



Bitlomat 200  
User Manual



# Contents

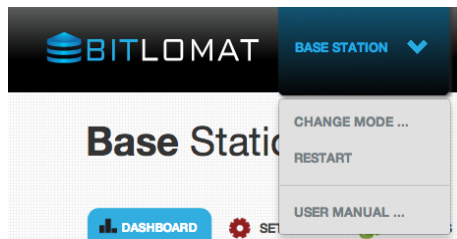
<b>1</b>	<b>Operating Modes</b>	<b>3</b>
1.1	Base Station.....	3
1.2	CPE.....	4
1.3	Home Router.....	5
1.4	Point-to-Point Link.....	6
<b>2</b>	<b>Bitlomat Default Settings</b>	<b>7</b>
<b>3</b>	<b>Dashboard</b>	<b>8</b>
<b>4</b>	<b>Settings Menu</b>	<b>10</b>
4.1	Base Station Settings.....	11
4.2	CPE Settings.....	15
4.3	Home Router Settings.....	18
4.4	Point-to-Point Link Settings.....	22
<b>5</b>	<b>Services</b>	<b>27</b>
5.1	SSH.....	27
5.2	SHAPER.....	28
5.3	MAC ACL.....	28
5.4	NAT and Port Forwarding.....	29
5.5	ROUTES.....	29
5.6	FIREWALL.....	30
5.7	DDNS.....	31
5.8	NTP.....	32
5.9	SNMP.....	33
<b>6</b>	<b>Tools</b>	<b>42</b>
6.1	PING.....	34
6.2	TRACE.....	34
6.3	IPERF.....	35
6.4	AP SCAN.....	35

# Bitlomat-200 User Manual

## 1. Operating Modes

- Base Station
- CPE
- Home Router
- Point-to-Point Link

The operating modes can be changed using the dashboard selector.



When an operating mode is selected, an intuitive wizard is launched to guide the user in the basic configuration of the operating modes. Please consult advanced configuration settings page for a detailed description of all the settings.

### 1.1 Base Station

When the Base Station mode is selected, the unit will operate as a Bridge to another Base Station or CPE. The network architecture is the typical point-to-point operation. The first step is to configure the wired WAN port which is supposed to be connected to the Internet.

The WAN port can be configured using a static IP address or DHCP.

With the second step, the wireless parameters can be configured including frequency, channel width, SSID and wireless security.

By scrolling down the menu, the network parameters for the wireless interface can be also configured as shown below. The wireless interface can be set to "bridge" the WAN and the Wireless interfaces together (same broadcast domain) or as a "router" by separating the WAN and Wireless broadcast domains (and IP addressing schemes).

## **1.2 CPE**

When the CPE mode is selected, the unit will operate as a Station that wirelessly connects to a Base Station. The network architecture is the typical point-to-point operation. The first step is to configure the Wireless interface which is supposed to be connected to the Internet through the Base Station. The wireless parameters can be configured including frequency, channel width, SSID and wireless security.

By scrolling down the menu, the network parameters for the wireless interface can be also configured as shown below. The wireless interface IP address can be static or assigned by a DHCP.

The second step is to configure wired LAN port which is supposed to be connected to the Customer Premises devices. A DHCP server can be also set up to provide IP addresses to the private Customer network.

### **1.3 Home Router**

The Home Router mode is typically used to provide wireless connectivity to home/office devices like PC and smartphone. Therefore the wireless interface is bridged with the LAN port of the Bitlomat unit whereas the WAN is connected to the Internet. The basic configuration consists of 3 steps.

In the first step, the wired WAN is configured as shown below. Static or dynamic (DHCP) IP addresses can be set. The port can also be configured to use PPPoE

In the second step, the wireless interface can be configured and it will be automatically bridged with the wired LAN interface. Therefore, no IP address is needed for it.

In the final step, the local wired LAN can be configured. A DHCP server can be also set up to provide IP addresses to the private Customer network both the wireless and the wired LAN interfaces.

## **1.4 Point-to-Point Link**

The Point-to-Point mode can be used to create transparent layer 2 bridges extending two network segments within the same broadcast domain. The two units at the ends of the link must be set as "master" and "slave", respectively. Once the Link Role is selected, a static IP address can be set for the unit.

Finally, the wireless interface parameters can be configured including frequency, channel width, SSID and wireless security.

## 2. Bitlomat Default Settings

The default IP address of the Bitlomat devices is:

**IP: 192.168.0.10**  
**Netmask: 255.255.255.0**

To log into the unit, set your PC to any IP address in the same IP class, e.g. 192.168.0.30/255.255.255.0.

Open the browser and connect to 192.168.0.10. The default username and password for Bitlomat is:

**username: bitlomat**  
**password: bitlomat**

The unit can be configured using the Web GUI as described in Chapter 1, Operating Modes.

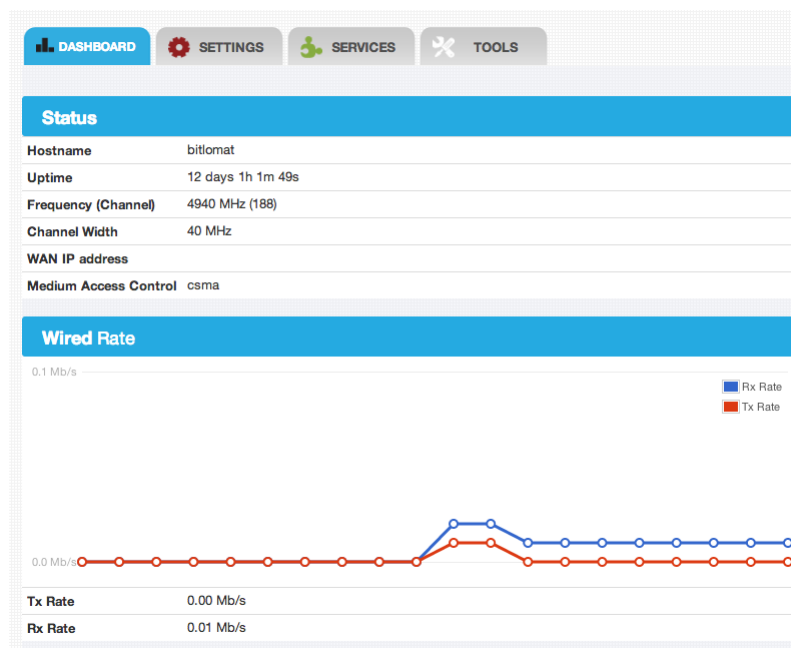
The SSH command line interface can be accessed with the default credentials above. SSH access can be customized as described in Chapter 5, Services.



### 3. Dashboard

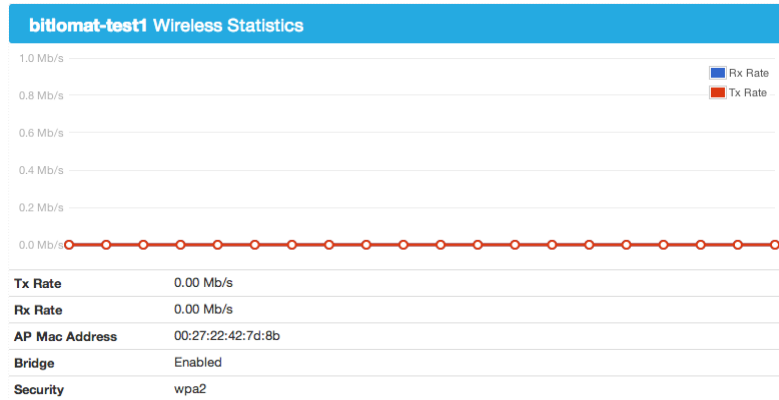
Once logged in into the Web GUI of the Bitlomat unit, the dashboard will be the first visible page reporting a complete summary of the status of the unit. The **Status** parameters include:

- Uptime: unit uptime
- Frequency (Channel): current frequency and channel the unit is set to work to (Base Station only)
- Channel Width: current width of the channel in use
- WAN/LAN IP addresses: configured IP addresses for the interfaces
- Medium Access Control: the current MAC in use, e.g. CSMA or TDMA



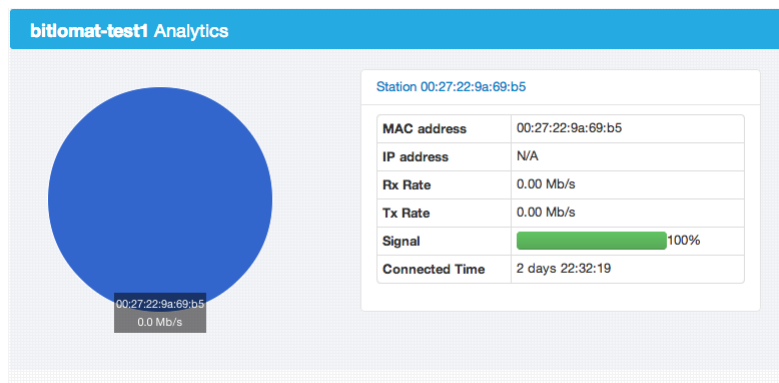
The **Wired Rate** graph reports the real-time wired ethernet utilization both in TX and RX directions.

By scrolling down the dashboard, the **Wireless Statistics** graph will report the TX and RX utilization of the wireless link grouped by SSID.



Finally, in **Base Station** and **Home Router only**, a piechart reporting the traffic divided per each connected CPE/device is shown. Additional information related to the CPE/devices connected are also reported. Those information include:

- MAC address: the HW address of the station connected
- IP address: the IP address of the station connected
- RX rate: rate of the traffic received by the station (downlink traffic)
- TX rate: rate of the traffic transmitted by the station (uplink traffic)
- Connected Time: connection time of the station



## 4. Settings Menu

The **Settings** menu contains all the (advanced) settings of the unit. Once the operation mode is selected using the wizard, the unit settings can be modified accordingly. The right-hand menu is used to navigate among specific interfaces or system parameters. As mentioned above the configuration menu are generated with respect to the specific operating mode and can thus be different if the unit is operated e.g. as a Base Station or as a CPE.

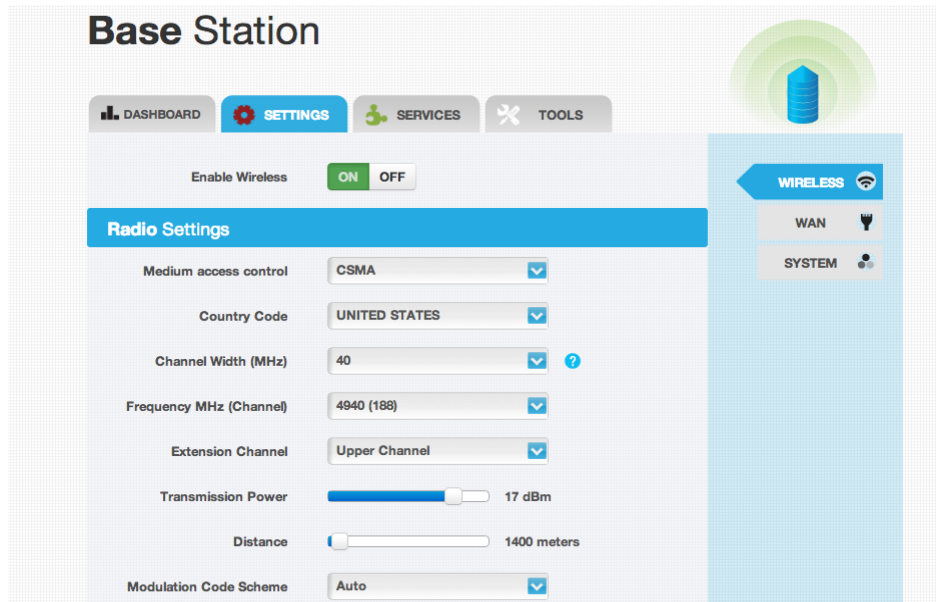
However, as a general rule of thumb, the **Wireless** menu contains the settings of the wireless interface including IP addressing whether it is used as a private LAN (Base Station mode) or as public WAN (CPE mode). The **WAN/LAN** menu is used to configure the wired connection. Finally, the **System** menu contains general system-wide settings.

Given that the menus are different depending on the operating mode please refer to following links for a detailed description:

- **Base Station**
- **CPE**
- **Home Router**
- **Point-to-Point Link**

## 4.1 Base Station Settings

### ➤ Wireless Menu



The wireless menu contains all the parameters relative to the wireless interface. The menu is divided into groups:

- Radio Settings
- Network Options

### ◆ Radio Settings

The Radio Settings menu, shown below, is used to configure all the radio-related parameters:

- **Medium access control** instructs the radio to operate using the standard IEEE 802.11 MAC (CSMA) or the Bitlomat proprietary point-to-point protocol (TDMA).
- **Country Code** must be set according to the country of operation. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where the device will be used.
- **Channel Width** is the spectral width of the wireless channel. Supported widths are 5, 10, 20 and 40 MHz.
- **Frequency** is the spectral frequency of operation of the wireless channel.

- **Extension Channel** indicates the use of channel bonding that allows the radio to use two channels at once.
- **Transmission Power** is the actual radio emitted power in dBm. Different countries have different regulation. The radio automatically obeys the regulation of the selected country.
- **Distance** represents the estimated link distance.
- **Modulation Code Scheme** defines the data rate (in Mbps) at which the device should transmit wireless packets. It is recommended to use automatic option.

## ◆ Network Options

The wireless interface can be operated as a **Router** or as a **Bridge**.

### ● Router

When the wireless interface is operated as a Router, the wireless and the wired broadcast domains are separate. Therefore, a different IP address must be specified for each SSID. Multiple SSIDs can be added up to 8. The SSID parameters are:

- **SSID** is the Name of the IEEE 802.11 Service Set and is used by the CPEs/clients to connect.
- **Hide SSID** will disable advertising the SSID in broadcast messages to the CPEs/clients.
- **Client Isolation** allows packets to be sent only from the external network to the CPE and vice versa, thus preventing different CPEs to communicate with each other.
- **Security** supports none, WPA, and WPA2 security options.
- **IP Address** is the private IP address of the wireless interface.
- **Netmask** is the subnet mask of the private IP address of the wireless interface.
- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.
- **DHCP Server** can be optionally enabled to automatically assign IP addresses to the CPEs/clients.

The image displays two side-by-side screenshots of the Bitlomat Web GUI's 'Network Options' page for a wireless network named 'bitlomat-test1'.

**Left Screenshot (Router Mode):** The 'Network Role' is set to 'ROUTER'. The 'Wireless Network "bitlomat-test1"' section includes fields for SSID (bitlomat-test1), Hide SSID (ON/OFF), Client Isolation (ON/OFF), Security (wpa2), Key Management Algorithm (PSK/EAP), WPA Preshared Key (bitlomat), IP address, Netmask, MTU (1500), and DHCP Server (ON/OFF).

**Right Screenshot (Bridge Mode):** The 'Network Role' is set to 'BRIDGE'. This mode includes additional options: 'Spanning Tree Protocol' (ON/OFF), 'Enable VLANs' (ON/OFF), and 'Management VLAN ID'. The wireless network configuration fields are similar to the router mode but lack the IP address, Netmask, and MTU fields.

▲ Router

▲ Bridge

## ● Bridge

In bridge mode the wireless interface and the wired WAN are bridged and belongs to the same broadcast domain. Therefore, there is no need to specify an IP address for the wireless interface, however, additional parameters are available:

- **Spanning Tree Protocol** is used for finding the shortest path within the network and to eliminate loops from the topology.
- **VLANs** can be enabled for the SSID. Using the Web GUI, it is possible to add one VLAN ID for each SSID. The wired WAN port will be then set to operate in trunking mode to work together with the wired VLAN-enabled switches present in the network. Bitlomat VLAN support is fully compatible with the standard IEEE 802.1q.
- **Management VLAN ID** is used to manage the Bitlomat units when VLANs are present. By adding the management VLAN ID to the wired network switch, it will be possible to access the units from it.

## ➤ WAN Menu

**Base Station**

DASHBOARD SETTINGS SERVICES TOOLS

**WAN Settings**

IP Address Assignment: Static

IP address: 10.10.3.65

Netmask: 255.255.0.0

Gateway: 10.10.0.1

Primary DNS: 10.10.0.1

Secondary DNS: 8.8.8.8

MTU: 1500

SAVE

WIRELESS

**WAN**

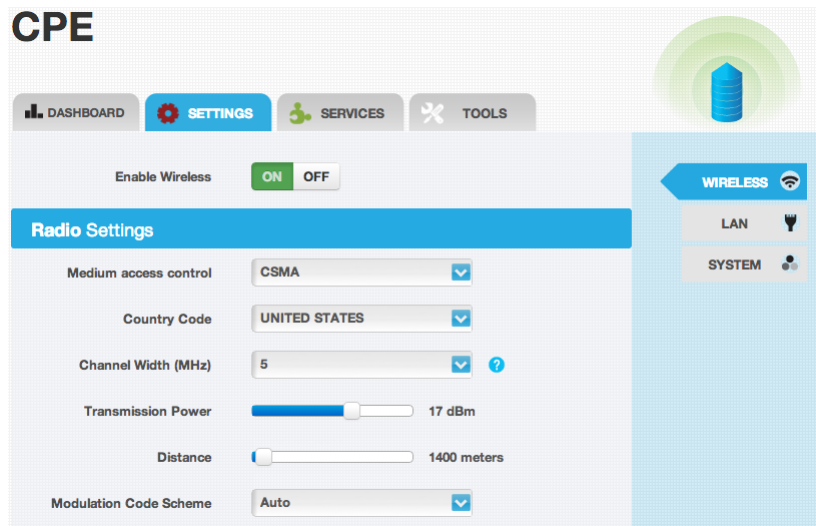
SYSTEM

The WAN menu is used to configure the wired WAN which is connected to the Internet. If the wireless interface is operated in **bridge mode** the WAN IP address will be the IP of the bridge. The WAN menu page settings are:

- **IP Address Assignment:** the Base Station IP address can be assigned statically or using a DHCP server in the network.
- **IP Address** is the private IP address of the WAN interface.
- **Netmask** is the subnet mask of the private IP address of the WAN interface.
- **Gateway** must be set to the IP address of the local network gateway used to accessing the Internet.
- **Primary DNS** is the mandatory server which translates domain names to IP addresses.
- **Secondary DNS** is the optional server which translates domain names to IP addresses.
- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.

## 4.2 CPE Settings

### ➤ Wireless Menu



The wireless menu contains all the parameters relative to the wireless interface. The menu is divided into groups:

- Radio Settings
- Wireless Network

### ◆ Radio Settings

The Radio Settings menu, shown below, is used to configure all the radio-related parameters:

- **Medium access control** instructs the radio to operate using the standard IEEE 802.11 MAC (CSMA) or the Bitlomat proprietary point-to-point protocol (TDMA).
- **Country Code** must be set according to the country of operation. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where the device will be used.
- **Channel Width** is the spectral width of the wireless channel. Supported widths are 5, 10, 20 and 40 MHz. Please note that it's not possible to choose the frequency as that depends on the Base Station to which the CPE connects.



- **Transmission Power** is the actual radio emitted power in dBm. Different countries have different regulation. The radio automatically obeys the regulation of the selected country.
- **Distance** represents the estimated link distance.
- **Modulation Code Scheme** defines the data rate (in Mbps) at which the device should transmit wireless packets. It is recommended to use automatic option.

## ◆ Wireless Network

The image shows a configuration interface divided into two sections: 'Wireless Network' and 'WAN Settings'.

**Wireless Network Section:**

- SSID:** A text input field containing 'bitomat-test1' and a blue 'SCAN' button to its right.
- BSSID:** An empty text input field.
- Security:** A dropdown menu showing 'wpa2' with a blue checkmark and a help icon (i).
- Key Management Algorithm:** Two radio buttons: 'PSK' (selected) and 'EAP'.
- WPA Preshared Key:** A text input field containing 'bifoloo333'.

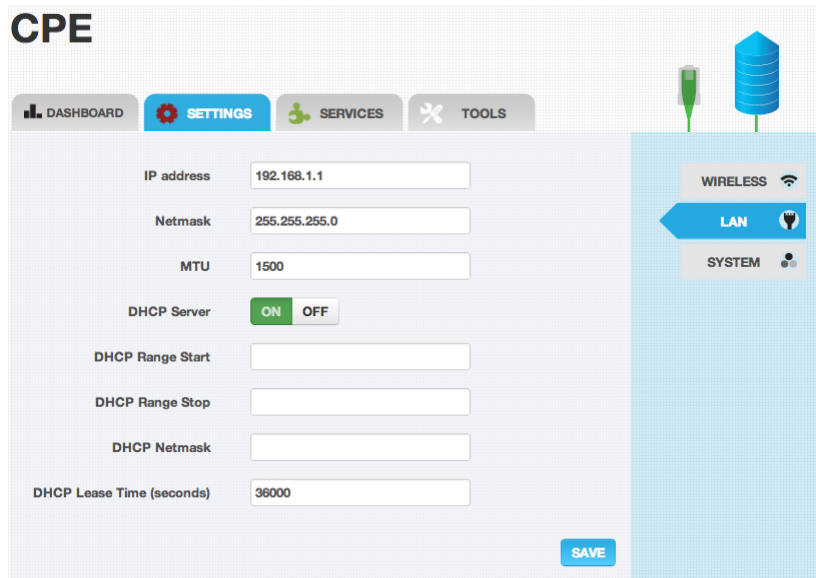
**WAN Settings Section:**

- IP Address Assignment:** A dropdown menu showing 'Static' with a blue checkmark.
- IP address:** A text input field containing '10.10.3.65'.
- Netmask:** A text input field containing '255.255.0.0'.
- Gateway:** A text input field containing '10.10.0.1'.
- Primary DNS:** A text input field containing '10.10.0.1'.
- Secondary DNS:** A text input field containing '8.8.8.8'.
- MTU:** A text input field containing '1500'.

- **SSID** is the Name of the IEEE 802.11 Service Set of the Base Station to connect to. The CPE can scan for SSIDs by clicking on the **SCAN** button
- **BSSID** can be optionally specified as the MAC address of the Base Station to which the CPE is connecting to.
- **Security** supports none, WPA, and WPA2 security options.
- **IP Address** is the IP address of the wireless interface. The IP address can be statically configured or automatically set via DHCP if properly configured in the Base Station.
- **Netmask** is the subnet mask of the IP address of the wireless interface.
- **Gateway** must be set to the IP address of the local network gateway used to accessing the Internet.
- **Primary DNS** is the mandatory server which translates domain names to IP addresses.
- **Secondary DNS** is the optional server which translates domain names to IP addresses.

- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.

## ➤ LAN Menu



The screenshot shows the CPE (Customer Premise Equipment) configuration interface. The top navigation bar includes 'DASHBOARD', 'SETTINGS' (active), 'SERVICES', and 'TOOLS'. The 'SETTINGS' section is divided into 'WIRELESS', 'LAN' (active), and 'SYSTEM'. The 'LAN' configuration area contains the following fields:

- IP address:** 192.168.1.1
- Netmask:** 255.255.255.0
- MTU:** 1500
- DHCP Server:** ON (selected), OFF
- DHCP Range Start:** (empty field)
- DHCP Range Stop:** (empty field)
- DHCP Netmask:** (empty field)
- DHCP Lease Time (seconds):** 36000

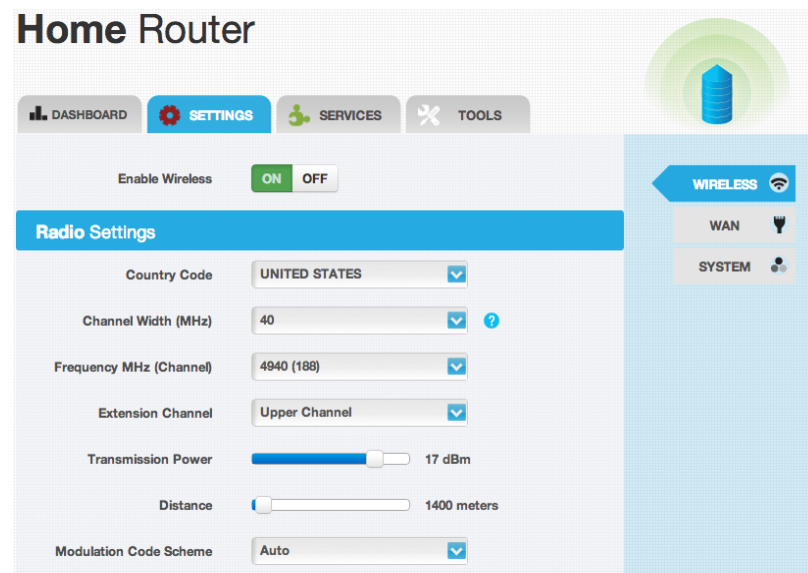
A 'SAVE' button is located at the bottom right of the configuration area.

The LAN menu is used to configure the wired LAN connected to private customer network. The LAN menu page settings are:

- **IP Address** is the private IP address of the LAN interface.
- **Netmask** is the subnet mask of the private IP address of the LAN interface.
- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.
- **DHCP Server** can be optionally enabled to automatically assign IP addresses to LAN PCs/devices.

## 4.3 Home Router Settings

### ➤ Wireless Menu



The wireless menu contains all the parameters relative to the wireless interface. The menu is divided into groups:

- Radio Settings
- Wireless Network

### ◆ Radio Settings

The Radio Settings menu, shown below, is used to configure all the radio-related parameters:

- **Country Code** must be set according to the country of operation. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where the device will be used.
- **Channel Width** is the spectral width of the wireless channel. Supported widths are 5, 10, 20 and 40 MHz.
- **Frequency** is the spectral frequency of operation of the wireless channel.
- **Extension Channel** indicates the use of channel bonding that allows the radio to use two channels at once.

- **Transmission Power** is the actual radio emitted power in dBm. Different countries have different regulation. The radio automatically obeys the regulation of the selected country.
- **Distance** represents the estimated link distance.
- **Modulation Code Scheme** defines the data rate (in Mbps) at which the device should transmit wireless packets. It is recommended to use automatic option.

## ◆ Wireless Network

The screenshot shows the 'Wireless Network' configuration page for a device named 'bitlomat-test1'. The settings are as follows:

- SSID:** bitlomat-test1
- Hide SSID:** ON (OFF button is highlighted)
- Client Isolation:** ON (OFF button is highlighted)
- Security:** wpa2 (dropdown menu)
- Key Management Algorithm:** PSK (selected), EAP (radio button)
- WPA Preshared Key:** bifoloo333
- IP address:** 192.168.1.1
- Netmask:** 255.255.255.0
- MTU:** 1500
- DHCP Server:** ON (OFF button is highlighted)

At the bottom, there are two buttons: 'ADD NEW SSID' and 'SAVE'.

When the wireless interface is operated as a Home Router, the wireless interface is bridged with the LAN interface whereas the wired WAN is connected to the Internet. A different IP address must be specified for each SSID. Multiple SSIDs can be added up to 8. The SSID parameters are:

- **SSID** is the Name of the IEEE 802.11 Service Set and is used by the CPEs/clients to connect.
- **Hide SSID** will disable advertising the SSID in broadcast messages to the CPEs/clients.
- **Client Isolation** allows packets to be sent only from the external network to the CPE and vice versa, thus preventing different CPEs to communicate with each other.
- **Security** supports none, WPA, and WPA2 security options.
- **IP Address** is the private IP address of the wireless interface.
- **Netmask** is the subnet mask of the private IP address of the wireless interface.

- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.
- **DHCP Server** can be optionally enabled to automatically assign IP addresses to the CPEs/clients.

## ➤ WAN Menu

The screenshot shows the 'Home Router' interface. At the top, there are tabs for 'DASHBOARD', 'SETTINGS', 'SERVICES', and 'TOOLS'. The 'SETTINGS' tab is active. On the right side, there is a sidebar with 'WIRELESS', 'WAN', and 'SYSTEM' options. The 'WAN' option is selected. The main content area is titled 'WAN Settings'. It features a dropdown menu for 'IP Address Assignment' with options 'Static', 'DHCP', and 'PPPoE'. Below this, there are input fields for 'IP address', 'Netmask' (pre-filled with 255.255.0.0), 'Gateway' (pre-filled with 10.10.0.1), 'Primary DNS' (pre-filled with 10.10.0.1), 'Secondary DNS' (pre-filled with 8.8.8.8), and 'MTU' (pre-filled with 1500). A 'SAVE' button is located at the bottom right of the settings area.

The WAN menu is used to configure the wired WAN which is connected to the Internet according to the Provider specifications. Static IP address can be used or the unit IP address can be automatically assigned enabling DHCP. Finally, a PPPoE tunnel can be setup.

**Static IP configuration** parameters are:

- **IP Address Assignment:** the Base Station IP address can be assigned statically or using a DHCP server in the network.
- **IP Address** is the private IP address of the WAN interface.
- **Netmask** is the subnet mask of the private IP address of the WAN interface.
- **Gateway** must be set to the IP address of the local network gateway used to accessing the Internet.
- **Primary DNS** is the mandatory server which translates domain names to IP addresses.
- **Secondary DNS** is the optional server which translates domain names to IP addresses.
- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.

# Home Router

DASHBOARD
SETTINGS
SERVICES
TOOLS

WIRELESS
 **WAN**
 SYSTEM

## WAN Settings

IP Address Assignment: PPPoE

Username:

Password:

Service:

Fallback IP Address:

Fallback Netmask:

MTU:

MRU:

SAVE

Valid authorization credentials are required for the **PPPoE** connection:

- **Username** to connect to the server (must match the configured on the PPPoE server).
- **Password** to connect to the server (must match the configured on the PPPoE server).
- **DHCP Fallback IP** is used 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.
- **DHCP Fallback Netmask** is used in case the Router is placed in Dynamic IP Address mode (DHCP) and unable to obtain an IP address from a valid DHCP server, it will fall back to the static Netmask listed here.
- **MTU/MRU** is the size (in bytes) of the Maximum Transmission Unit (MTU) and Maximum Receive Unit (MRU) used for the data encapsulation while transferring it through the PPP tunnel; (MTU/MRU default value: 1492).

## 4.4 Point-to-Point Link Settings

A transparent point-to-point link consists of two units operating in **Link Master** and **Link Slave**, respectively.

### ⌘ Link Master



### ➤ Wireless Menu

The wireless menu contains all the parameters relative to the wireless interface. The menu is divided into groups:

- Radio Settings
- Wireless Network

### ◆ Radio Settings

The Radio Settings menu, shown below, is used to configure all the radio-related parameters:

- **Country Code** must be set according to the country of operation. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where the device will be used.
- **Channel Width** is the spectral width of the wireless channel. Supported widths are 5, 10, 20 and 40 MHz.

- **Frequency** is the spectral frequency of operation of the wireless channel.
- **Extension Channel** indicates the use of channel bonding that allows the radio to use two channels at once.
- **Transmission Power** is the actual radio emitted power in dBm. Different countries have different regulation. The radio automatically obeys the regulation of the selected country.
- **Distance** represents the estimated link distance.
- **Modulation Code Scheme** defines the data rate (in Mbps) at which the device should transmit wireless packets. It is recommended to use automatic option.

## ◆ Wireless Network

The screenshot shows a configuration page for a wireless network. The title is 'Wireless Network'. The settings are as follows:

- SSID:** bitlomat-test1
- Hide SSID:** ON (disabled), OFF (selected)
- Client Isolation:** ON (disabled), OFF (selected), with a help icon (?)
- Security:** wpa2 (selected from a dropdown menu, with a help icon ?)
- Key Management Algorithm:** PSK (selected), EAP
- WPA Preshared Key:** bitlomat
- SAVE** button at the bottom right.

When the wireless interface is operated as a Home Router, the wireless interface is bridged with the LAN interface. Therefore, there is no need to specify any IP address for the wireless interface.

- **SSID** is the Name of the IEEE 802.11 Service Set and is used by the CPEs/clients to connect.
- **Hide SSID** will disable advertising the SSID in broadcast messages to the CPEs/clients.
- **Client Isolation** allows packets to be sent only from the external network to the CPE and vice versa, thus preventing different CPEs to communicate with each other.
- **Security** supports none, WPA, and WPA2 security options.

## ➤ LAN Menu



# Link Master

DASHBOARD
SETTINGS
SERVICES
TOOLS

IP address

192.168.1.1

Netmask

255.255.255.0

MTU

1500

SAVE

WIRELESS

LAN

SYSTEM

The LAN menu is used to configure the wired LAN connected to private customer network. The LAN menu page settings are:

- **IP Address** is the private IP address of the LAN interface.
- **Netmask** is the subnet mask of the private IP address of the LAN interface.
- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.

## ⌘ Link Slave

# Link Slave

DASHBOARD
SETTINGS
SERVICES
TOOLS

Enable Wireless

ON OFF

Radio Settings

Country Code

UNITED STATES

Channel Width (MHz)

5

Transmission Power

17 dBm

Distance

1400 meters

Modulation Code Scheme

Auto

WIRELESS

LAN

SYSTEM

## ➤ Wireless Menu

The wireless menu contains all the parameters relative to the wireless interface. The menu is divided into groups:

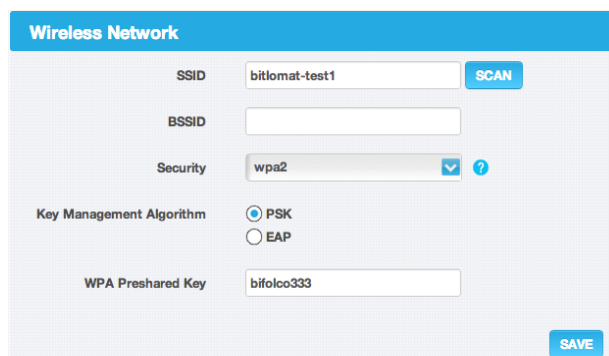
- Radio Settings
- Wireless Network

### ◆ Radio Settings

The Radio Settings menu, shown below, is used to configure all the radio-related parameters:

- **Country Code** must be set according to the country of operation. To ensure device operation follows regulatory compliance rules, please make sure to select your correct country where the device will be used.
- **Channel Width** is the spectral width of the wireless channel. Supported widths are 5, 10, 20 and 40 MHz. Please note that it's not possible to choose the frequency as that depends on the Base Station to which the CPE connects.
- **Transmission Power** is the actual radio emitted power in dBm. Different countries have different regulation. The radio automatically obeys the regulation of the selected country.
- **Distance** represents the estimated link distance.
- **Modulation Code Scheme** defines the data rate (in Mbps) at which the device should transmit wireless packets. It is recommended to use automatic option.

### ◆ Wireless Network



The screenshot shows the 'Wireless Network' configuration page. It has a blue header with the title 'Wireless Network'. Below the header, there are several input fields and buttons. The 'SSID' field contains 'bitlomat-test1' and has a 'SCAN' button next to it. The 'BSSID' field is empty. The 'Security' dropdown menu is set to 'wpa2' and has a blue question mark icon to its right. Below this, the 'Key Management Algorithm' section has two radio buttons: 'PSK' (which is selected) and 'EAP'. At the bottom, the 'WPA Preshared Key' field contains 'bifoloo333'. A 'SAVE' button is located at the bottom right of the form.

When the wireless interface is operated as a Home Router, the wireless interface is bridged with the LAN interface. Therefore, there is no need to specify any IP address

for the wireless interface.

- **SSID** is the Name of the IEEE 802.11 Service Set of the Base Station to connect to. The CPE can scan for SSIDs by clicking on the **SCAN** button.
- **BSSID** can be optionally specified as the MAC address of the Base Station to which the CPE is connecting to.
- **Security** supports none, WPA, and WPA2 security options.

## ➤ LAN Menu

The LAN menu is used to configure the wired LAN connected to private customer network. The LAN menu page settings are:

- **IP Address** is the private IP address of the LAN interface.
- **Netmask** is the subnet mask of the private IP address of the LAN interface.
- **MTU** defines the size (in bytes) of the largest protocol data unit the interface can pass on.

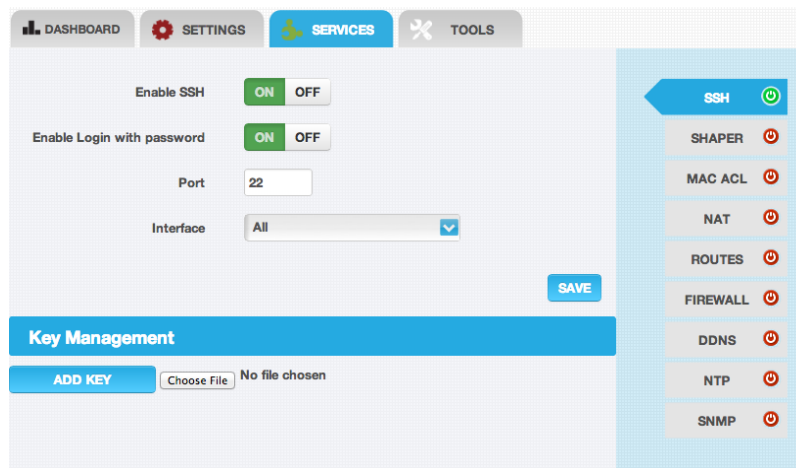


The screenshot shows the 'Link Slave' configuration interface. At the top, there are four tabs: 'DASHBOARD', 'SETTINGS' (which is active and highlighted in blue), 'SERVICES', and 'TOOLS'. Below the tabs, there are three input fields for configuration: 'IP address' with the value '192.168.1.1', 'Netmask' with the value '255.255.255.0', and 'MTU' with the value '1500'. A blue 'SAVE' button is located to the right of these fields. On the right side of the interface, there is a vertical sidebar with three options: 'WIRELESS' (with a Wi-Fi icon), 'LAN' (which is highlighted with a blue arrow and a network icon), and 'SYSTEM' (with a gear icon). Above the sidebar, there are icons for a mobile phone and a database cylinder.

## 5. Services

Through the Service page, system-wide services can be configured. Please note that not all the services listed below are available for every operating mode.

### 5.1 SSH



SSH Server can be enabled/disabled through this page.

- **Enable SSH** enables SSH access to the Bitlomat unit.
- **Enable Login with password** is used to authenticate using Administrator credentials in order to grant SSH access to the device. An Authentication Key will be required otherwise.
- **Port** is the SSH service TCP/IP port setting.
- **Interface** selector can be used to prevent from accessing the unit via SSH through certain interfaces.
- **Key Management** can be used to add a Public key file to get SSH access to the unit instead of using an admin password.

## 5.2 SHAPER

The screenshot shows the 'SERVICES' tab in a web interface. At the top, there are tabs for DASHBOARD, SETTINGS, SERVICES, and TOOLS. Under the SERVICES tab, there is a section for 'Enable Traffic Shaping' with 'ON' and 'OFF' buttons. Below this is a table with columns: Interface, Incoming, Limit (kb/s), Outgoing, and Limit (kb/s). The table has two rows: WAN and LAN bitlomat-test1. For each interface, there are 'ON' and 'OFF' buttons for Incoming and Outgoing traffic, and input fields for Limit (kb/s). A 'SAVE' button is at the bottom right. On the right side, there is a sidebar with a list of services: SSH, SHAPER, MAC ACL, NAT, ROUTES, FIREWALL, DDNS, NTP, and SNMP. The 'SHAPER' service is highlighted with a blue arrow.

Interface	Incoming	Limit (kb/s)	Outgoing	Limit (kb/s)
WAN	ON OFF	0	ON OFF	0
LAN bitlomat-test1	ON OFF	0	ON OFF	0

Traffic shaping for the cabled and wireless interfaces (per SSID) can be set up.

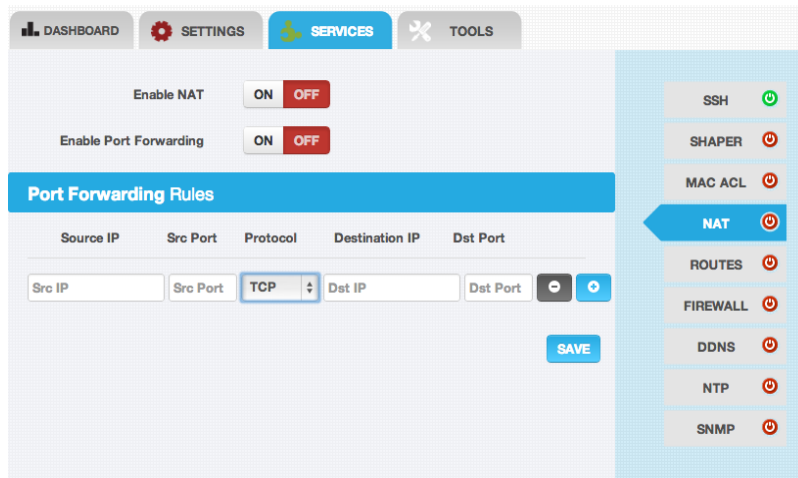
- **Enable Traffic Shaping** is used to enable/disable the service.
- The **list of the available interfaces/SSID** is reported. For each interface, incoming and outgoing traffic limits in Kb/s can be defined.

## 5.3 MAC ACL

The screenshot shows the 'SERVICES' tab in a web interface. At the top, there are tabs for DASHBOARD, SETTINGS, SERVICES, and TOOLS. Under the SERVICES tab, there is a section for 'Access Control List for bitlomat-test1'. It has an 'Enable' section with 'ON' and 'OFF' buttons. Below that is a 'Permissions' dropdown menu set to 'Deny'. At the bottom, there is a 'MAC addresses' section with a text input field labeled 'MAC address' and '+' and '-' buttons. A 'SAVE' button is at the bottom right. On the right side, there is a sidebar with a list of services: SSH, SHAPER, MAC ACL, NAT, ROUTES, FIREWALL, DDNS, NTP, and SNMP. The 'MAC ACL' service is highlighted with a blue arrow.

A MAC address Access Control List to allow or prevent specific MAC addresses from joining the wireless network. For each MAC address it is possible to specify the behavior rule (deny or allow).

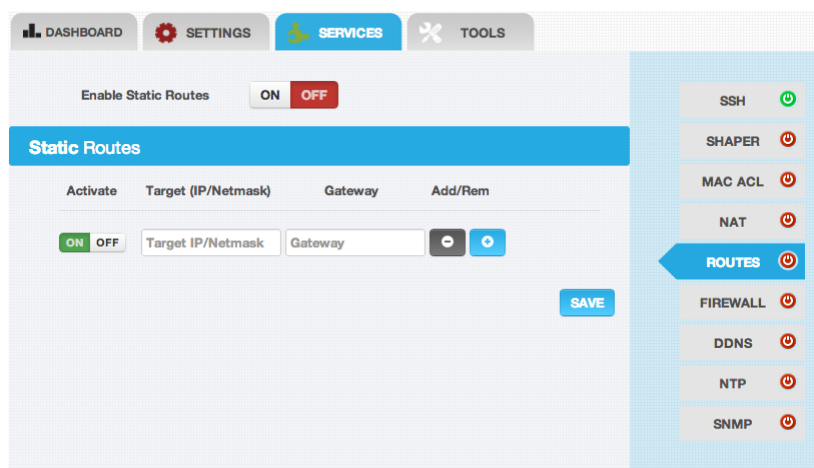
## 5.4 NAT and Port Forwarding



Network Address Translation (NAT) can be enabled for the unit and is implemented using the masquerade type firewall rules. NAT firewall entries are stored in the iptables NAT table.

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.

## 5.5 ROUTES



Through the **Static Routes** page, it is possible to add static routing rules to specify e.g. that a specific target IP address (es) passes through a determined gateway.

For each entry, a valid Target Network IP/Netmask and Gateway IP can be specified. Check the “ON” checkbox, in order to enable this rule.

## 5.6 FIREWALL

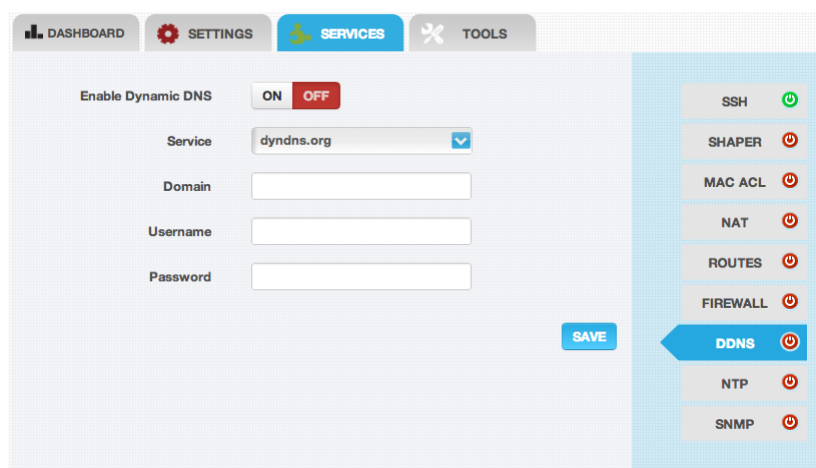
Firewall rules can be configured, enabled or disabled.

Firewall entries can be specified by using the following criteria:

- **Rule Number** indicates the priority of the firewall rule. The smaller the number, the higher the priority.
- **Action** allows two specific firewall rules: ALLOW or DENY. By enabling “ALLOW”, the packets can pass the firewall unmodified. When choosing “DENY”, the packets are denied passage through the firewall and no response is sent.
- **Input Interface** specifies where filtering of the incoming/passing-through packets is processed;
- **Protocol** sets which particular L3 protocol type (IP, ICMP, TCP, UDP) should be filtered;
- **Source IP/Netmask** is the source IP of the packet (specified within the packet header), usually it is the IP of the host system that 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 that sends the packets;

- **Destination IP/Netmask** 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.
- **Not operators** can be enabled 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).

## 5.7 DDNS



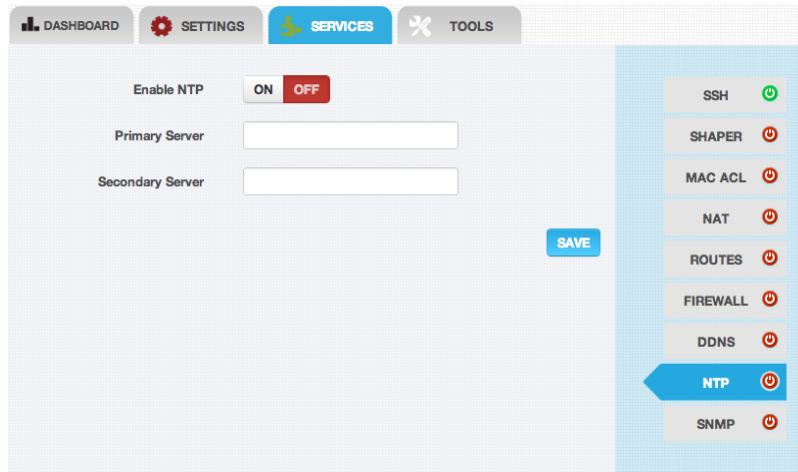
**Enable Dynamic DNS** enables Dynamic DNS service. Dynamic DNS allows real-time notification to the DNS Server of any changes occurring in the device's IP setting, therefor allowing access to the device through a Domain Name even if the device's IP address has changed.

- **Service** selector is used to point the DDNS Bitlomat unit client to an online DDNS provider.
- **Domain** defines the Dynamic DNS Host Name used to access the unit from remote as specified by the online DDNS providers.
- **Username** defines the Dynamic DNS Username.



- **Password** defines the Dynamic DNS password. Check “show” to display the password.

## 5.8 NTP



The screenshot shows the 'SERVICES' tab in the Bitlomat interface. On the left, there are three fields: 'Enable NTP' with a toggle switch set to 'OFF', 'Primary Server' with an empty text box, and 'Secondary Server' with an empty text box. A blue 'SAVE' button is located to the right of these fields. On the right side of the interface, there is a vertical list of services with status icons: SSH (green power icon), SHAPER (red power icon), MAC ACL (red power icon), NAT (red power icon), ROUTES (red power icon), FIREWALL (red power icon), DDNS (red power icon), NTP (blue power icon, highlighted with a blue arrow), and SNMP (red power icon).

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 system time of the Bitlomat units.

**Enable NTP** will enable NTP client.

It is possible to specify the IP address or domain name of a **Primary** and a **Secondary NTP Server**.

## 5.9 SNMP

The screenshot shows a web-based configuration interface for a network device. At the top, there are four tabs: DASHBOARD, SETTINGS, SERVICES, and TOOLS. The SERVICES tab is currently selected. The main content area is divided into two sections. The left section is for SNMP configuration, featuring a toggle switch for 'Enable SNMP' (currently set to 'OFF'), and three text input fields for 'Community', 'Contact', and 'Location'. A 'SAVE' button is located at the bottom right of this section. The right section is a sidebar containing a list of services with status indicators: SSH (green circle), SHAPER (red circle with a slash), MAC ACL (red circle with a slash), NAT (red circle with a slash), ROUTES (red circle with a slash), FIREWALL (red circle with a slash), DDNS (red circle with a slash), NTP (red circle with a slash), and SNMP (red circle with a slash). The SNMP service is highlighted with a blue arrow pointing to it.

Simple Network Monitor Protocol (SNMP) is used in network management systems to monitor network devices for conditions that require administrative attention. The SNMP agent allows communication to SNMP manage applications for network provisioning.

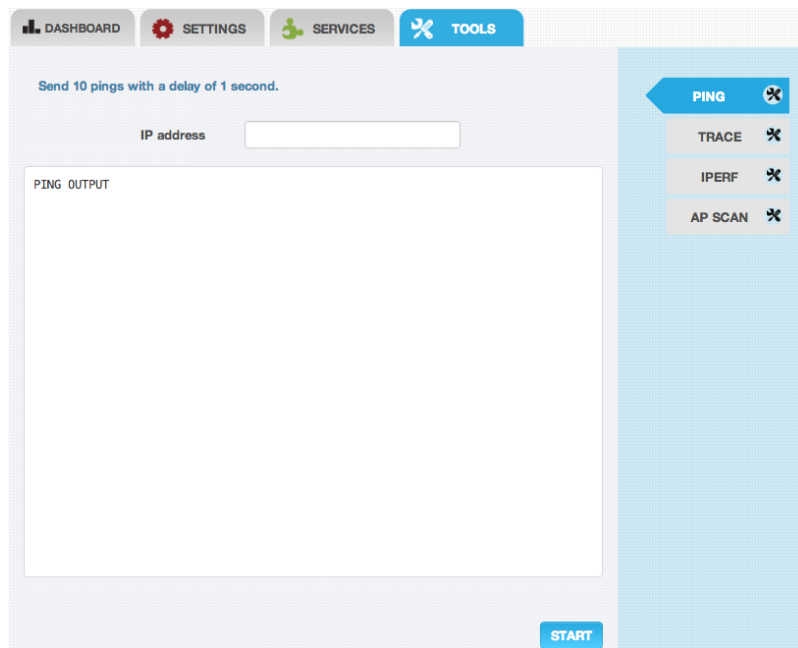
- **Enable SNMP** control will enable SNMP Agent.
- **SNMP Community** specifies SNMP community string. It is required to authenticate access to MIB objects and functions as embedded password. The device supports a Read-only community string that gives read access to authorized management servers to all the objects in the MIB. The default SNMP Community is "public".
- **Contact** specifies the identity or the contact who should be contacted in case a emergency situation arise.
- **Location** specifies the physical location of the device.

## 6. Tools

The tools page contains a number of useful tool for testing or troubleshooting.

### 6.1 PING

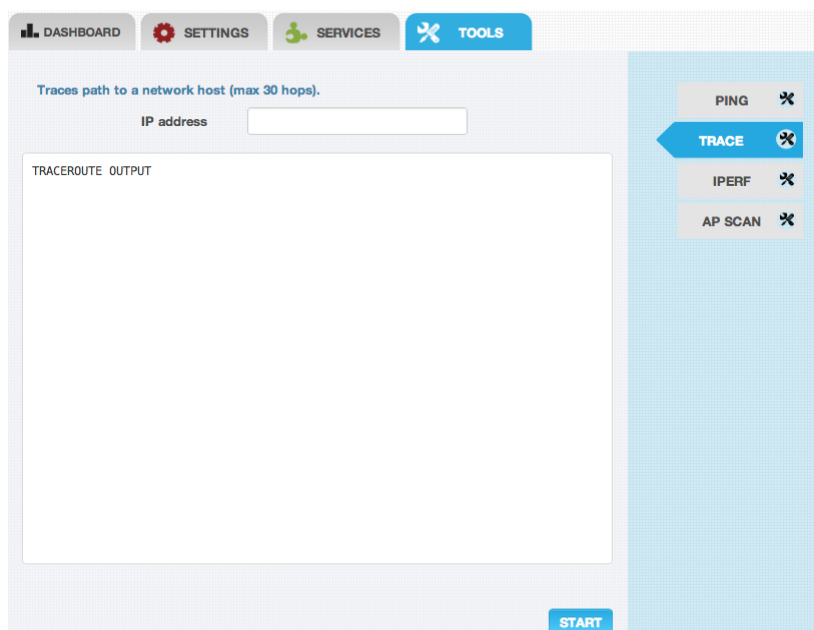
Ping commands can be run to test the reachability of a specific **IP address**.



The screenshot shows a web dashboard with a navigation bar at the top containing 'DASHBOARD', 'SETTINGS', 'SERVICES', and 'TOOLS'. The 'TOOLS' tab is selected. The main area is titled 'Send 10 pings with a delay of 1 second.' and features an 'IP address' input field. Below the input field is a large text area labeled 'PING OUTPUT'. A 'START' button is located at the bottom right of the main area. On the right side, there is a vertical sidebar with buttons for 'PING', 'TRACE', 'IPERF', and 'AP SCAN', each with a small icon to its right. The 'PING' button is highlighted with a blue arrow pointing to it.

### 6.2 TRACE

Traceroute commands can be run to verify the path to reach a specific IP address.



The screenshot shows the same web dashboard as the previous image, but with the 'TRACE' button highlighted in the sidebar. The main area is titled 'Traces path to a network host (max 30 hops).' and features an 'IP address' input field. Below the input field is a large text area labeled 'TRACEROUTE OUTPUT'. A 'START' button is located at the bottom right of the main area. The sidebar buttons are 'PING', 'TRACE', 'IPERF', and 'AP SCAN', with 'TRACE' being the active selection.

## 6.3 IPERF

Iperf is a commonly used network testing tool that can create UDP data streams and measure the throughput of a network that is carrying them. The tool can be used by specifying the destination **IP address** (Iperf server) and the **Rate** in kbps transmitted during the test. Please note that the Iperf tool is CPU intensive. Therefore, the result might not be accurate especially when testing with high rates.

The screenshot shows a web dashboard with a navigation bar at the top containing 'DASHBOARD', 'SETTINGS', 'SERVICES', and 'TOOLS'. The 'TOOLS' tab is selected. The main content area for the IPERF tool includes a description: 'Perform network throughput test sending UDP packets at the specified rate for 10 seconds.' Below this, there are input fields for 'IP address' and 'Rate (kbps)'. A large text area labeled 'IPERF OUTPUT' is provided for results. A 'START' button is located at the bottom right of the main area. On the right side, a vertical sidebar contains buttons for 'PING', 'TRACE', 'IPERF' (which is highlighted with a blue arrow), and 'AP SCAN', each with a close icon.

## 6.4 AP SCAN

The AP SCAN tool can be used to search for Access Points/Base Station SSIDs in the area. The tool will scan the frequencies and report back the list of SSIDs found.

The screenshot shows the same web dashboard as the previous image, but with the 'AP SCAN' tool selected. The main content area has a description: 'Scan for APs.' and a large empty text area for results. A 'START' button is at the bottom right. The right sidebar shows the same navigation buttons, but 'AP SCAN' is now highlighted with a blue arrow, while 'IPERF' is no longer highlighted.

# APPENDIX A

## FCC Notices

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

### CAUTION:

Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

## RF exposure warning

This equipment must be installed and operated in accordance with provided instructions and the antenna(s) used for this transmitter must be installed to provide a separation distance of at least 60 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter. End-users and installers must be provide with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

This device is operation in 5.15 – 5.25GHz frequency range, then restricted in indoor use only, Outdoor operations in the 5150~5250MHz is prohibit.

The availability of some specific channels and / or operational frequency bands are country dependent and are firmware programmed at factory to match the intended destination. The firmware setting is not accessible by the end user.

This device is Master equipment, the transmission is disabled in the 5600-5650MHz band.

## **Industry Canada**

### **Radio Frequency (RF) Exposure Information**

The radiated output power of the Wireless Device is below the Industry Canada (IC) radio frequency exposure limits. The Wireless Device should be used in such a manner such that the potential for human contact during normal operation is minimized.

This device has also been evaluated and shown compliant with the IC RF Exposure limits under mobile exposure conditions. (antennas are greater than 20cm from a person's body).

### **Informations concernant l'exposition aux fréquences radio (RF)**

La puissance de sortie émise par l'appareil de sans fil est inférieure à la limite d'exposition aux fréquences radio d'Industry Canada (IC). Utilisez l'appareil de sans fil de façon à minimiser les contacts humains lors du fonctionnement normal.

Ce périphérique a également été évalué et démontré conforme aux limites d'exposition aux RF d'IC dans des conditions d'exposition à des appareils mobiles (les antennes se situent à moins de 60 cm du corps d'une personne).