index:** 1 ▾
WPA Preshared Key:	[ ]

Change

Security: select the security mode of your wireless network.

None – disable security.

WEP – enable WEP encryption.

WPA – enable WPA™[i] with Pre-shared Key encryption.

WPA2 – enable WPA2™ with Pre-shared Key encryption.

Authentication Type: choose the one of the following authentication modes for WEP security method:

Open Authentication – station is authenticated automatically (more secure method).

Shared Authentication – station is authenticated after the challenge, generated by AP (less secure method).

WEP Key Length: select the WEP Key length here, either 64-bit, or 128-bit.

Key Type: use the **HEX** or **ASCII** option to specify the character format for the WEP key.

WEP Key: enter the WEP encryption key to be used to encrypt and decrypt wireless traffic:

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

For **128-bits** – specify pre-shared key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.
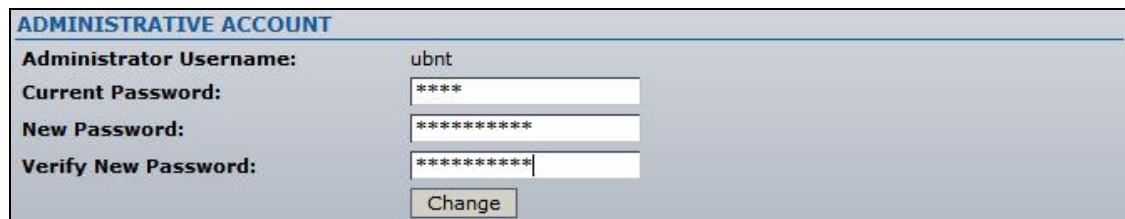
Key Index: specify the Index of the WEP Key used.

WPA Pre-shared Key: enter a passphrase for WPA™ or WPA2™ encryption. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

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

Step 6 Change administrator password

For the security reasons the default administrator's password should be changed immediately. Use the **System** menu and specify the parameters:

Current Password: enter a current password value. Default administrators password is **ubnt**.(Default username is also ubnt)

New Password: enter a new password value used for administrator authentication.
Verify Password: re-enter the new password to verify its accuracy.

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

Step7 Apply changes

After each configuration change the informational message suggesting you to apply changes and reboot the device will appear:
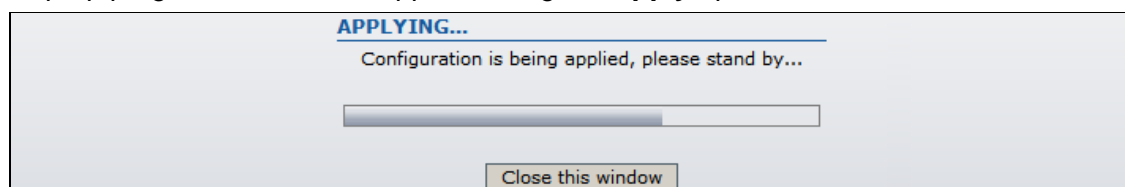

Click **Apply** button to apply the changes and reboot the device.

Click **Discard** button to discard the changes.

Pop-up progress window will appear during the **Apply** operation:

After the configuration of the general settings, the device is ready for basic operation. Web interface menu can be used for further device configuration. Please refer to the chapter *Configuration Guide* for detailed configuration instructions.

Configuration Guide

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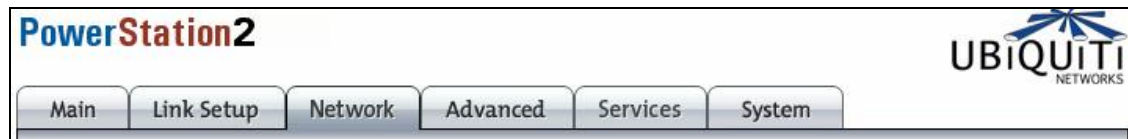

Figure 1 – Configuration Management Menu

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

Link Setup page let to prepare the device for use in a wireless network, while covering basic wireless settings – i.e. controls how a subscriber station associates to an access point, authenticates to the wireless network, encrypts and decrypts data.

Network page covers the configuration of IP settings and network services (i.e. DHCP).

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

Services page covers the configuration of system management services (i.e. SNMP, Ping Watchdog).

System page contains controls for system maintenance routines, administrator account management, device customization and configuration backup.

Main Settings

This page displays a summary of status information. It shows important information for the device operating mode, network settings as well as traffic statistics of the wireless and LAN interfaces.

Figure 2 – Current Status of the Subscriber Station

Base Station SSID:

While operating in *Station* mode, displays the SSID of the Access Point where the device has associated.

While operating in in *Access Point* mode, displays the SSID of the device itself.

AP MAC: displays the MAC address of the Access Point where the device has associated while operating in *Station* mode.

Signal Strength, dBm: displays the received signal level (client-side) while operating in *Station* mode. The represented value coincides with the graphical bar.

8

Use antenna alignment tool to adjust the device antenna to get better link with the wireless device. The antenna of wireless client has to be adjusted to get maximum signal strength.

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

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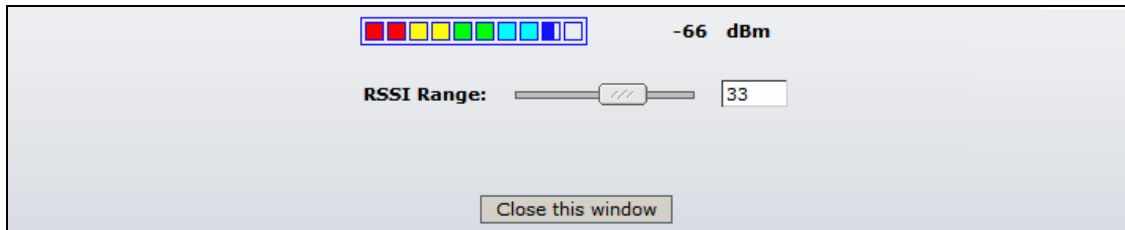

Figure 3 – Antenna alignment Tool

TX Rate: displays the current data transmission rate while operating in *Station* mode.

RX Rate: displays the current data reception rate while operating in *Station* mode.

Channel: displays the channel used by device to transmit and receive data.

Frequency: displays the frequency used by device to transmit and receive data.

Antenna Polarity: displays the current Antenna Polarity setting.

Security: displays the security method, which is set on the device.

ACK Timeout: displays current ACK Timeout value, which is set on the device manually or adjusted automatically.

QoS Status: displays the QoS Status, which is set on the device.

Uptime: indicates the time, expressed in days, hours, minutes and seconds since last hard-reboot.

LAN Cable: displays the current status of the Ethernet port connection.

LAN MAC: displays the MAC address of the LAN (Ethernet) interface.

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

LAN IP address: displays the current IP address of the LAN (Ethernet) interface while operating in *Router* mode.

WLAN IP address: displays the current IP address of the WLAN (Wireless) interface while operating in *Router* mode.

LAN IP address and **WLAN IP address** displays the same value - current IP address of the virtual bridge interface, while operating in *Bridge* mode.

Extra Info: displays the current usage statistics in pop-up window:

Show Stations… selection lists the stations which are connected to the device while operating in Access Point mode. Each station **RSSI**, **Tx Rate** and **Idle** time (sec) can be updated using the **Reload** button:

Station MAC	RSSI	Tx Rate	Idle (sec)
00:15:6D:A6:00:1E	51	54M	30

Reload   Close this window

Figure 4 – Current Status of the Associated Stations

Show ARP Tables… selection lists all the entries in the system ARP tables. The list can be updated using the **Reload** button:

IP Address	MAC address	Interface
10.10.0.1	00:40:F4:FF:51:0D	LAN
10.10.0.101	00:A0:D1:6A:70:A5	LAN

Reload   Close this window

Figure 5 – Current Status of the system ARP tables

Show Routes… selection lists all the entries in the system routing tables. The list can be updated using the **Reload** button:

Destination	Gateway	Netmask	Interface
192.168.1.0	*	255.255.255.0	WLAN
10.0.0.0	*	255.0.0.0	LAN
default	10.10.0.1	0.0.0.0	LAN

Reload   Close this window

Figure 6 – Current Status of the system routing tables

Show DHCP Leases… selection shows the current status of the leased IP addresses by the device's DHCP server. **Interface** name shows from which device interface DHCP client which has specified **MAC Address** is connected. **Remaining Lease** time shows for how long the leased **IP address** will be valid and reserved for particular DHCP client. The list can be updated using the **Reload** button:

MAC Address	IP Address	Remaining Lease	Interface
00:15:6d:a6:00:1e	192.168.1.23	00:59:51	WLAN

Reload   Close this window

Figure 7 – Current Status of the DHCP leases

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

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

WLAN Errors: section displays the counters of 802.11 specific errors which were registered on wireless interface (**invalid packets received**, **transmitted excessive retries**, **missed beacons** and other).

Link Setup

The **Link Setup** page allows you to manage general wireless connection parameters of the device.

Basic Wireless Settings

The general wireless settings, such as wireless device SSID, country code, output power, 802.11 mode and data rates can be configured on this section:

Figure 8 – Basic Wireless Settings

Wireless Mode: specify the operating mode of the device. The mode depends on the network topology:

   Station – in this mode the device acts as Subscriber Station, while connecting to Access Point defined by SSID.

   Station WDS – in this mode the device acts as Subscriber Station, while connecting to Access Point using the WDS protocol.

   Access Point – in this mode the device acts as Access Point.

   Access Point WDS – in this mode the device acts as Access Point with the WDS protocol support.

Station - *Bridge* mode has pass-through restrictions for Layer2 protocols while it is transparent for DHCP and PPPoE protocols.

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

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

SSID/ESSID:

   While operating in *Access Point* mode, specify the SSID of the device itself.

   While operating in *Station* mode, specify the ESSID of the Access Point where the device will be associated to.

Hide SSID: selected control will disable broadcasting of the SSID 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.

Channel: select the operating 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** and **IEEE** mode.

Country Code: choose from drop-down list the country in which you will use the device.

Output Power: specify the output power (dBm) at which wireless module transmits data using the slider. When entering output power value manually, the slider position will change according to the entered value. The transmit power level that is actually used is limited to the maximum value allowed by your country's regulatory agency.

IEEE 802.11 Mode: select the IEEE 802.11 mode of your wireless network.

> PowerStation2/LiteStation2 supported IEEE 802.11 modes:
>> **B only** – connect to a 802.11b only network.
>> **B/G Mixed** – connect to a 802.11b/g network (selected by default).
>> **G only** – connect to a 802.11g only network.
> LiteStation5 supported IEEE 802.11 modes:
>> **A** – connect to a 802.11a network (selected by default).
>> **A (Dynamic Turbo)** – connect to a 802.11a network which supports Dynamic Turbo feature.
>> **A (Static Turbo)** – connect to a 802.11a network which supports Static Turbo feature.

Data Rate: choose the data rate in Mbps at which the device should transmit wireless packets. Use **Auto** option if you are having trouble getting connected or losing data at a higher rate. In this case the lower data rates will be used by device automatically.

Rate Mode: choose the channel width (**20** Mhz/**Full** Rates, **10** MHz/**Half** Rates or **5** MHz/**Quarter** Rates) which will be utilized for data transmission.

Lock to AP MAC: specify the MAC address of the Access Point where the device will be associated to while operating in *Station* mode. The device connects to a network (ESSID) composed of many Access Points with roaming by default. Specification of the MAC address will restrict the association to one particular Access Point:

ESSID:	Ubiquiti_AP	Select...
Lock to AP MAC:	00:15:6D:A6:05:1A	

Figure 9 – Locking the Station to Access Point specified by MAC

Use the **Select…** button next to **ESSID** entry field to load the **Site Survey** tool in pop-up window while operating in *Station* mode. Site Survey will search for all wireless networks in range 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.

	MAC address	ESSID	Encryption	Signal, dBm	Frequency, GHz	Channel
○	00:15:6D:A3:05:04	Ubiquiti_AP	-	-57	2.412	1
○	00:11:2F:0E:93:46	Meta_AP	WEP	-61	2.422	3
○	00:15:6D:A3:03:96	WPA_AP	WPA	-60	2.422	3

Select Scan   Close this window

Figure 10 – Site Survey Scan

Select the Access Point from the list and click **Select** button for association.

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

Close this window button closes Site Survey window.

Wireless Security

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

WIRELESS SECURITY

Security:	none ▼
Authentication Type:	⦿ Open ○ Shared Key
WEP Key Length:	64 bit ▼ **Key Type:** HEX ▼
WEP Key:	____ **Key Index:** 1 ▼
WPA Preshared Key:	____

Change

Figure 11 – Wireless Security Settings

Security: select the security mode of your wireless network.

None – disable security.

WEP – enable WEP encryption.

WPA – enable WPA™ with Pre-shared Key encryption.

WPA2 – enable WPA2™ with Pre-shared Key encryption.

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

WIRELESS SECURITY

Security:	WEP ▼
Authentication Type:	⦿ Open ○ Shared Key
WEP Key Length:	64 bit ▼ **Key Type:** HEX ▼
WEP Key:	00AA22CC33 **Key Index:** 2 ▼

Figure 12 – Configuration of the WEP

13

Authentication Type: choose the one of the following authentication modes for WEP security method:

> **Open Authentication** – station is authenticated automatically.
>
> **Shared Authentication** – station is authenticated after the challenge, generated by AP.

WEP Key Length: select the WEP Key length here, either **64-bit**, or **128-bit** (stronger).

Key Type: use the **HEX** or **ASCII** option to specify the character format for the WEP key.

WEP Key: enter the WEP key for wireless traffic encryption/decryption:

> For **64-bits** – specify pre-shared key as 5 HEX (0-9, A-F or a-f) pairs (e.g. 00112233AA) or 5 ASCII characters.
>
> For **128-bits** – specify pre-shared key as 13 HEX (0-9, A-F or a-f) pairs (e.g. 00112233445566778899AABBCC) or 13 ASCII characters.

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

WPA™ (IEEE 802.11i/D3.0) and WPA2™ (IEEE 802.11i) with pre-shared key management protocol offers improved security methods. WPA™ and WPA2™ supports the following ciphers for data encryption:

> TKIP - Temporal Key Integrity Protocol which uses RC4 encryption algorithm.
>
> CCMP - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol which uses the Advanced Encryption Standard (AES) algorithm.

The device will use the strongest cipher (CCMP) in *Station* and *Access Point* wireless mode by default. If CCMP is not supported on the other side of the link the TKIP encryption will be used - like in situation when the device acts as Access Point with WPA security enabled and at least one wireless station (without CCMP support) is connected to it. Enable WPA2™ (RSN) security:
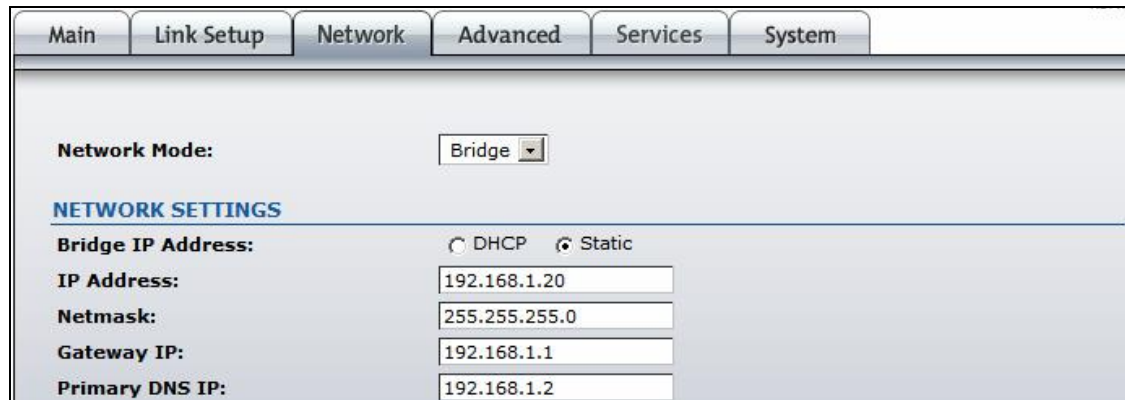

Figure 13 – WPA Security Settings

WPA Pre-shared Key: enter a passphrase for WPA™ or WPA2™ encryption. The pre-shared key is an alpha-numeric password between 8 and 63 characters long.

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

Network Settings

PowerStation2/LiteStation2 and LiteStation5 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:

Figure 14 – Bridge mode Network Settings

Network Mode: specify the operating network mode for the device. The mode depends on the network topology:

    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.

    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. The device can act as DHCP server and use Network Address Translation (Masquerading) feature in router mode which is widely used by the Access Points.

Bridge IP Address: specify the IP mode:

    DHCP – choose to assign the dynamic IP settings by the DHCP server.

    Static – choose to assign a static IP address.

IP Address: enter IP address of the device.

Netmask: enter a subnet mask of the device.

Gateway IP: enter a Gateway IP address.

Primary DNS IP: enter a DNS IP address.

Figure 15 – Router mode Network Settings

There are two network segments (**WLAN** and **LAN**) configured separately when device is operating in **Router** mode.

Wireless network segment can be configured in **WLAN Network Settings** section:

IP Address: enter IP address of the WLAN interface.

Netmask: enter a subnet mask of the WLAN interface.

Enable NAT: control will enable Network Address Translation (Masquerading) feature between WLAN and LAN interfaces.

Enable DHCP Server: control will enable DHCP Server feature on WLAN interface.

The DHCP options should be configured while **DHCP Server** is enabled:

Range Start: Enter the IP address that begins the range of IP address space reserved for DHCP.

Range End: Enter the IP address that ends the range of IP address space reserved for DHCP.

Netmask: Enter the subnet mask of IP address space reserved for DHCP.

Lease Time: Enter the lease period (in seconds) during which DHCP guarantees that the IP address assigned to one particular client is not reassigned to another client.

LAN (Ethernet) connection settings can be configured in **LAN Network Settings** section which is identical to the bridge mode Network Settings section described above.

LAN IP settings can be assigned automatically using the **DHCP** or **PPPoE**. If **PPPoE** mode is selected, the **Username** and **Password** credentials are required for PPPoE authentication.

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

Advanced

The **Advanced** options page allows you to manage advanced settings that influence on the device performance and behavior.

Advanced Wireless Settings

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.

Figure 16 – Advanced Wireless Settings

Rate Algorithm: defines data rate algorithm convergence:

Optimistic Algorithm is aggressive enough to move to a higher rate but yet tries to conservatively capture the fluctuations of the RSSI. It starts with the highest possible rate and then decreases till the rate can be supported while periodically transmitting packets at higher rates and computing the transmission time.

Conservative Algorithm is less sensitive to individual packet failure as it is based on a function of number of successful and erroneous transmission/retransmission over a sampling period. It steps down to a lower rate after continuous packet failure and steps up after number of successful packets.

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

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

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

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

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

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

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

ACK Timeout: specify the ACK Timeout (20-520). This is the amount of time the subscriber station will wait to hear a acknowledgement response from the wireless device after the data packet is transmitted. If the timeout is set too short or too long, it will result poor connection and throughput performance. Changing the ACK Timeout value will change the **Distance** to the appropriate distance value for the ACK Timeout.

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

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

> **Fast Frame** – utilizes frame aggregation and timing modifications.
> **Bursting** – more data frames per given time period are transmitted.
> **Compression** – real-time hardware data compression is enabled.

RSSI LED Thresholds

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

RSSI LED THRESHOLDS	
LED 1:	1
LED 2:	15
LED 3:	22
LED 4:	30

Figure 17 – RSSI LED Thresholds Configuration

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

Antenna

PowerStation2 has a possibility to switch the antenna polarities with a single web

management control. This is achieved by using Ubiquiti's patent-pending Adaptive Antenna Polarity (AAP) technology.

ANTENNA

Antenna Polarity:	Adaptive ▾

Figure 18 – Antenna Polarity Configuration

Antenna polarity defines embedded hi-gain antenna polarity:

Vertical – switches vertical antenna polarity.

Horizontal – switches horizontal antenna polarity.

Adaptive – switches adaptive antenna polarity mode which allows for the beam polarities to be switched dynamically on the fly for improved performance in heavy noise environments.

Wireless Traffic Shaping

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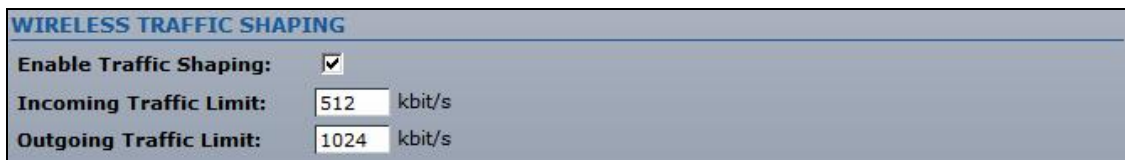
WIRELESS TRAFFIC SHAPING

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

Figure 19 – Wireless Traffic Shaping Setup

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

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

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

802.11e QoS (WMM) Settings

Wi-Fi Multimedia (WMM) is a component of the IEEE 802.11e wireless LAN standard for quality of service (QoS). The QoS assigns priority to the selected network traffic, prevents packet collisions and delays thus improving VoIP calls and watching video over WLANs.
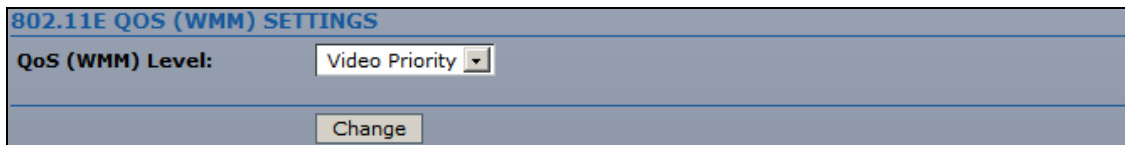
802.11E QOS (WMM) SETTINGS

QoS (WMM) Level:	Video Priority ▾
	Change

Figure 20 – QoS Setup

QoS (WMM) Level: choose the type of the network traffic to which the priority will be set or disable the QoS feature.

No QoS – disable QoS.

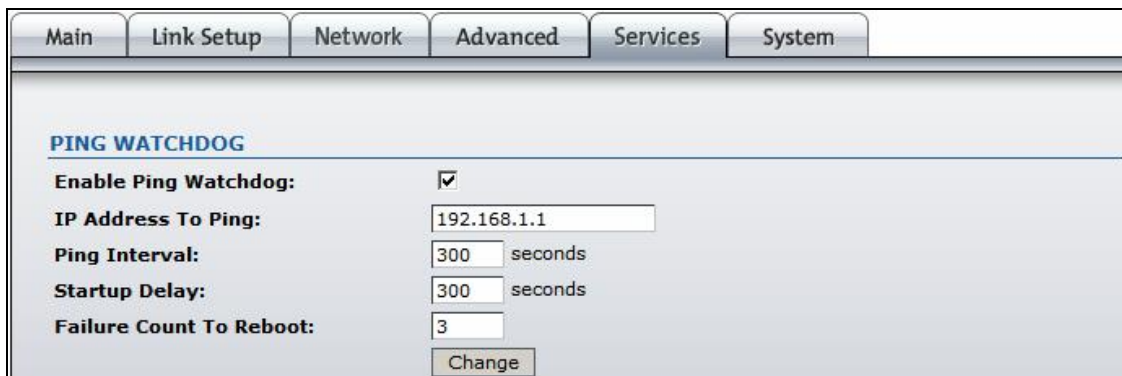**Video Priority** – enable priority of the video traffic.

Voice Priority – enable priority of the voice traffic.

Services

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

Ping Watchdog

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.

Figure 21 – Ping Watchdog configuration

Enable Ping Watchdog: control will enable Ping Watchdog Tool.

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

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

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

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

SNMP Agent

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:

Figure 22 – SNMP Agent Configuration

Enable SNMP Agent: control will enable SNMP Agent.

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

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

Location: specify the physical location of the device.

System

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

Firmware

Use this section to find out current software version and update the device with the new firmware.

The device firmware update is compatible with all configuration settings. When the device is updated with a newer version or the same version firmware builds, system configuration will be preserved.

Figure 23 – Firmware Upgrade. Step 1

Firmware version: displays version of the current firmware.

Upgrade…: click to load the device firmware upgrade window.

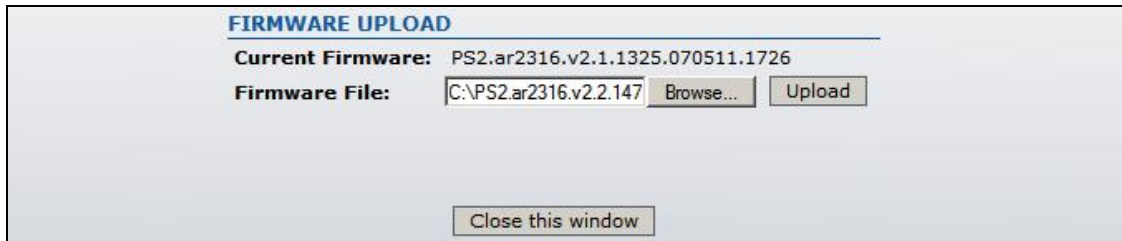After the **Upgrade…** button is clicked the new Firmware Upload pop-up window will be displayed:

FIRMWARE UPLOAD

Current Firmware: PS2.ar2316.v2.1.1325.070511.1726

Firmware File: C:\PS2.ar2316.v2.2.147 [Browse…] [Upload]

[Close this window]

Figure 24 – Firmware Upgrade. Step 2

Current Firmware: displays version of the current firmware.

Firmware File: click the **Browse…** button to specify the new firmware image location or specify the full path and click the **Upload** button.

Close this window – cancel the upload process.

After the new firmware image is uploaded into the system, use **Upgrade** button to upgrade a device:
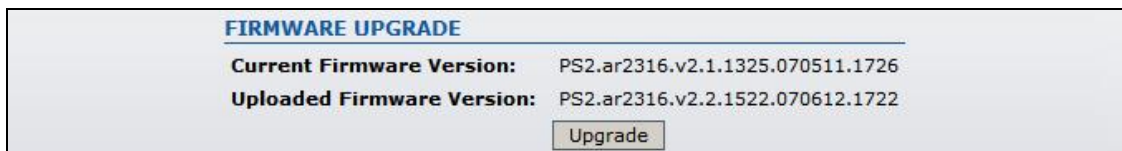

FIRMWARE UPGRADE

Current Firmware Version: PS2.ar2316.v2.1.1325.070511.1726

Uploaded Firmware Version: PS2.ar2316.v2.2.1522.070612.1722

[Upgrade]

Figure 25 – Firmware Upgrade. Step 3

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

After clicking the **Upgrade** button the upgrade process starts immediately:
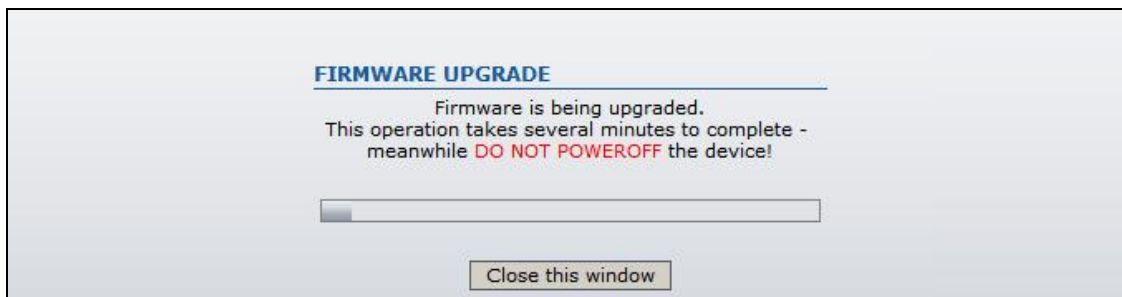

FIRMWARE UPGRADE

Firmware is being upgraded.
This operation takes several minutes to complete -
meanwhile DO NOT POWEROFF the device!
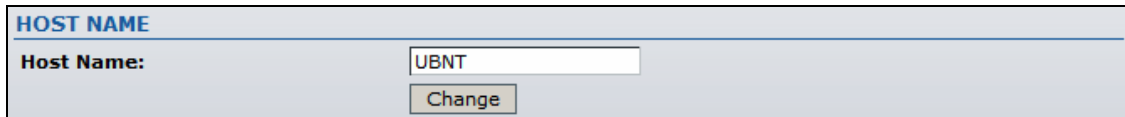
[Close this window]

Figure 26 – Progress of the Firmware Upgrade

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

Host Name

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

HOST NAME

Host Name:	UBNT
	Change

Figure 27 - Host Name Configuration

Host Name: specify the system identity.

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

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 setup:

ADMINISTRATIVE ACCOUNT

Administrator Username:	ubnt
Current Password:	****
New Password:	**********
Verify New Password:	**********
	Change

Figure 28 - Change Administrator Settings

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

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

> User Name: **ubnt**
> Password: **ubnt**

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

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

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

Logo Customization

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

 The size limit of the logo is 50Kb.

 The maximum height of logo should be 70 pixels.

 Only .gif format images are accepted.

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

Figure 29 – Custom Logo Upload

Enable Custom Logo: control will enable logo customization. Deselecting this option the custom logo will be removed and the default Ubiquiti logo will be restored.

Logo Target URL: specify the target URL of custom logo. Target URL is opened when clicking on custom logo.

Logo File: click **Browse…** button to navigate to and select the logo file or specify the full path and click the **Upload** button.

Configuration Management

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

Figure 30 – Configuration Management

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

Upload Configuration: click **Browse…** button to navigate to and select the new configuration file or specify the full path and click the **Upload** button.

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

Device Maintenance

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

Figure 31 – Device Maintenance Settings

Reboot: click to hard-reboot the device in the current configuration. Any non-applied changes will be lost.

Reset to Defaults: click to reset the device to factory defaults.

---

[i] WPA™, WPA2™, Wi-Fi Protected Access™ are trademarks of the Wi-Fi Alliance.
[ii] SuperG® and SuperAG® are registered trademarks of Atheros Communications, Inc.