DLB APC v5.95

User's Guide

Revision 1.0
9 October 2014

Copyright

Notice

Deliberant reserves the right to change specifications without prior notice.

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. Deliberant shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from Deliberant.

Trademarks

Deliberant logo is trademark of Deliberant LLC.

All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Contents

About this Guide

Prerequisite Skills and Knowledge

To use this document effectively, you should have a working knowledge of Local Area Networking (LAN) concepts and wireless Internet access infrastructures.

Conventions Used in this Document

The following typographic conventions and symbols are used throughout this document:

ℹ️	Additional information that may be helpful but which is not required.
❗	Important information that should be observed.
bold	Menu commands, buttons, input fields, links, and configuration keys are displayed in bold
italic	References to sections inside the document are displayed in italic.
`code`	File names, directory names, form names, system-generated output, and user typed entries are displayed in constant-width type

Abbreviation List

Abbreviation	Description
ACL	Access Control List
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
CRC	Cyclic Redundancy Check
DHCP	Dynamic Host Control Protocol
EAP	Extensible Authentication Protocol
GHz	Gigahertz
GMT	Greenwich Mean Time.
GUI	Graphical User Interface
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
ISP	Internet Service Provider
IP	Internet Protocol
LAN	Local Area Network
LED	Light-Emitting Diode

Abbreviation	Description
MAC	Media Access Control
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple Input, Multiple Output
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NAT	Network address translation – translation of IP addresses (and ports)
PC	Personal Computer
PDA	Personal Digital Assistant
PTP	Point To Point
PTMP	Point To Multi Point
PSK	Pre-Shared Key
QoS	Quality of Service
PEAP	Protected Extensible Authentication Protocol
RSSI	Received Signal Strength Indication – received signal strength in mV, measured on BNC outdoor unit connector
RX	Receive
SISO	Simple Input, Simple Output
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TTLS	Tunneled Transport Layer Security (EAP-TTLS) protocol
TX	Transmission
UDP	User Datagram Protocol
UAM	Universal Access Method
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

First Connection to the APC

The default product address is `192.168.2.66`.

> The default administrator login settings are:
> Login: **admin**
> Password: **admin01**

Follow the steps for first connection to the device:

Step 1.   Connect an Ethernet cable between your computer and the AP.

Step 2.   Make sure your computer is set to the same subnet as the AP, i.e. 192.168.2.150

Step 3.   Start your Web browser.

Step 4.   Each devices uses following default settings:

- WAN IP: **192.168.2.66**
- Subnet mask: **255.255.255.0**
- Username: **admin**
- Password: **admin01**

The initial login screen looks as follow:
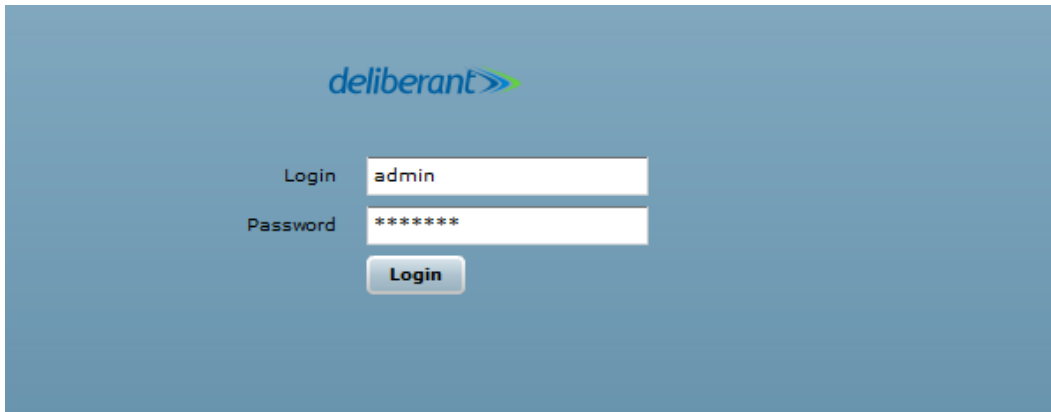
Step 5.   **Confirm the disclaimer of the APC.** According to the chosen country the regulatory domain settings may differ. You are not allowed to select radio channels and RF output power values other the permitted values for your country and regulatory domain.
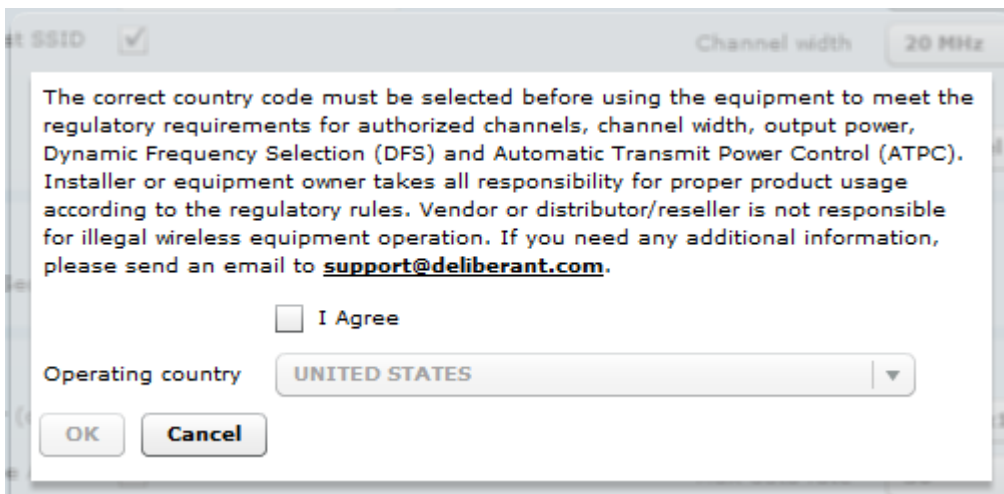
Step 6.   After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

Network Operation Modes

The device can operate as transparent Bridge or Router.

Bridge Mode

The device can act as a wireless network bridge and establish wireless links with other APs. In this mode all LAN port and Wireless interface will be a part of the Bridge.
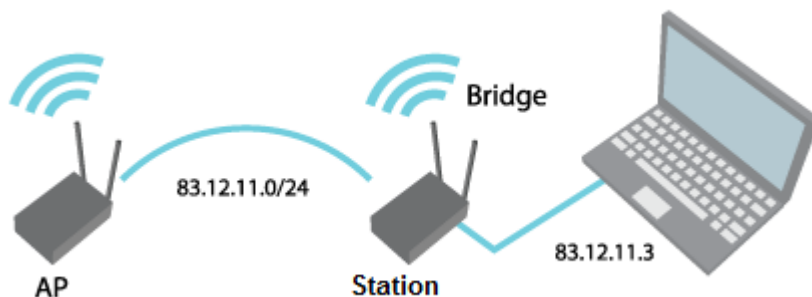
Figure 1 – Bridge Mode

With a Bridge, all connected computers are in the same network subnet. The only data that is allowed to cross the bridge is data that is being sent to a valid address on the other side of the bridge.

Router Mode

In router mode the device will receive internet through WAN port and will share it to the LAN ports that will be separated with a different IP range. The type of connection to the WAN interface can be made by Static IP, DHCP client or PPPoE client.
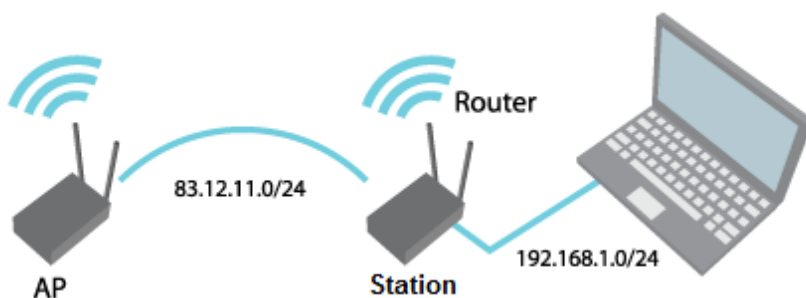
Figure 2 – Router Mode

When device operates in Router mode, the traffic coming on wired interface and going out on wireless interface can be masqueraded by enabling NAT. NAT allows a set of station's clients to invisibly access the Internet via the wireless station. To other clients on the Internet, all this outgoing traffic will appear to be from the APC device itself.

General Device Operation

Web Management Structure

The main web management menu is displayed after successfully login into the system (see the figure below). From this menu all essential configuration pages are accessed. The active menu tab is displayed in a different color:


Figure 3 – AP Web Management Menu

By default the **Status | Information** menu is activated where the main device information is displayed.

The APC web management menu has the following structure:

Status

> **Information** – displays general information and of the device.
>
> **Network** – displays network statistics of the device.
>
> **Wireless** – displays information about connected stations on each wireless interface (only on AP wireless mode).
>
> **Graphs** – graphically displays current Wireless and Ethernet data traffic.
>
> **Routes** – displays unit's route table.
>
> **ARP** – displays ARP table.

Configuration

> **Network** – to configure network mode, Ethernet speed, IP settings, management and data VLANs, DHCP, PPPoE.
>
> **Wireless** – specify wireless mode (AP, Station, Station WDS, iPoll AP, iPoll Station), country, SSID, IEEE mode, channel configuration, security and advanced radio settings.
>
> **Virtual AP** – create and setup virtual AP (only in AP wireless mode).
>
> **Wireless ACL** – access control by MAC address (only in AP and IPoll AP wireless modes).
>
> **Traffic shaping –** download and upload traffic control.
>
> **Port forwarding** – port forwarding rules (only in router network mode for AP and IPoll AP).
>
> **Static routes** – static route rules (only in router network mode for AP and IPoll AP).

Services

> **WNMS** – set WNMS server/collector URL allowing remote device configuration and monitoring.
>
> **System Alerts** – set alerts which can be sent via SNMP Traps or/and SMTP notifications.
>
> **SNMP** – SNMP service settings allowing remote device monitoring.
>
> **Clock/NTP** – set device date manually or enable and configure NTP service.
>
> **SSH** – control SSH connection.
>
> **HTTP** – control HTTP connection.
>
> **Autodiscovery** – control device autodiscovery function (only on Station, Station WDS and IPoll Station wireless modes).
>
> **Ping watchdog** – self-recover feature enables the APC unit to reboot itself in case the network connection with the specified host is lost.
>
> **DHCP proxy** – enables the AP to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources.

System

> **Administration** – change password, reboot, restore factory default settings, backup/restore configuration, troubleshooting file support.
>
> **Log** – view device log, set system log forwarding settings.
>
> **LED** – control operation of LEDs.
>
> **Firmware upgrade** – upgrade device firmware.

Tools

> **Antenna alignment** – measure received signal quality of the wireless link to align antenna in the best direction.
>
> **Site Survey** – information about other wireless networks in the local area.
>
> **Delayed reboot** – setup delayed reboot for APC unit.
>
> **Ping** – perform ping command.
>
> **Traceroute** – perform graphical traceroute command.
>
> **Spectrum analyzer** – check the signal strength on available channels.
>
> **Link test** – check the quality of the established link.

Appling and Saving Configuration Changes

There are three general buttons located on the right top corner of the WEB GUI allowing managing device configuration:

Apply – if pressed new configuration settings are applied instantly. It will take few seconds and the device will be running with new settings. It should be noted that pressing Apply button settings are not written to the permanent memory. Therefore, if the device is rebooted it will start with old configuration settings.

Discard – if pressed parameter changes are discarded. It should be noted that if Apply or Save&Apply is pressed it is not possible to discard changes.

Save&Apply – if pressed new configuration settings are applied instantly and written to the permanent memory.

> It is not required to press **Apply** or **Save&Apply** in every Web GUI tab. The device remembers all changes made in every tab and after action button is used, all changes will be applied.

Configuration Guide

This document contain product's powerful web management interface configuration description allowing setups ranging from very simple to very complex.

Status

Information

The Information page displays a summary of status information of your device. It shows important information for the APC operating mode, network settings.

Figure 4 – Device Information

System information – displays general information about the device.

Wireless information – displays general information about the wireless connection. The wireless information will differ on Access Point, Station, iPoll wireless modes:

- **AP mode** – displays access point operating information, number of connected clients and SSID details (including VAPs).
- **Station mode** – displays settings at which the station is connected to the access point.
- **iPoll AP –** displays iPoll access point operating information, number of connected wireless stations.
- **iPoll Station** – displays settings at which the iPoll wireless station is connected to the iPoll AP.

Ethernet – displays status of Ethernet ports (UP/Down).

SSID details – displays short information (SSID and security type) of wireless interfaces, including VAPs

Network mode – displays short summary about current network configuration (bridge or router).

Network

The **Network** sections displays statistics of the network interfaces and DHCP leases (depending on network mode):

Figure 5 – Network Statistics

Interface – displays the interface name. The SSID name is displayed in the brackets near the radio interface (and VAPs).

IP address – displays the IP address of the particular interface.

MAC – displays the MAC address of the particular interface.

Received – displays the number of received packets.

RX errors – displays the number of the RX errors.

Transmitted – displays the number of transmitted packets.

TX errors – displays the number of the TX errors.

DHCP leases – table displays information about leased DHCP addresses. This table appears only on AP which acts as Router and has DHCP server enabled.

Wireless

ℹ️ **Status Wireless** section is not available if APC is operating in Station wireless mode. In this case all necessary information about wireless connection with AP unit will be under *Information* section.

The Wireless statistics displays the receive/transmit statistics between AP and successfully associated wireless clients:
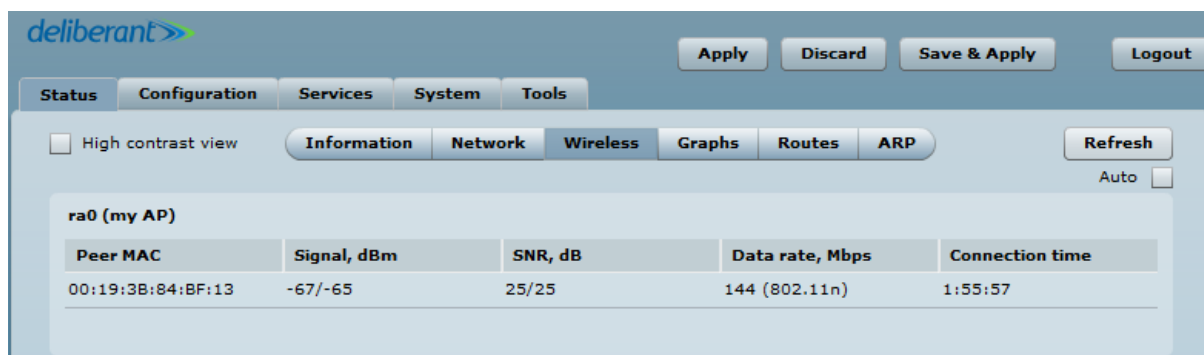
Figure 6 – Access Point's Wireless Statistics

In case the access point has more than one wireless interface (VAPs), the appropriate number of tables with information about connected wireless clients will be displayed.

Peer MAC – displays MAC address of the successfully connected wireless client.

Signal – indicates the signal strength of the access point main and auxiliary antennas that the station communicates with displayed dBm.

Noise – displays the noise level in dBm.

IEEE mode – displays the IEEE mode at which the access point communicates with the particular station.

Data rate – displays the data rate at which the access point communicates with the particular station.

Connection time – displays the duration of the session.

Graphs

The Graphs page displays real-time data traffic on the Ethernet and Wireless interfaces. The graphs are regularly updated in 5 seconds.
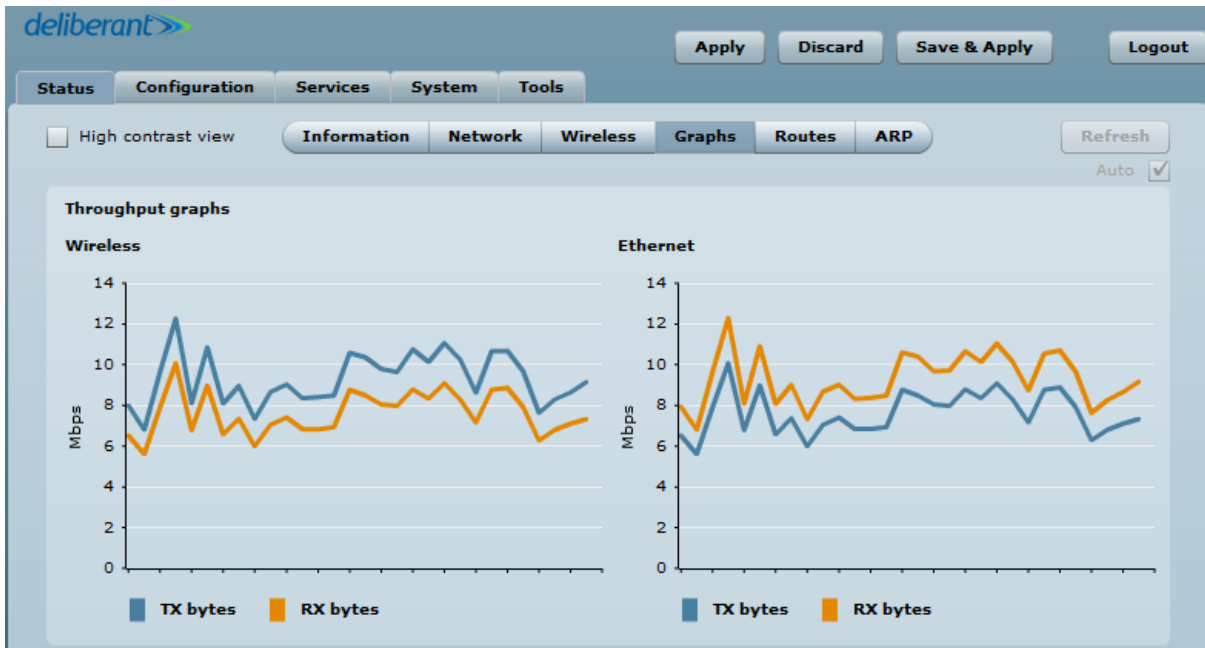
Figure 7 – APC Data Traffic Graphs

Routes

The **Routes** page displays the routing table for each interface:
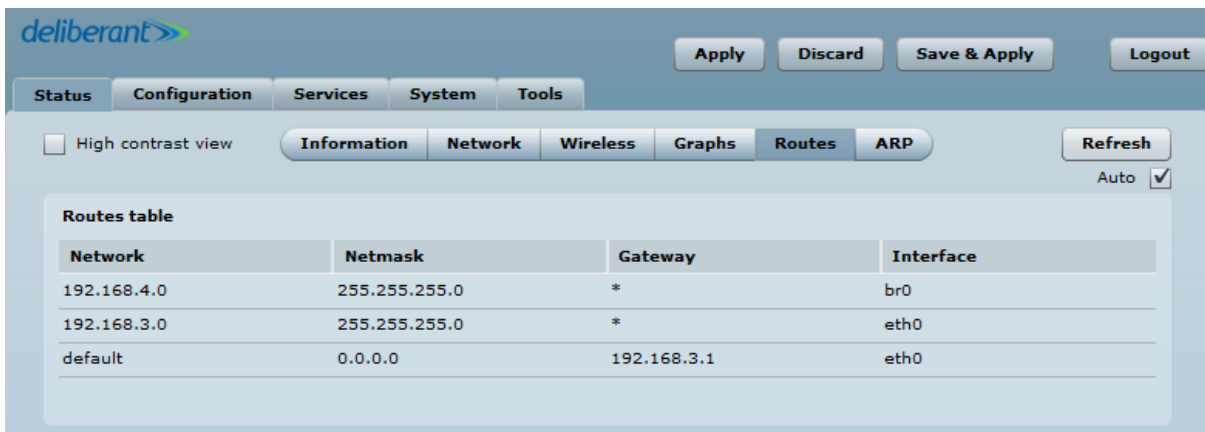
Figure 8 – Routes Table

ARP

The **ARP** page displays the ARP (Address Resolution Protocol) table currently recorded on the device. Use **Refresh** button to reload ARP table results.
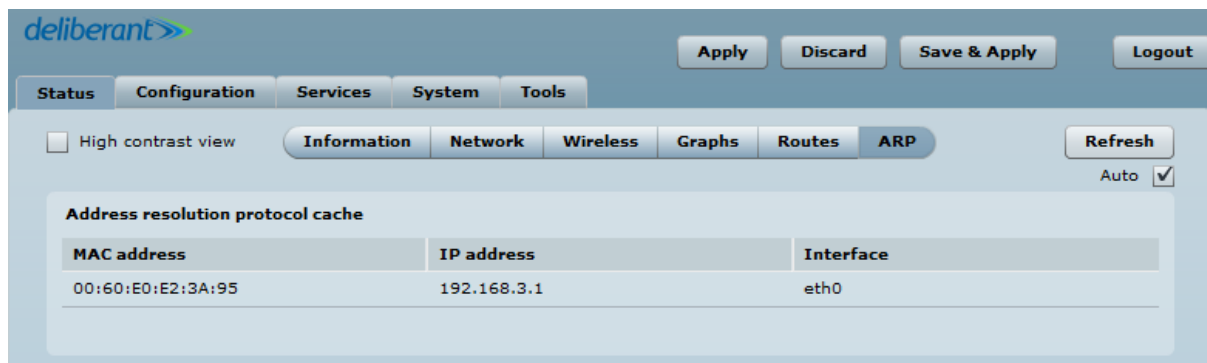
Figure 9 – ARP Table Records

Configuration

Network

The **Configuration | Network** page allows you to control the network configuration and settings of the device. First, the device operation mode must be defined to work as a bridge or router. The content of the window varies depending on your selection:

Figure 10 – Network Mode Options

Network mode – choose the device operating mode [bridge/router]

▪ **Bridge** – in this mode the device works as transparent bridge interconnecting wireless network and LAN port.
▪ **Router** – in this mode the device works as router between wireless network and all LAN ports.

Network settings will vary according to the selected Network mode. The Bridge mode allows configuring device LAN IP settings, while the Router mode requires more parameters such as LAN network settings, WAN network settings, LAN DHCP settings.

Bridge Mode

Port forwarding and **Static routes** are not available on Bridge mode.

When device is configured to operate in Bridge mode, only device LAN settings should be configured on the **Network** page:
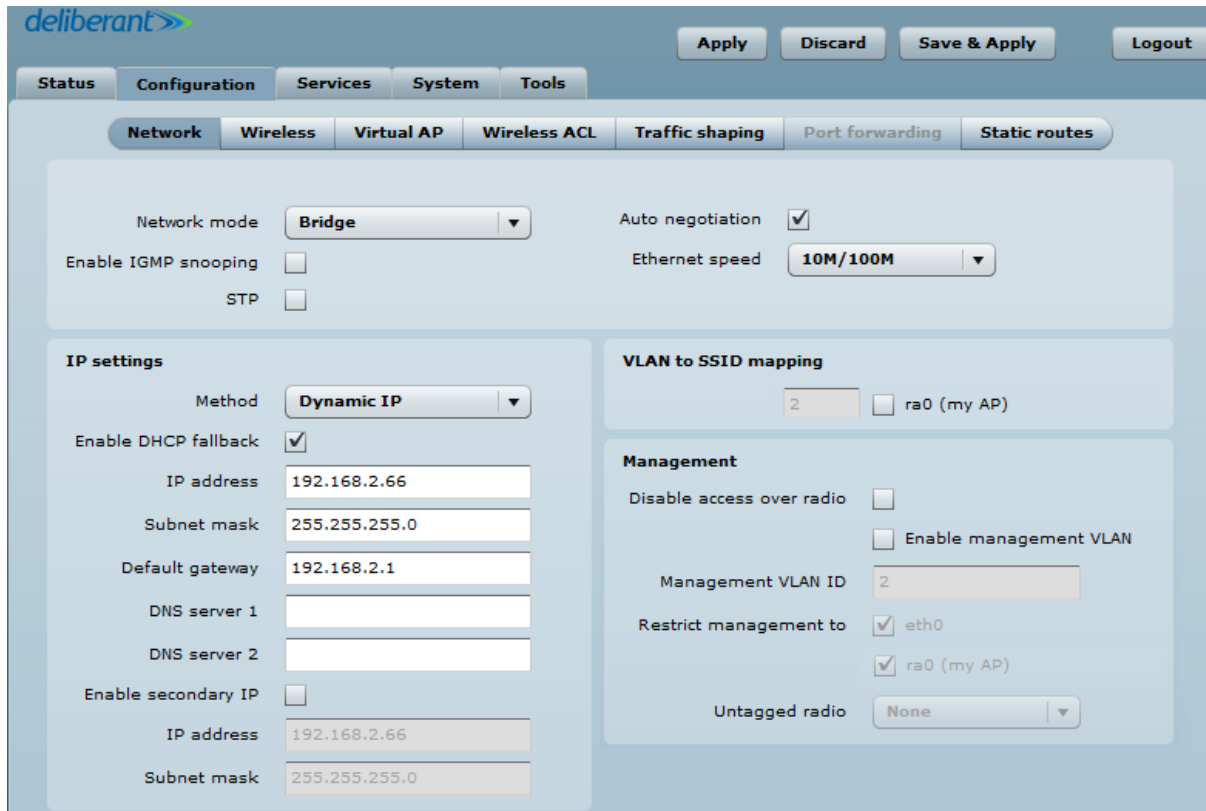
Figure 11 – Bridge Mode Settings

IGMP snooping (only on AP or iPoll Bridge modes) – when enabled AP will passively snoop on IGMP Report and Leave packets transferred between it's clients and IP Multicast hosts. It checks IGMP packets passing through it, picks out the group registration information and generates internal L2 MAC forwarding table. Then it forwards multicast traffic using unicast packets directed according to forwarding table.

STP - select to enable Spanning Tree Protocol (STP). If STP enabled, it provides a single path between network devices, avoiding and eliminating loops.

Auto negotiation - select the auto negotiation which advertise and negotiate Ethernet link duplex configuration (half/full) for the highest possible data rates.

Ethernet speed – select the Ethernet link speed and the duplex mode (if ETH auto negotiation is disabled) of the particular Ethernet port.

IP Settings

> When assigning IP address make sure that the chosen IP address is unused and belongs to the same IP subnet as your wired LAN, otherwise you will lose the connection to the device from your current PC. If you enable the DHCP client, the browser will lose the connection after saving, because the IP address assigned by the DHCP server is not predictable.

Method – specify IP reception method: IP addresses can either be retrieved from a DHCP server or configured manually:

- **Static IP** – the IP address must be specified manually.
- **Dynamic IP** – the IP address for this device will be assigned from the DHCP server. If DHCP server is not available, the device will try to get an IP. If has no success, it will use pre-configured fallback IP address. The fallback IP settings can be changed to custom values.

IP Address – specify IP address for device

Subnet mask – specify a subnet mask for device.

Default gateway – specify a gateway IP address for device.

DNS server – specify the Domain Naming Server.

Enable IP alias – specify the alternative IP address and the netmask for APC unit management.

VLAN to SSID Mapping

Virtual Local Area Networks (VLANs) are logical groupings of network resources.
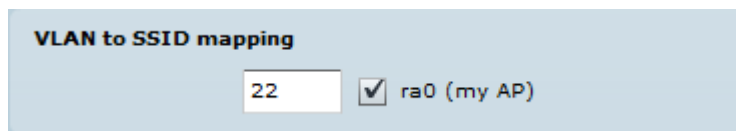
Figure 12 - VLAN to SSID Mapping

VLAN to SSID mapping – specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices that associate using the particular SSID will be grouped into this VLAN.

Network Management

> Available only on Bridge network mode.

> When you specify a new management VLAN, your HTTP connection to the device will be lost. For this reason, you should have a connection between your management station and a port in the new management VLAN or connect to the new management VLAN through a multi-VLAN router.
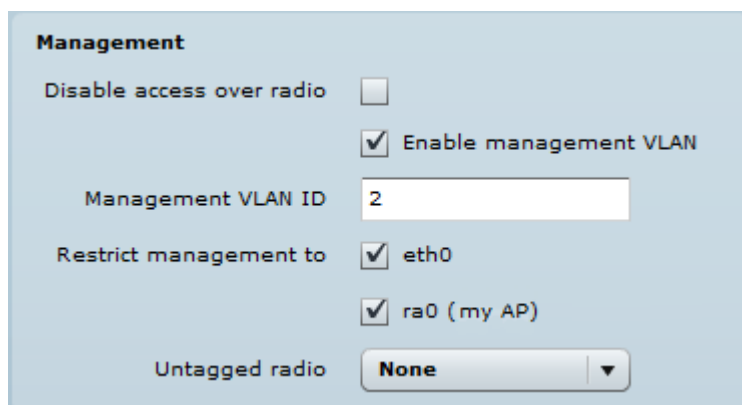
Figure 13 – Network Management Settings

Disable access over radio - select to disable wireless administrative access. For security reasons, it is recommended disable wireless access and instead require a physical network connection using an Ethernet cable for administrative access to APC.

Access to the AP for management purposes can further be limited using VLAN tagging. By defining Management VLAN, the device will only accept management frames that have the appropriate Management VLAN ID. All other frames using any management protocol will be rejected.

Enable management VLAN – select to enable a VLAN tagging for management traffic.

Management VLAN ID – specify the VLAN ID [2-4095]. When device interfaces are configured with a specific VLAN ID value, only management frames that matching configured VLAN ID will be accepted by device.

Restrict management to interfaces – select interfaces that will be restricted with management VLAN.

Untagged radio – select the interface for untagged traffic.

Router Mode

This section allows customizing parameters of the Router to suit the needs of network, including ability to use the built-in DHCP server. When device is configured to operate as Router, the following sections should be specified: WAN network settings, LAN network settings and LAN DHCP settings.

Figure 14 – Router Settings

Enable NAT – select to enable NAT (Network Address Translation), that functions by transforming the private IP address of packets originating from hosts on your network so that they appear to be coming from a single public IP address and by restoring the destination public IP address to the appropriate private IP address for packets entering the private network, the multiple PCs on your network would then appear as a single client to the WAN interface.

Enable IGMP snooping – if enabled, the APC will passively snoop on IGMP Report and Leave packets transferred between it's clients and IP Multicast hosts. It checks IGMP packets passing through it, picks out the group registration information and generates internal L2 MAC forwarding table. Then it forwards multicast traffic using unicast packets directed according to forwarding table.

Enable IGMP proxy - enables APC router to issue IGMP host messages on behalf of hosts that the APC router discovered through standard IGMP interfaces. The APC router acts as a proxy for its hosts.

Auto negotiation - select the auto negotiation which advertise and negotiate Ethernet link duplex configuration (half/full) for the highest possible data rates.

Ethernet speed – select the Ethernet link speed and the duplex mode (if ETH auto negotiation is disabled) of the particular Ethernet port.

WAN Settings

WAN network settings include settings related to the WAN interface. The access type of the WAN interface can be configured as: Static IP, Dynamic IP, PPPoE client.

WAN mode – choose **Static IP** to specify IP settings for device WAN interface:

Figure 15 – Router WAN Settings: Static IP

MAC address – specify the clone MAC address if required. The ISPs registers the MAC address of the router, and allows only that MAC address to connect to their network. In such case if there is need to change hardware (router), you need to notify your ISP about MAC address change, or simply set the router's MAC address to the MAC address of the previously router/computer.

VLAN ID – specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices that associate using the particular SSID will be grouped into this VLAN.

WAN mode – choose Static IP to specify IP settings manually. This option needs parameters listed below:

IP address – specify static IP address.

Subnet mask – specify a subnet mask.

Default gateway – specify a gateway.

DNS server – specify primary and/or secondary DNS server

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

WAN mode – choose **Dynamic IP** to enable DHCP client on the WAN side. This option does not need any parameters:

Figure 16 – Routers WAN Settings: Dynamic IP
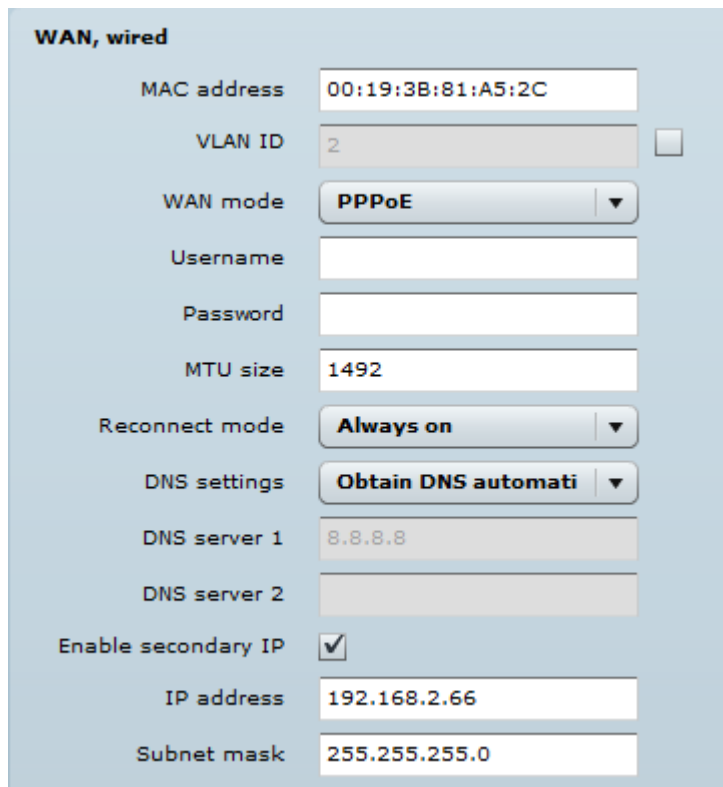
MAC address – specify the clone MAC address if required. The ISPs registers the MAC address of the router, and allows only that MAC address to connect to their network. In such case if there is need to change hardware (router), you need to notify your ISP about MAC address change, or simply set the router's MAC address to the MAC address of the previously router/computer.

VLAN ID – specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices that associate using the particular SSID will be grouped into this VLAN.

DHCP fallback setting – specify IP address, Subnet mask, Default gateway and optionally DNS server for DHCP fallback. In case the APC unit will not get the IP address from the DHCP, the specified fallback IP settings will be used.

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

WAN mode – choose PPPoE to configure WAN interface to connect to an ISP via a PPPoE:

Figure 17 – Routers WAN Settings: PPPoE client

MAC address – specify the clone MAC address if required. The ISPs registers the MAC address of the router, and allows only that MAC address to connect to their network. In such case if there is need to change hardware (router), you need to notify your ISP about MAC address change, or simply set the router's MAC address to the MAC address of the previously router/computer.

VLAN ID – specify the VLAN ID for traffic tagging on required radio interface [2-4095]. The Station devices that associate using the particular SSID will be grouped into this VLAN.

User name – specify the user name for PPPoE.

Password – specify the password for PPPoE.

MTU – specify the MTU (Maximum Transmission Unit). The default value is 1500 bytes.

Reconnect mode – specify PPPoE reconnection mode:
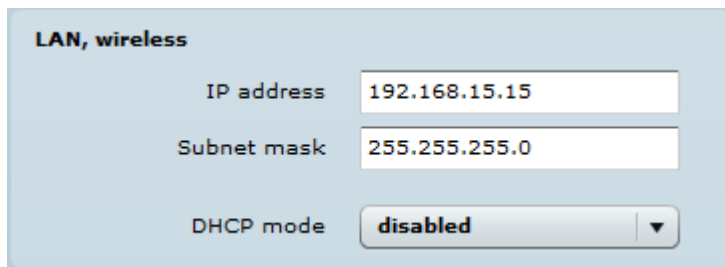
▪ **Always on** – PPPoE connection automatically starts without timeout. The router will keep trying to bring up the connection if it is disconnected for some reason.
▪ **On demand** – the PPPoE connection automatically starts when there is outbound traffic to the Internet, and it automatically terminates if the connection is idle based on the value specified in the **Idle time** [1-65535] setting.

DNS settings – allows selecting if automatically assigned or alternative DNS servers should be used.

Enable secondary IP – specify the alternative IP address and the netmask for APC unit management.

LAN Network Settings

LAN network settings includes settings related to the LAN interface.
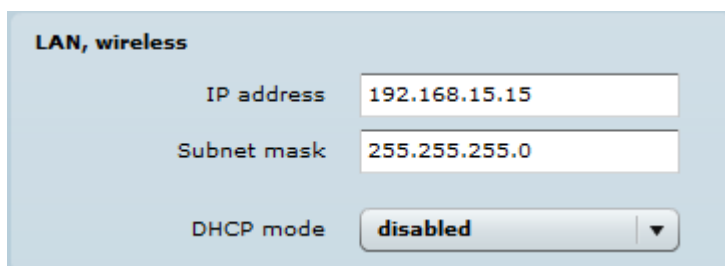
Figure 18 – Router LAN Settings

IP address – specify the IP address of the device LAN interface.

Subnet mask – specify the subnet mask of the device LAN interface.

LAN DHCP Settings

DHCP mode – choose disabled to disable DHCP on LAN interface.
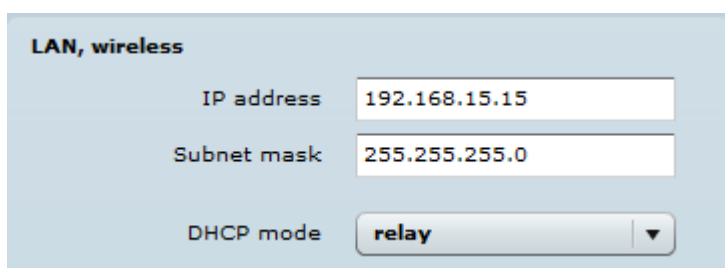
Figure 19 – Router LAN Settings: DHCP Disabled

DHCP mode – choose relay to enable DHCP relay. The DHCP relay forwards DHCP messages between subnets with different sublayer broadcast domains.
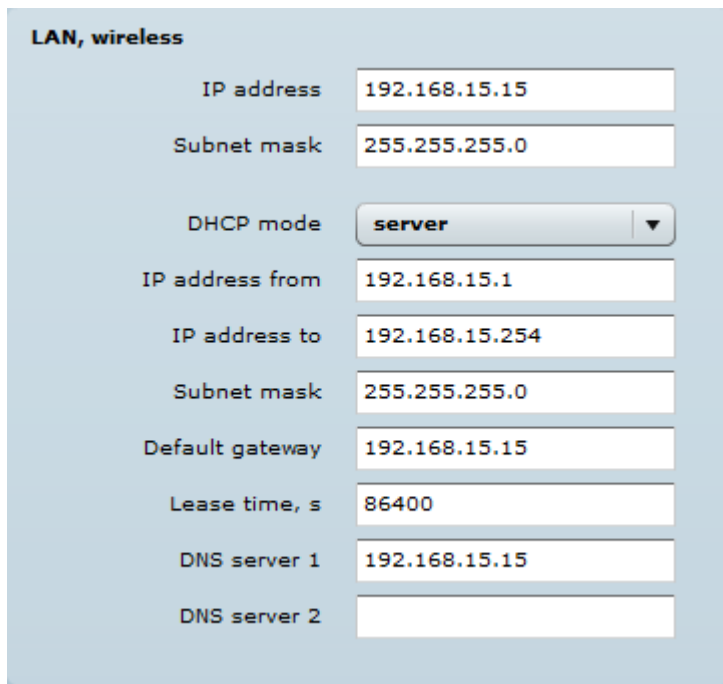
Figure 20 – Router LAN Settings: DHCP Relay

DHCP mode – choose server to enable DHCP server on LAN interface.

Figure 21 – Router LAN Settings: DHCP Server

IP address from – specify the starting IP address of the DHCP address pool.

IP address to – specify the ending IP address of DHCP address pool.

Subnet mask – specify the subnet mask.

Default gateway – specify DHCP gateway IP address.

Lease time – specify the expiration time in seconds for the IP address assigned by the DHCP server.

DNS server – specify the DNS server IP address.

Wireless

The Wireless tab is divided in three sections: Basic, Security and Advanced configuration sections. The Basic section contains all parameters that required to configure in order have working wireless link. Security section is used to select authentication and encryption settings. Advanced section contains parameters allowing optimizing the link capacity.

> **i** Before changing radio settings manually verify that your settings will comply with local government regulations. At all times, it is the responsibility of the end-user to ensure that the installation complies with local radio regulations.

The APC device can operate in four wireless modes: Access Point, Access Point Repeater, Station, iPoll Access Point and iPoll Station.
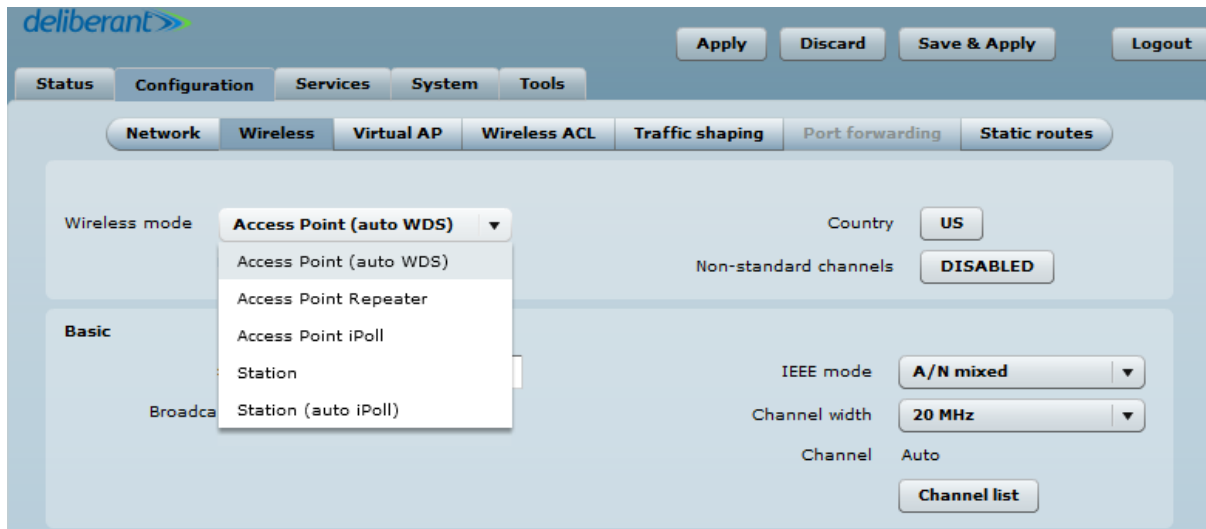
Figure 22 – Device Wireless Operating Mode

Depending on the wireless operation mode selection some of the displayed configuration parameters will differ (e.g. security or advanced wireless settings).

Wireless mode – select wireless operation mode:

- **Access Point (auto WDS)** – enables the APC function as an access point to connect multiple wireless clients. Auto WDS mode allows connect wireless clients with and without WDS enabled (the packet forwarding at layer 2 level).
- **Access Point Repeater** – enables the access point radio operate as a wireless repeater to extend the signal range.
- **Access Point iPoll** – enables APC radio function as access point for point-to-multipoint solution. The Access Point Poll establishes connection with Station auto iPoll, other clients requests will be not accepted.
- **Station** – sets the radio to run in client mode. In this mode wireless station does not broadcast an SSID and clients cannot connect to it. Station mode allows the APC radio to connect to other radios functioning as an AP.
- **Station (auto iPoll)** – with this wireless mode the APC will act as an Station and will automatically turn on iPoll mode if detects that selected AP is an Access Point iPoll.

> **i** Be sure that both ends of the link have the appropriate wireless mode, otherwise the connection will be not established (e.g. Station is not able to establish a connection with Access Point iPoll).

Wireless Mode: Access Point (auto WDS)

Use Basic Wireless Settings to setup radio interface of the device.

Figure 23 – Access Point Wireless Settings

Country - displays APC unit operating country. The Country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the APC unit's installation, though can be updated if required.

Non-standard channels - with this option enabled, the Channel list can be expanded in 5MHz channel step. Note that some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all 802.11a/n standard clients or Access Points.

> The **Non-standard channels** option is available on APC devices with 5GHz radio only.

> The Access Point and the Station must have the same configured **Non-standard channels** option; otherwise the connection can be not established regarding the channel interference.

AP Basic Wireless Settings

SSID – specify the SSID of the wireless network device.

Broadcast SSID – enables or disables the broadcasting of the SSID for AP.

IEEE mode – specify the wireless network mode.

Channel width – The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Channel – displays the channel at which the AP is operating, or indicates that autochannel function is used.

Channel list – select the channel(s) at which the AP unit will operate. If more than one channel is selected, then autochannel feature will be enabled. Automatic channel selection allows AP to select a channel which is not used by any other wireless device or, if there are no free channels available - to select a channel which is least occupied. The table displays detailed information about each channel:

Figure 24 – Channel List Table

AP Advanced Wireless Settings

Advanced parameters allow configuring the device to get the best performance/capacity of the link.

Figure 25 – Wireless Advanced Settings

Tx power – set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Fragmentation – specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS – specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.

Auto BA session – enable or disable BA (Block ACK) session.

Quality of service (WMM) – enable to support quality of service for traffic prioritizing.

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other. Client isolations is available only in Access Point (auto WDS) and Access Point Repeater mode.

Enable DFS – select to enable radar detection. With enabled DFS, APC unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the APC unit randomly selects a different channel.

Enable AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

BA window size – specify BA (Block ACK) window size [1-64].

Max clients limit - specify the maximum number of associated wireless clients on the radio.

Min client signal (dBm) - if enabled, the AP will drop the connection for clients that have signal level below configured threshold.

Mode – choose the AP antenna operating mode:

▪ **SISO** – single input single output. The device will use only one antenna for data transfer. The antenna will be chosen automatically.
▪ **MIMO** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max data rate N – choose the data rates in Mbps at which should transmit packets for the selected 802.11n mode. The APC will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the APC will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which should transmit packets. The APC will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the APC will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Auto data rate - select the algorithm at which the APC will choose the proper data rates in case the signal degrades (possibly due to distance from the access point):

- **Fixed algorithm** - with this method the APC will start transmitting data with the specified **Max data rate N** or **Max legacy data rate** and step down gradually until the best data rate of the transmission will be reached.
- **Dynamic algorithm** - with this method the APC will start transmitting data with automatically calculated data rate by specific algorithm and step down to the next automatically calculated data rate until the best data rate of the data packet transmission will be reached.

Data rate fallback – choose the data rate fallback method: normal or aggressive.

- **Normal** - the APC will start transmitting data at the highest data rate and then decreases it until the best rate of the transmission will be reached.
- **Aggressive** - with this method selected, the data rate will be decreasing down faster and more aggressive: the APC will start transmitting data at the highest data rate and renegotiate down every two data rate until the best rate of the transmission will be reached, even changing the radio mode from MIMO to SISO.

Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns.

MPDU density – define minimum time between PPDU's.

ACK timeout – specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Mode: Access Point Repeater

Use **Access Point Repeater** mode in order to extend the range of the existing network infrastructure. The Access Point repeater's wireless settings have possibility to scan SSID of the surrounding APs and choose the required one.

Figure 26 – Access Point Repeater Wireless Settings

Country - displays APC unit operating country. The Country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the APC unit's installation, though can be updated if required.

Non-standard channels - with this option enabled, the Channel list can be expanded in 5MHz channel step. Note that some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all 802.11a/n standard clients or Access Points.

The **Non-standard channels** option is available on APC devices with 5GHz radio only.

The both ends of the link must have the same configured **Non-standard channels** option; otherwise the connection can be not established regarding the channel interference.

Peer AP Settings – click to configure Peer AP settings:
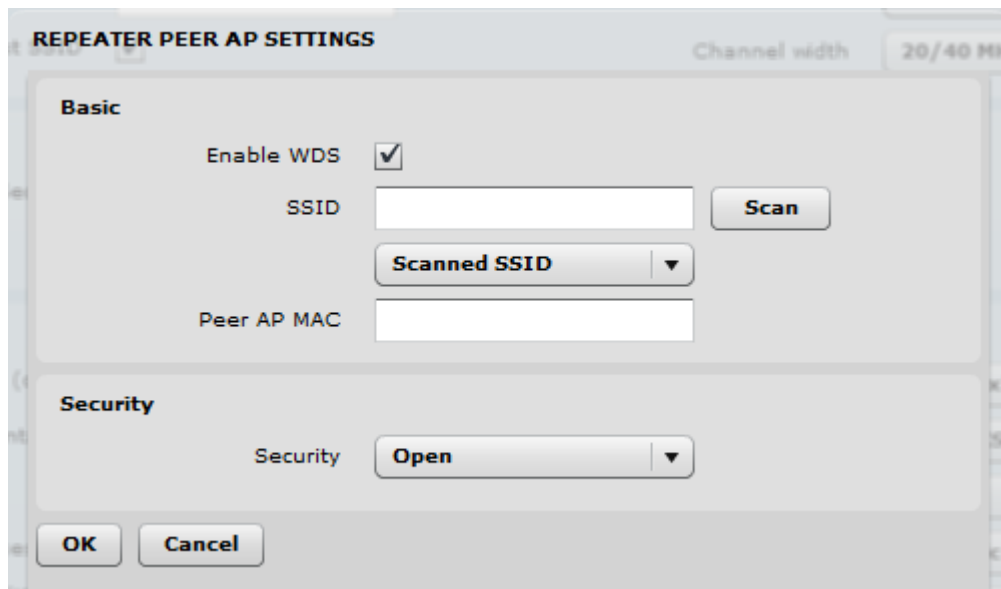
SSID – specify the SSID of the repeater's peer access point.

▪ **Scan** – click this button to scan for surrounding wireless networks. Found network SSID's will be available in drop down menu.

Peer Access Point MAC – enter the MAC address of the peer access point.

Security – choose and specify the security settings of the peer access point

Repeater Basic Wireless Settings

Broadcast SSID - enable or disable the broadcasting of the SSID.

IEEE mode – specify the operating wireless mode.

Channel width - The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Repeater Advanced Wireless Settings

Advanced parameters allow configuring the Repeater to get the best performance/capacity of the link.
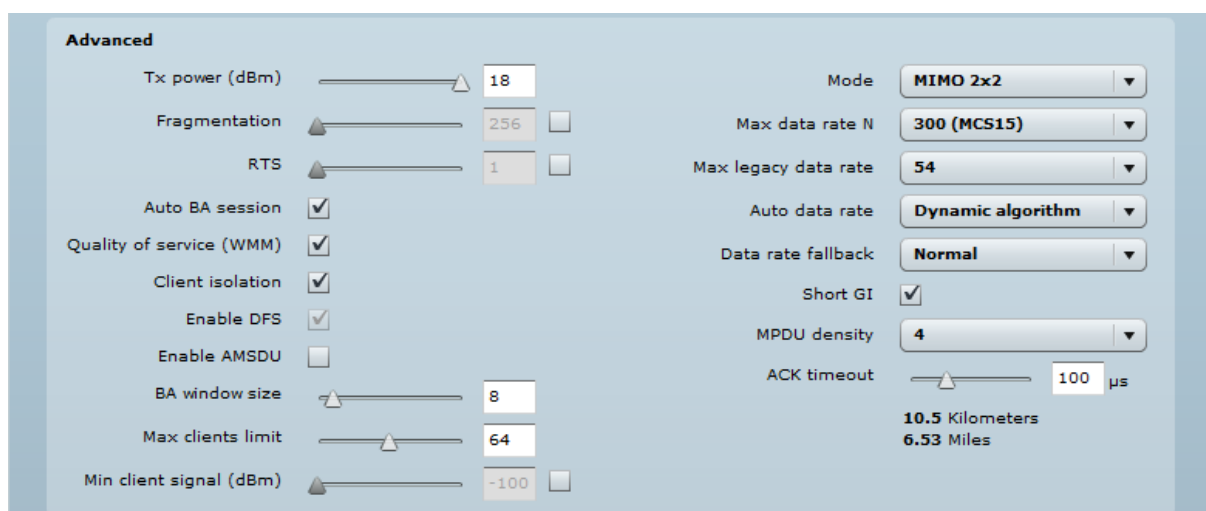
Figure 27 – Repeater's Advanced Wireless Settings

Tx power – set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Fragmentation – specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS – specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.

Auto BA session – enable or disable BA (Block ACK) session.

Quality of service (WMM) – enable to support quality of service for traffic prioritizing.

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other. Client isolations is available only in Access Point (auto WDS) and Access Point Repeater mode.

Enable DFS – select to enable radar detection. With enabled DFS, APC unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the APC unit randomly selects a different channel.

Enable AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

BA window size – specify BA (Block ACK) window size [1-64].

Max clients limit - specify the maximum number of associated wireless clients on the radio.

Min client signal (dBm) - if enabled, the AP Repeater will drop the connection for clients that have signal level below configured threshold.

Mode – choose the AP antenna operating mode:

- **SISO** – single input single output. The device will use only one antenna for data transfer. The antenna will be chosen automatically.
- **MIMO** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max data rate N – choose the data rates in Mbps at which should transmit packets for the selected 802.11n mode. The APC will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the AP Repeater will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which should transmit packets. The APC will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the AP Repeater will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Auto data rate - select the algorithm at which the AP Repeater will choose the proper data rates in case the signal degrades (possibly due to distance from the access point):

- **Fixed algorithm** - with this method the AP Repeater will start transmitting data with the specified **Max data rate N** or **Max legacy data rate** and step down gradually until the best data rate of the transmission will be reached.
- **Dynamic algorithm** - with this method the AP Repeater will start transmitting data with automatically calculated data rate by specific algorithm and step down to the next automatically calculated data rate until the best data rate of the data packet transmission will be reached.

Data rate fallback – choose the data rate fallback method: normal or aggressive.

- **Normal** - the AP Repeater will start transmitting data at the highest data rate and then decreases

it until the best rate of the transmission will be reached.

- ▪ **Aggressive** - with this method selected, the data rate will be decreasing down faster and more aggressive: the AP Repeater will start transmitting data at the highest data rate and renegotiate down every two data rate until the best rate of the transmission will be reached, even changing the radio mode from MIMO to SISO.

Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns.

MPDU density – define minimum time between PPDU's.

ACK timeout – specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Mode: Access Point iPoll

The iPoll wireless mode is designed for point to multipoint wireless solutions. The iPoll Access Point establishes a connection only with iPoll Stations thus creating a reliable network.

Figure 28 – iPoll Access Point's Wireless Settings

Country - displays APC unit operating country. The Country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the APC unit's installation, though can be updated if required.

Non-standard channels - with this option enabled, the Channel list can be expanded in 5MHz channel step. Note that some center frequencies will not be valid with 802.11 specifications. This feature may interfere with other networks and may not support all 802.11a/n standard clients or Access Points.

> iPoll Access Point and iPoll Station must have the same configured **Non-standard channels** option; otherwise the connection can be not established regarding the channel interference.

Poll AP Basic Wireless Settings

Use Basic section to setup basic operating settings of the iPoll Access Point's radio.

> iPoll Access Point and iPoll Station will operate in 802.11n IEEE mode only.

SSID – specify the SSID of the wireless network device.

Broadcast SSID – enables or disables the broadcasting of the SSID for AP.

Channel width – The default channel bandwidth for 802.11n radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Channel – displays the channel at which the iPoll AP is operating, or indicates that autochannel function is used.

Channel list – select the channel(s) at which the iPoll AP will operate. If more than one channel is selected, then autochannel feature will be enabled. Automatic channel selection allows iPoll AP to select a channel which is not used by any other wireless device or, if there are no free channels available - to select a channel which is least occupied. The table displays detailed information about each channel:

Channel/Frequency	Channel width	TX power limit	EIRP limit	DFS/ATPC required
36 (5180 MHz)	20/40 MHz	17 dBm	17 dBm	No
40 (5200 MHz)	20/40 MHz	17 dBm	17 dBm	No
44 (5220 MHz)	20/40 MHz	17 dBm	17 dBm	No
48 (5240 MHz)	20/40 MHz	17 dBm	17 dBm	No
52 (5260 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
56 (5280 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
60 (5300 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
64 (5320 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
100 (5500 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
104 (5520 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
108 (5540 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
112 (5560 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
116 (5580 MHz)	20 MHz	20 dBm	20 dBm	Yes
132 (5660 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
136 (5680 MHz)	20/40 MHz	20 dBm	20 dBm	Yes
140 (5700 MHz)	20 MHz	20 dBm	20 dBm	Yes
149 (5745 MHz)	20/40 MHz	30 dBm	30 dBm	No
153 (5765 MHz)	20/40 MHz	30 dBm	30 dBm	No

Figure 29 – Channel Selection

iPoll AP Advanced Wireless Settings

Advanced wireless settings allow configuring the APC unit to get the best performance/capacity of the link:
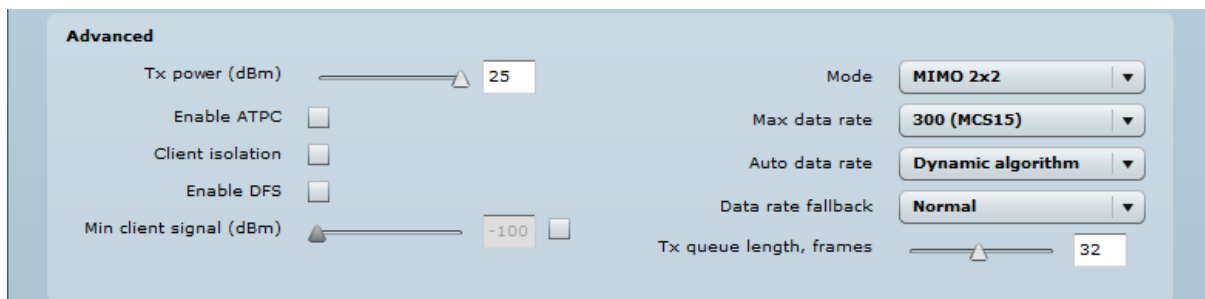
Figure 30 – iPoll Access Point Advanced Wireless Settings

Tx power – set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Enable ATPC – select to enable Automatic Transmit Power Control (ATPC). If enabled, device radio will continuously communicate with remote unit's radio in order to adjust the optimal transmit power automatically.

Enable DFS – select to enable a radar detection. With enabled DFS, APC unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the unit randomly selects a different channel.

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other. Client isolations is available only in Access Point (auto WDS) and Access Point Repeater mode.

Min client signal (dBm) - if enabled, the AP will drop the connection for clients that have signal level below configured threshold.

Mode – choose the unit's antenna operating mode:

- **SISO** – single input single output. The device will use only one antenna for data transfer. The antenna will be chosen automatically.
- **MIMO** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max data rate – select the device data transmission rates in Mbps from the drop-down list. The Access Point iPoll will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the Access Point iPoll will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data packet transmission.

Auto data rate - select the algorithm at which the Access Point iPoll will choose the proper data rates in case the signal degrades (possibly due to distance from the access point):

- **Fixed algorithm** - with this method the Access Point iPoll will start transmitting data with the specified **Max data rate** and step down gradually until the best data rate of the transmission will be reached.
- **Dynamic algorithm** - with this method the Access Point iPoll will start transmitting data with automatically calculated data rate by specific algorithm and step down to the next automatically calculated data rate until the best data rate of the data packet transmission will be reached.

Data rate fallback – choose the data rate fallback method: normal or aggressive.

- **Normal** - the Access Point iPoll will start transmitting data at the highest data rate and then decreases it until the best rate of the transmission will be reached.
- **Aggressive** - with this method selected, the data rate will be decreasing down faster and more aggressive: the Access Point iPoll will start transmitting data at the highest data rate and renegotiate down every two data rate until the best rate of the transmission will be reached, even changing the radio mode from MIMO to SISO.

Transmit queue length, frames – specify the length in frames of the transmit queue.

Wireless Mode: Station

The Station wireless settings a bit differ from the Access Point's settings: there is possibility to scan SSID of the surrounding APs and choose the required one.

Use Wireless Settings to setup radio interface of the device.
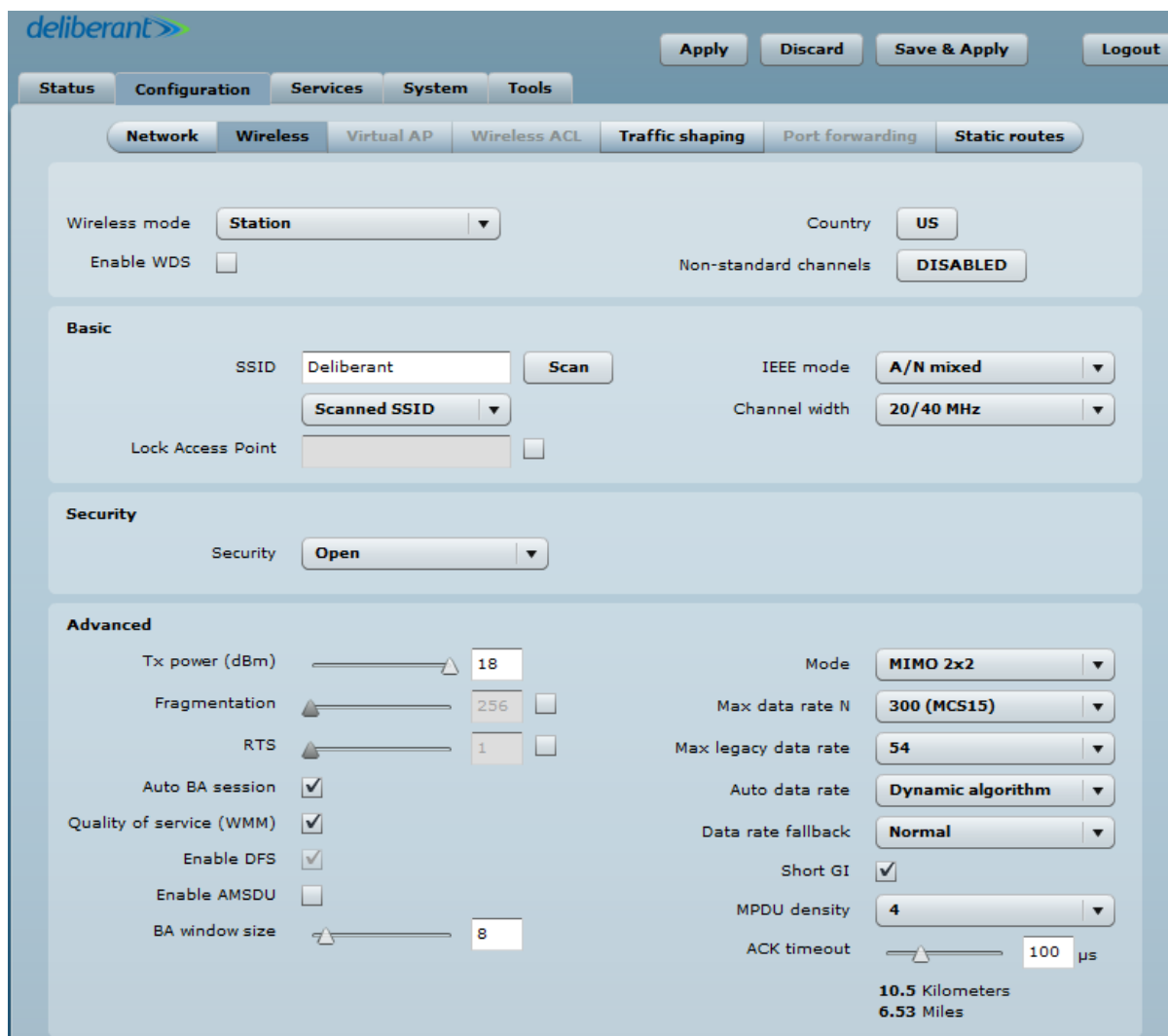
Figure 31 – Station Wireless Settings

Enable WDS – if enabled, the wireless station will communicate with access point in WDS mode. Station WDS mode enables packet forwarding at layer 2 level.

Country - displays APC unit operating country. The Country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the APC unit's installation, though can be updated if required.

Non-standard channels - with this option enabled, the Channel list can be expanded in 5MHz channel step. Note that some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all 802.11a/n standard clients or Access Points.

> The Access Point and Station must have the same configured **Non-standard channels** option; otherwise the connection can be not established regarding the channel interference.

Station Basic Wireless Settings

SSID – specify the SSID of the wireless network device.

Scan – click this button to scan for surrounding wireless networks. Found network SSID's will be available in drop down menu.

Lock Access Point - specify the MAC address of the particular access point, thus preventing the roaming between access points with the same SSID.

IEEE mode – specify the wireless network mode.

Channel width - The default channel bandwidth for 802.11 radio is 20MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Station Advanced Wireless Settings

Advanced parameters allow configuring the device to get the best performance/capacity of the link.
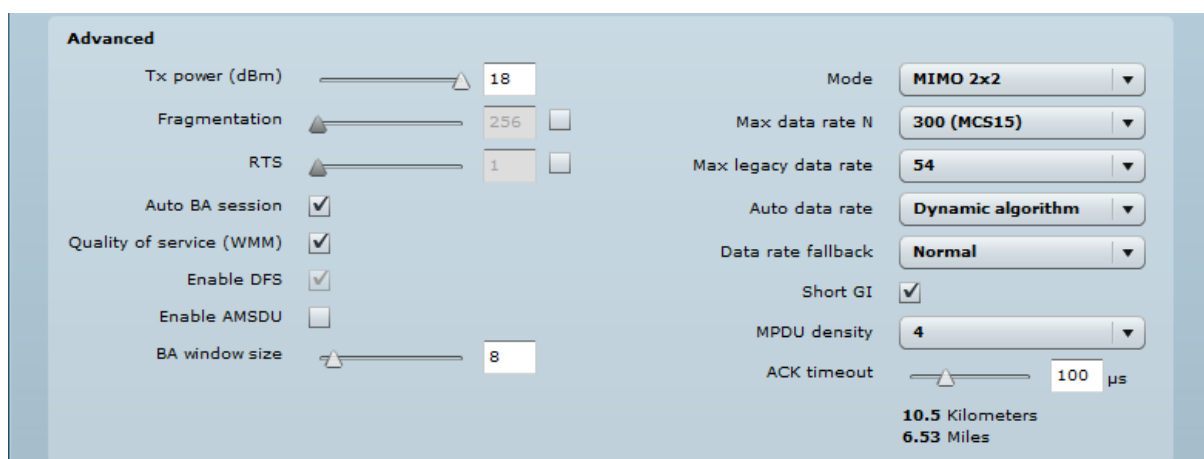
Figure 32 – Station Advanced Wireless Settings

Tx power – set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Fragmentation – specify the Fragmentation threshold using slider or enter the value manually [256-2346 bytes]. This is the maximum size for a packet before data is fragmented into multiple packets. Setting the Fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

RTS – specify the RTS threshold using slider or enter the value manually [0-2347 bytes]. The RTS threshold determines the packet size of a transmission and, through the use of an access point, helps control traffic flow.

Auto BA session – enable or disable BA (Block ACK) session.

Quality of service (WMM) – enable to support quality of service for traffic prioritizing.

Enable DFS – select to enable radar detection. With enabled DFS, APC unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the APC unit randomly selects a different channel.

Enable AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased.

BA window size – specify BA (Block ACK) window size [1-64].

Mode – choose the AP antenna operating mode:

- **SISO** – single input single output. The device will use only one antenna for data transfer. The antenna will be chosen automatically.
- **MIMO** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max data rate N – choose the data rates in Mbps at which should transmit packets for the selected 802.11n mode. Station will attempt to transmit data at the highest data rate set. If there will be an interference encountered, Station will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which should transmit packets. Station will attempts to transmit data at the highest data rate set. If there will be an interference encountered, Station will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Auto data rate - select the algorithm at which the Station will choose the proper data rates in case the signal degrades (possibly due to distance from the access point):

- **Fixed algorithm** - with this method Station will start transmitting data with the specified **Max data rate N** or **Max legacy data rate** and step down gradually until the best data rate of the transmission will be reached.
- **Dynamic algorithm** - with this method Station will start transmitting data with automatically calculated data rate by specific algorithm and step down to the next automatically calculated data rate until the best data rate of the data packet transmission will be reached.

Data rate fallback – choose the data rate fallback method: normal or aggressive.

- **Normal** - Station will start transmitting data at the highest data rate and then decreases it until the best rate of the transmission will be reached.
- **Aggressive** - with this method selected, the data rate will be decreasing down faster and more aggressive: Station will start transmitting data at the highest data rate and renegotiate down every two data rate until the best rate of the transmission will be reached, even changing the radio mode from MIMO to SISO.

Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns.

MPDU density – define minimum time between PPDU's.

ACK timeout – specify the ACK timeout using slider or enter the value manually. Ack timeout can be entered by defining the link distance or specifying time value. Too low value of the ACK timeout will give very low throughput. A high value may slow down the link in noisy environment. A low value is far worse than a value slightly too high. ACK Timeout value should be tuned to the optimal value for the maximum link throughput.

Wireless Mode: Station (auto iPoll)

With this wireless mode, the APC will operate as wireless Station, though it automatically switch on the iPoll mode if the specified access point will be detected as an AP iPoll. If the Station finds two networks with the same SSID, where one is iPoll, another 11n, the connection priority will be iPoll.
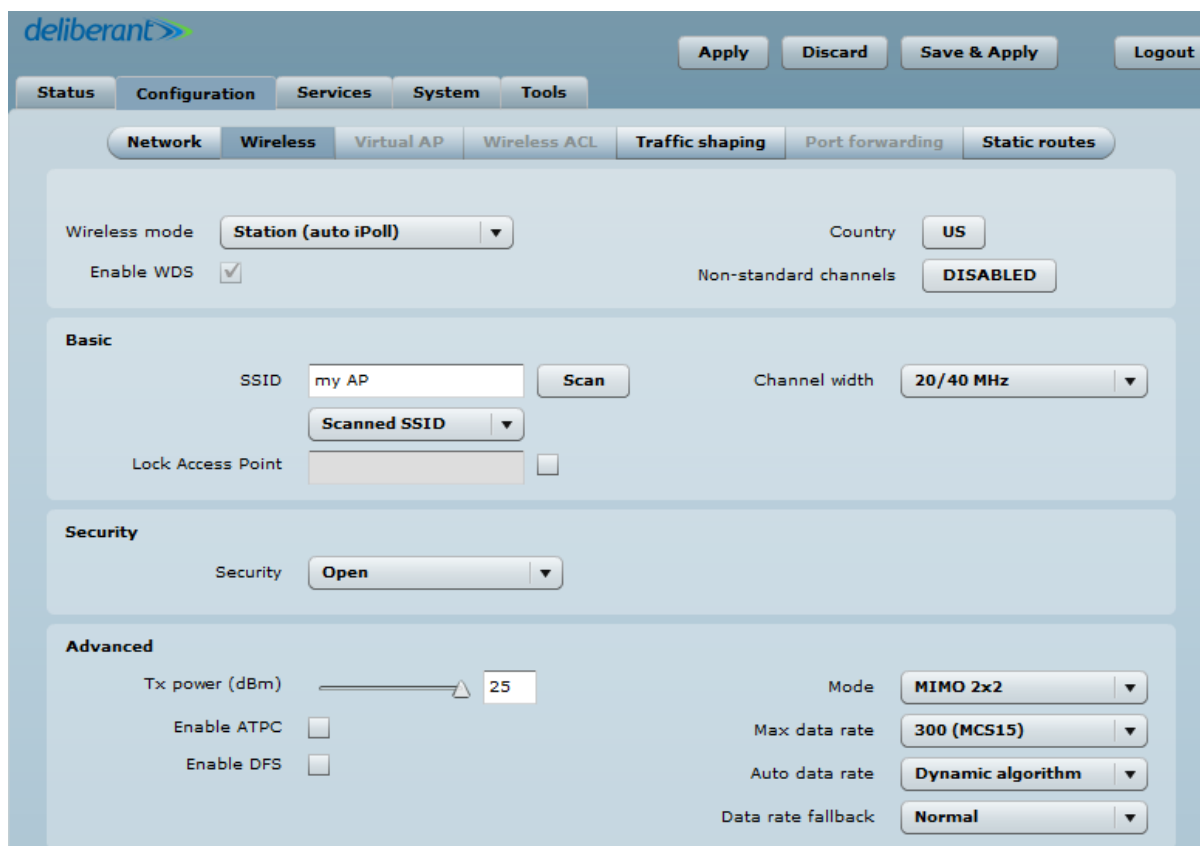
Figure 33 – Station (autoiPoll) Wireless Settings

Country - displays APC unit operating country. The Country selection determines the available channels and transmission power level based on regulatory restrictions in the operating country. The country has been selected on the first step of the APC unit's installation, though can be updated if required.

Non-standard channels - with this option enabled, the Channel list can be expanded in 5MHz channel step. Note that some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all 802.11a/n standard clients or Access Points.

The both ends of the link must have the same configured **Non-standard channels** option; otherwise the connection can be not established regarding the channel interference.

Station (auto iPoll) Basic Wireless Settings

Use this section to setup basic operating settings of the iPoll Station radio.

iPoll Access Point and iPoll Station will operate in 802.11n IEEE mode only.

SSID – specify the SSID of the wireless network device manually, or use **Scan** to find iPoll Access Points automatically.

Scan – click this button to scan for surrounding Access Points. Found network SSID's will be available in drop down menu.

Lock Access Point - specify the MAC address of the particular Access Points, thus preventing the roaming between Access Points with the same SSID.

Channel width – The default channel bandwidth for 802.11 N radio is 20/40MHz. The 802.11n allow channel bonding in such way the total channel width becomes 40MHz.

Station (auto iPoll) Advanced Wireless Settings

Advanced wireless settings allow configuring the Station (auto iPoll) to get the best performance/capacity of the link:
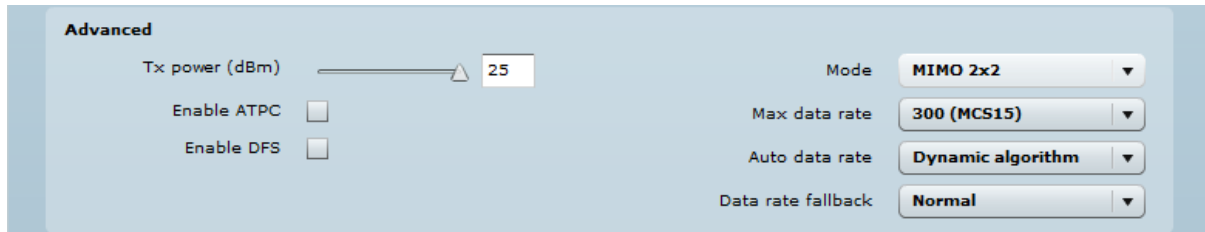

Figure 34 – Station (autoiPoll) Advanced Wireless Settings

TX power – set the unit's transmitting power at which the device will transmit data. The larger the distance, the higher transmit power is required. To set transmit power level use the slider or enter the value manually. When entering the transmit power value manually, the slider position will change according to the entered value. The maximum transmit power level is limited to the allowed value by country in which device is operating regulatory agency.

Enable ATPC – select to enable Automatic Transmit Power Control (ATPC). If enabled, device radio will continuously communicate with remote unit's radio in order to adjust the optimal transmit power automatically.

Enable DFS – select to enable a radar detection. With enabled DFS, APC unit monitors the operating frequency for radar signals. If radar signals are detected on the channel, the unit randomly selects a different channel.

Mode – choose the unit's antenna operating mode:

- **SISO** – single input single output. The device will use only one antenna for data transfer. The antenna will be chosen automatically.
- **MIMO** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max data rate – select the device data transmission rates in Mbps from the drop-down list. The APC will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the Station will step down according the selected method (**Auto data rate** and **Data rate fallback** settings below) to the highest rate that allows data transmission.

Auto data rate - select the algorithm at which the Station will choose the proper data rates in case the signal degrades (possibly due to distance from the access point):

- **Fixed algorithm** - with this method Station will start transmitting data with the specified **Max data rate N** or **Max legacy data rate** and step down gradually until the best data rate of the transmission will be reached.
- **Dynamic algorithm** - with this method Station will start transmitting data with automatically calculated data rate by specific algorithm and step down to the next automatically calculated data rate until the best data rate of the data packet transmission will be reached.

Data rate fallback – choose the data rate fallback method: normal or aggressive.

- **Normal** - Station will start transmitting data at the highest data rate and then decreases it until the best rate of the transmission will be reached.
- **Aggressive** - with this method selected, the data rate will be decreasing down faster and more aggressive: Station will start transmitting data at the highest data rate and renegotiate down every

two data rate until the best rate of the transmission will be reached, even changing the radio mode from MIMO to SISO.

Wireless Security

If APC acts as an Access Point (AP (auto WDS), AP Repeater or AP iPoll) the wireless security settings will be used by the wireless stations for association. Thus wireless station security settings must conform the settings configured on the AP that station is associated with.

The APC supports various authentication/encryption methods:

- **Open** – no encryption. Additionally RADIUS MAC authentication can be configured (on access point).
- **WEP** – encrypts the data portion of each packet exchanged on a wireless network using a 64-bit or 128-bit WEP encryption key. Additionally RADIUS MAC authentication can be configured (on access point).
- **Personal WPA/WPA2** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals. WPA uses TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) for data encryption. Additionally RADIUS MAC authentication can be configured (on access point).
- **Enterprise WPA/WPA2** – RADIUS server based authentication with WPA/WPA2 encryption using AES or TKIP (requires configured RADIUS server).

Available security methods, according APC operating wireless mode is listed in the table below:

Security method	Access Point (autoWDS)	Access Point Repeater	Access Point iPoll	Station	Station (auto iPoll)
Open	✕ [!]	✕ [!]	✕ [!]	✕	✕
WEP 64bit/128bit	✕ [!]	✕ [!]		✕	
Personal WPA/WPA2 AES	✕ [!]	✕ [!]	✕ [!]	✕	✕
Personal WPA/WPA2 TKIP	✕ [!]	✕ [!]		✕	
Personal WPA/WPA2 AES/TKIP	✕ [!]				
Enterprise WPA/WPA2 AES	✕		✕	✕	✕
Enterprise WPA/WPA2 TKIP	✕			✕	
Enterprise WPA/WPA2 AES/TKIP	✕				

[!] - additionally RADIUS MAC authentication is available.

Open

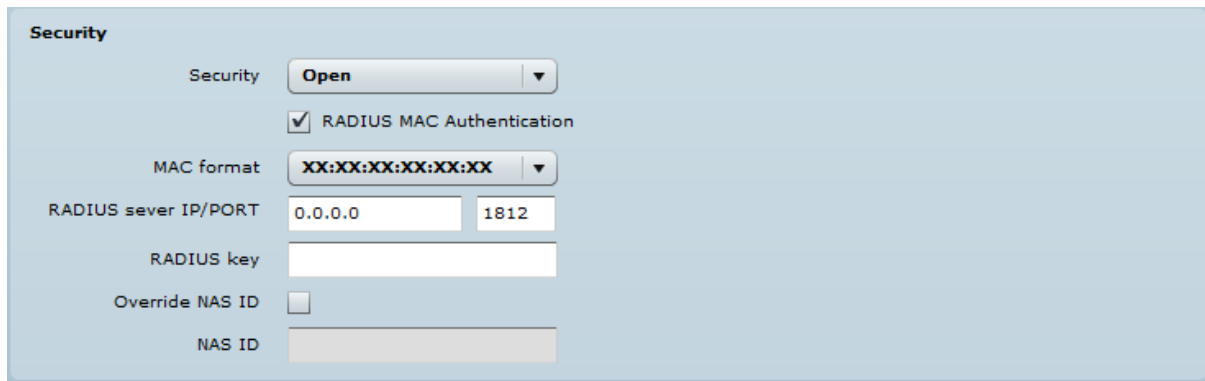By default there is no encryption enabled on the APC device:

Figure 35 – Wireless Security: Open with RADIUS MAC Authentication Enabled

RADIUS MAC authentication - enable the RADIUS MAC authentication. If enabled, the access point will send wireless station's MAC address to RADIUS server for authentication before associating with wireless station.

> Configuration of RADIUS MAC authentication is available only on following wireless modes: *Access Point (auto WDS)*, *Access Point Repeater* and *Access Point iPoll*

MAC format - choose the format of the MAC address, relevant to RADIUS server.

RADIUS IP/PORT – specify the IP address and port of the authentication RADIUS server where the access requests will be send to.

RADIUS key – specify the secret key [string]. The shared secret is used to encrypt data packets transmitted between RADIUS server and client.

Override NAS ID – if selected, the default NAS ID will be overridden with the new specified value.

NAS ID – specify the new NAS ID value.

WEP

WEP encryption can be either 64bit or 128bit and with or without RADIUS MAC authentication.
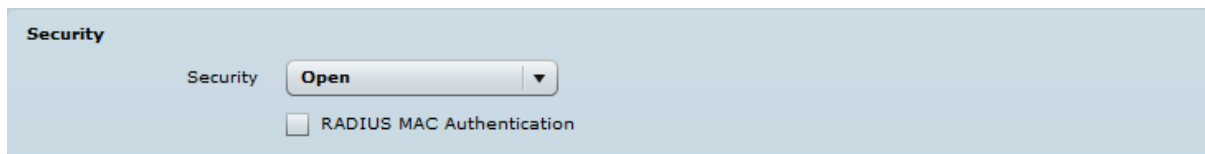

Figure 36 –Wireless Security: WEP Security

Key index - select the WEP key index [1-4]. Each number represents one of the four static keys of WEP. The selected key index will be used for frame encryption and decryption.

WEP passkey – specify the passkey, for the chosen WEP security:

▪ For **WEP 64bit** encryption – 5 HEX pairs (e.g. aa:bb:cc:dd:ee), or 5 ASCII characters (e.g. abcde);
▪ For **WEP 128bit** encryption – 13 HEX pairs (e.g. aa:bb:cc:dd:ee:ff:gg:hh:00:11:22:33:44), or 13 ASCII characters (e.g. abcdefghijklm);

RADIUS MAC authentication – enable the RADIUS MAC authentication (for detailed information about configuration refer to the section above: *Open*).

Personal WPA/WPA2

To setup **Personal WPA/WPA2** encryption, need to specify the pre-shared key and encryption with chosen AES, TKIP or Auto method:
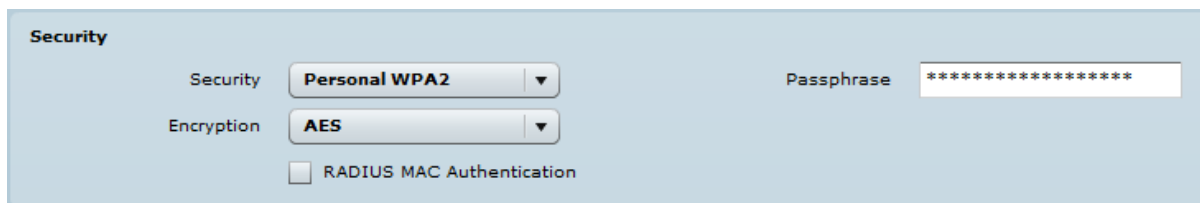
Figure 37 – Wireless Security: Personal WPA/WPA2 Security

Passphrase – specify WPA or WPA2 passphrase [8-63 characters]. The passphrase will be converted to key format, selected above.

Encryption – specify WPA/WPA2 encryption algorithm:

- **AES** – APC will accept clients with passphrase encrypted with AES method only;
- **TKIP** – APC will accept clients with passphrase encrypted with TKIP method only;
- **Auto** – APC will accept clients with passphrase encrypted with both: AES and TKIP methods;

RADIUS MAC authentication – enable the RADIUS MAC authentication (for detailed information about configuration refer to the section above: *Open*).

Enterprise WPA/WPA2

APC has possibility to configure **Enterprise WPA/WPA2** encryption with RADIUS authentication. Properly configured AP will accept wireless stations requests and will send the information to configured RADIUS server for client authentication.
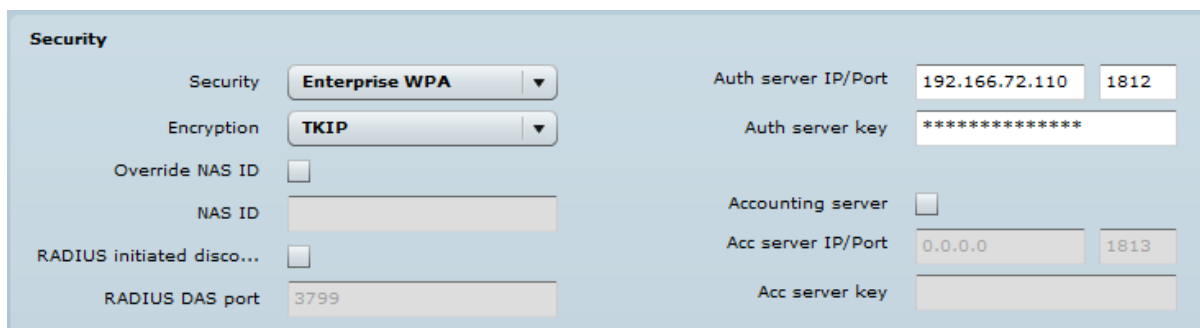

Figure 38 – Wireless Security: Enterprise WPA/WPA2 Security 1

The properly configured RADIUS server is required for **Enterprise WPA/WPA2** encryption.

Encryption – specify WPA/WPA2 encryption algorithm:

- **AES** – AP will accept clients with passphrase encrypted with AES method;
- **TKIP** – AP will accept clients with passphrase encrypted with TKIP method;
- **Auto** – AP will accept clients with passphrase encrypted with both: AES and TKIP methods;

Override NAS ID – if selected, the default NAS ID will be overridden with the new specified value.

NAS ID – specify the new NAS ID value.

RADIUS initiated disconnect – select to enable Radius initiated user session termination.

RADIUS DAS port – specify the RADIUS DAS (Dynamic Authorization Server) port where the disconnect requests will be sent to. Default port is 3799.

RADIUS authentication settings:

Auth server IP/port – specify the IP address and port of the authentication RADIUS server where the authentication requests will be send to.

Auth server key – specify the secret key of the authentication server [string]. The shared secret is used to encrypt data packets transmitted between RADIUS server and client.

RADIUS accounting settings:

Acc server IP/port – specify the IP address and port of the accounting RADIUS server where the accounting requests will be send to.

Acc server key – specify the secret key of the accounting server [string]. The shared secret is used to encrypt data packets transmitted between RADIUS server and client.

If APC is operating in Station wireless mode, Station will send requests to AP, which will redirect authentication parameters to required RADIUS server.

Figure 39 – Wireless Security: Enterprise WPA/WPA2 Security 2

Encryption – choose WPA/WPA2 encryption type:

- **AES** – data encrypted with AES method;
- **TKIP** – data encrypted with TKIP method;

EAP method – choose EAP method:

- **EAP-TTLS-MSCHAPv2**
- **PEAP/ MSCHAPv2**

Identity – specify the identity of the authentication to the RADIUS server.

Password – specify the password of the authentication to the RADIUS server.

> Identity and Password on the APC must match the identity and password running on the RADIUS server's user list.

Virtual AP

> Virtual AP functionality is available only in **Access Point (auto WDS)** and **Access Point Repeater** wireless modes.

Use the **Configuration | Virtual AP** page to configure to create up to 3 additional Virtual AP interfaces. The Virtual AP defines a logical wireless network, and the APC can be configured to provide additional 3 wireless networks on each device radio. All the VAPs may be active at the same time meaning that client devices can associate to the APC using any of the VAP SSID.

The Virtual AP table displays a summary of all virtual radio interfaces running on the APC:
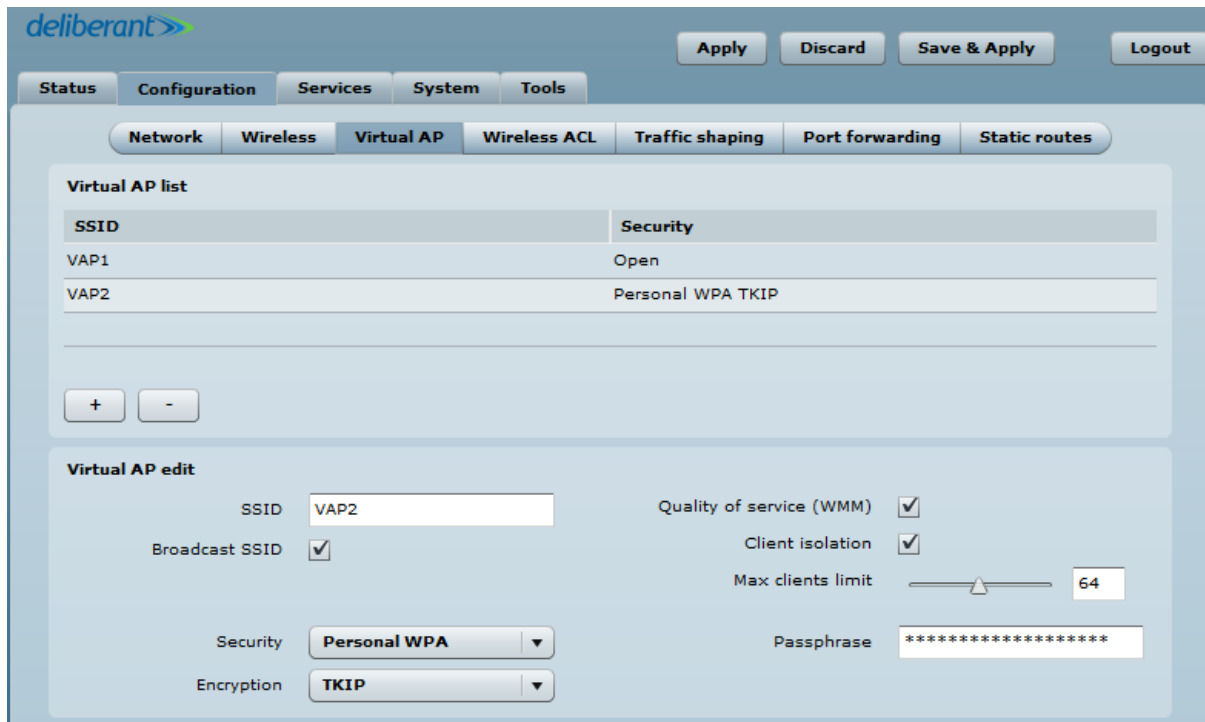
Figure 40 – VAP Table

To create a new Virtual AP, click on **+** button to add new entry on the VAP table, then select this entry and specify required parameters:

SSID – specify the unique name for the VAP [string].

Broadcast SSID – when this option is selected the particular SSID is visible during network scans on a wireless station. When unselected, the VAP SSID is not visible and not broadcasted to wireless stations.

Quality of service (WMM) – enable to support quality of service for prioritizing traffic.

Client isolation – enable the client Layer 2 isolation. The Layer 2 isolation blocks the wireless clients from communicating with each other.

Each VAP security is configured by default as an "open system", which broadcasts a beacon signal including the configured SSID. For more secure network choose one of the security mechanisms for each VAP interface.

Security – choose the wireless security and encryption method from the drop-down list (for detailed security configuration, refer to the respective section *Wireless Security*).

- **Open** – no encryption.
- **WEP** – encrypts the data portion of each packet exchanged on a wireless network using a 64-bit or 128-bit WEP encryption key.
- **Personal WPA/WPA2** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals. WPA uses TKIP (Temporal Key Integrity Protocol) and AES (Advanced Encryption Standard) for data encryption.
- **Enterprise WPA/WPA2** – RADIUS server based authentication with WPA/WPA2 encryption using AES or TKIP (requires configured RADIUS server).
- **UAM** – Web browser based user authentication method. UAM authentication is available only if Access Point is working in router mode. For UAM configuration details refer at the respective chapter *Universal Access Method (UAM)*.

Wireless clients must be able to respond with a specific security configuration.

Wireless ACL

Wireless ACL is active only in **Access Point (auto WDS)**, **Access Point Repeater** and **iPoll Access Point** wireless modes.

Access Control provides the ability to limit associations wirelessly based on MAC address to an AP by creating an Access Control List (ACL) on each wireless interface (including VAPs).
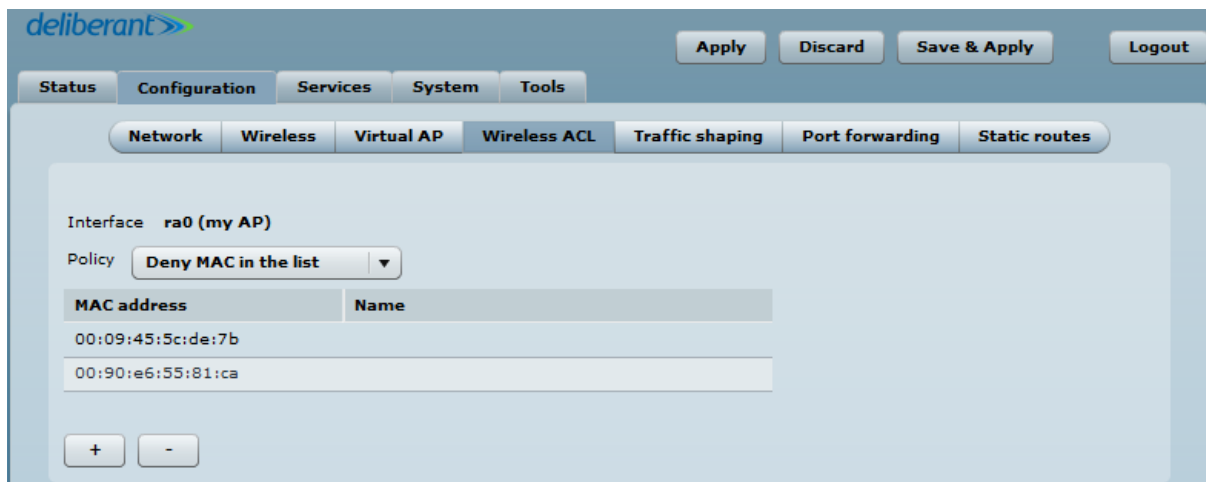

Figure 41 – Wireless ACL Configuration

Policy – define the policy:

- **Open** – no rules applied
- **Allow MAC in the list** – only listed MAC clients can connect to the AP (white list).
- **Deny MAC in the list** – only listed MAC clients can NOT connect to the AP (black list).

To add new rule, press the "**+**" button.

To remove the rule, first select the rule then press the "**–**" button.

To edit the rule double click on the field.

Traffic Shaping

> Traffic shaping is not available on Access Point Repeater wireless modes.

Use **Traffic Shaping** to control download or upload bandwidth in order to optimize or guarantee performance. There are two methods to control network traffic:

- **Limit all traffic** – limits overall APC upload and download traffic.
- **Limit per IP traffic** – limits upload and download traffic for a specified IP addresses.
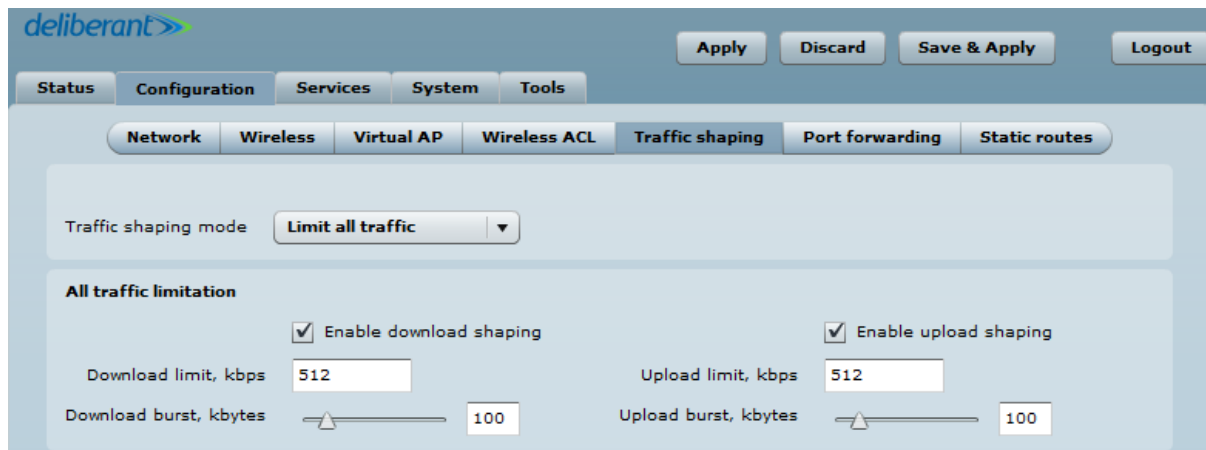

Figure 42 – Traffic Shaping Configuration

Limit all traffic

Enable download shaping – select to enable limitation of the download traffic.

Download limit, kbps – specify the maximum download bandwidth value in Kbps.

Download burst, kbytes – specify the download burst size in kbytes.

Enable upload shaping – select to enable limitation of the upload traffic.

Upload limit, kbps – specify the maximum upload bandwidth value in Kbps.

Upload burst, kbytes – specify the upload burst size in kbytes

Limit per IP traffic
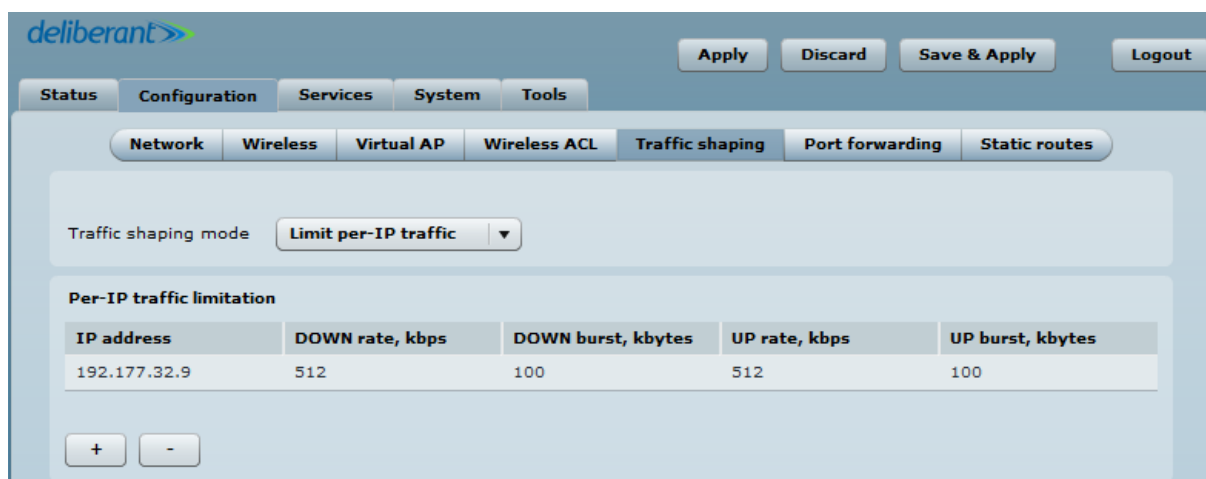
Use + button to create new traffic limitation rules

Figure 43 – Traffic Shaping: Per IP Limitation

IP address – specify IP address for which the traffic will be limited.

Down rate, kbps – specify the maximum download bandwidth value in Kbps.

Down burst, kbytes – specify the download burst size in kbytes.

UP rate, kbps – specify the maximum upload bandwidth value in Kbps.

UP burst, kbytes – specify the download burst size in kbytes

Port Forwarding

Port forwarding is active only in Router network mode..

Port Forwarding, **UPnP** and **DMZ** is effective only if **NAT** is enabled.

The **Port forwarding** section gives the ability to pass traffic behind an interface that has NAT enabled. For instance if the unit is in router mode with NAT enabled on the WAN interface, no devices on the outside of the WAN interface can see any private IPs on the LAN side of the unit. By using port forwarding or DMZ it is possible to pass traffic through to these private IP addresses.
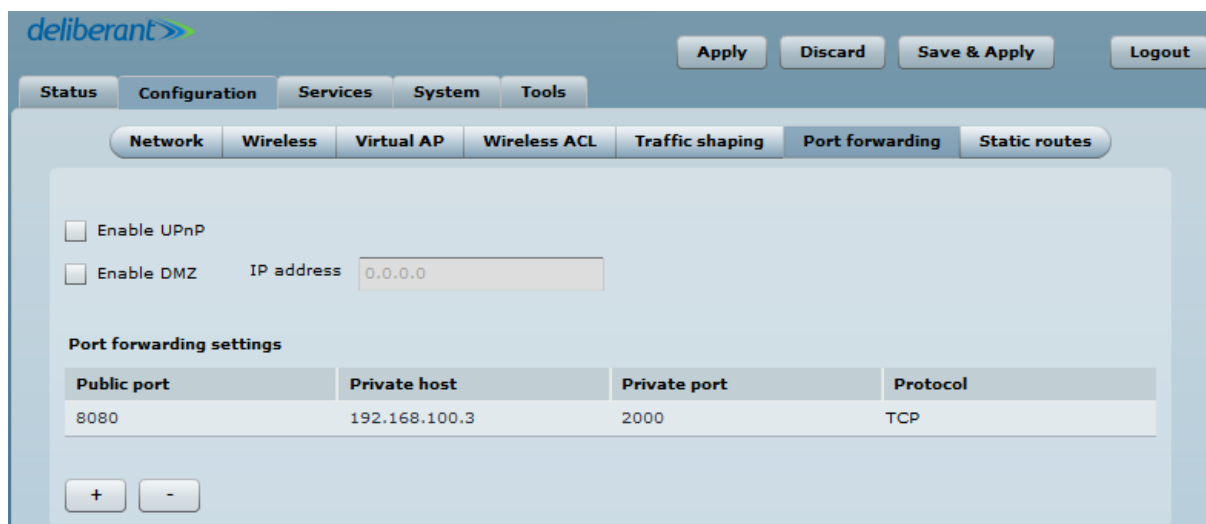

Figure 44 – Port Forwarding Configuration

Enable UPnP – select to enable UPnP (Universal Plug and Play connectivity) service. The UPnP enables APC communicate with other network devices automatically opening required ports, without manual intervention.

Enable DMZ – select to enable DMZ. DMZ opens all TCP/UDP ports to particular IP address. It allows setting up servers behind the APC. The feature is used commonly for setting up VoIP or Multi-Media servers.

Public port – specify the port that will be accessed externally using the public IP address.

Private host – specify the IP address behind NAT that public traffic will get forwarded to.

Private port – specify the listening port on private computer behind NAT.

Protocol – select type of forwarding traffic: TCP or UDP.

Static Routes

> **Static routes** is active only in Router network mode.

A routing rule is defined by the destination subnet (Destination IP address and netmask) and/or gateway where to route the target traffic. To add a new static route, specify the following parameters:

Figure 45 – Static Route Configuration

Destination IP – specify the destination IP address.

Netmask – specify destination netmask.

Gateway – specify the gateway address for the route. 0.0.0.0 stands for the default gateway of the selected interface.

Services

WNMS

Wireless Network Management System (WNMS) is a centralized monitoring and management system for wireless network devices. The communication between managed devices and the WNMS server is always initiated by an WNMS client service running on every device.

Enable WNMS agent – select to enable WNMS agent.

Server/Collector URL – specify the URL of the WMS server to which that heartbeat notifications will be sent to.

Test - click this button to check if the specified server responses successfully.

System alerts

The device is able to send external alerts when there are system errors. The alerts can be sent via SNMP Traps or/and SMTP notifications.
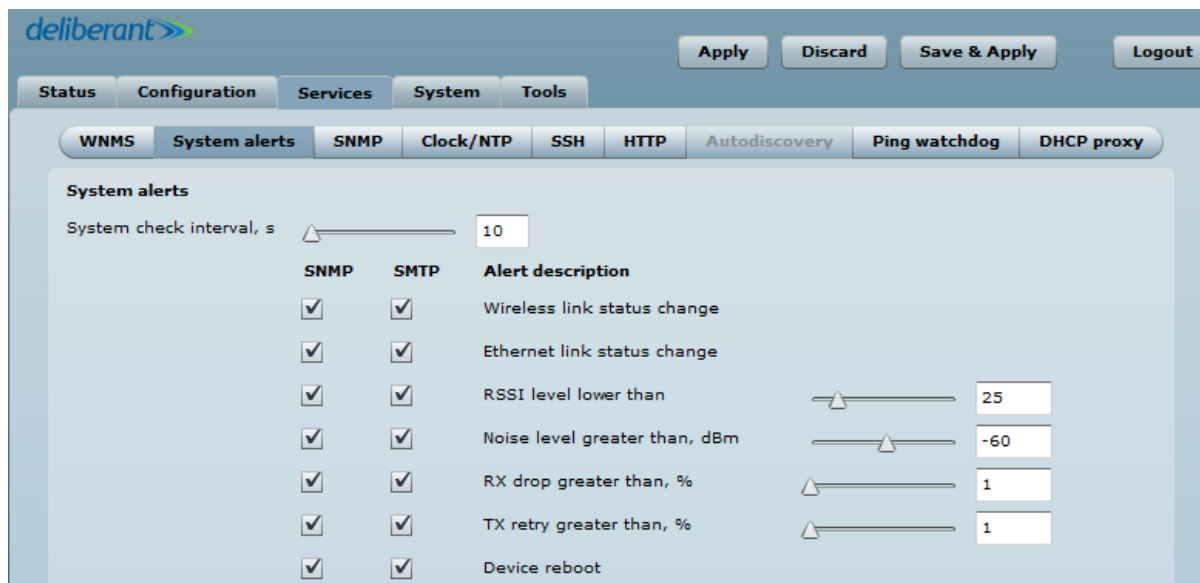

Figure 46 – Device Alerts

Enable alerts – select to enable alert notifications on the system.

System check interval, s – specify interval in seconds at which the device will send notifications of unexpected system behavior.

System alerts:

Wireless link status change – system will send notification on Wireless link status change.

Ethernet link status change – system will send notification on Ethernet link status change.

RSSI level lower than – system will send notification when RSSI reach value lower than specified. Default: 25

Noise level greater than – system will send notification when signal noise will reach value greater than specified. Default: -60 dBm.

RX drop greater than – system will send notification when percent of RX dropped packets become higher than specified value. Default: 250 packets per seconds.

TX retry greater than – system will send notification when percent of TX retries becomes higher than specified value. Default: 250 packets per seconds.

Device reboot – system will send notification about unexpected or administrator initiated device reboot.
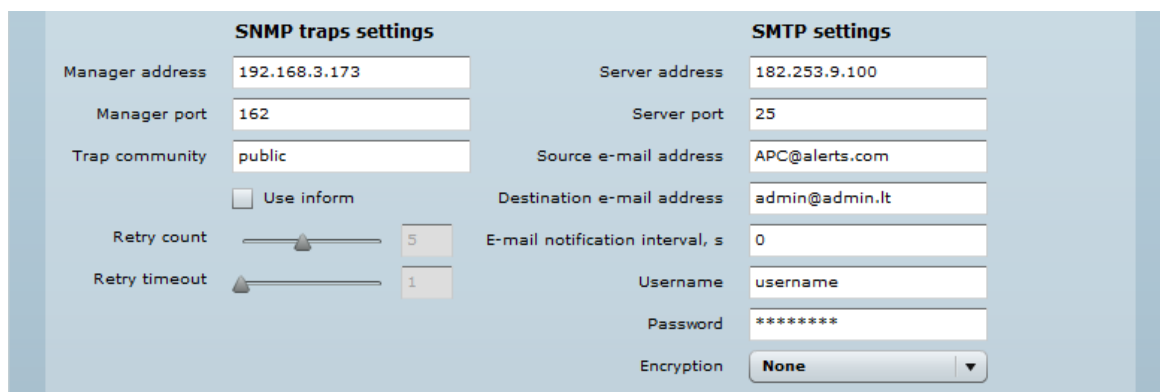
Figure 47 – Device Alerts: SNMP Traps and SMTP Configuration

SNMP Traps Settings

Manager address – specify the IP address or hostname of SNMP Trap receiver.

Manager port – specify the port number of the Trap receiver. Default port number is 162.

Trap community - specify the SNMP community string. This community string acts as password between SNMP manager and device by default Trap community string is "public".

Use inform – select to wait for an acknowledgment from SNMP manager that trap was received.

Retry count – specifies maximum number of times to resend an inform request [1-10]. Default: 5.

Retry timeout – specifies number in seconds to wait for an acknowledgment before resending request [1-10]. Default: 1.

SMTP Settings

Server address – specify the IP address or hostname of the networked SMTP server.

Server port – specify the SMTP Port Number is the port number used by the networked SMTP server. By default the port number is 25.

Source e-mail address – specify the e-mail address that will be used by the device.

Destination e-mail address – specify the e-mail address where the device will send the alert messages.

E-mail notification interval – specify interval in seconds at which the e-mail notification will be sent from the device [0-86400]. If 0 specified, then device will send an e-mail notification immediately after unexpected system behavior.

Username - provide the user name required to access the SMTP server.

Password - provide the password required to access the SMTP server.

Encryption - select the encryption method of SMTP authentication: none, TLS 1.0 or SSL 3.0

SNMP

SNMP is the standard protocol that is widely used for remote network management over the Internet. With the SNMP service enabled, the device will act as SNMP agent.

Figure 48 – SNMP Service Settings

Enable SNMP – specify the SNMP service status.

Friendly name – displays name of the APC that will be used to identify the unit. This name has the same value as Friendly name in the Device settings.

Link location – displays the physical location of the device. This name has the same value as Device location in the Device settings.

Contact information – specify the identification of the contact person for this managed device, together with information on how to contact this person.

SNMP v1/v2c

R/O community – specify the read-only community name for SNMP version 1 and version 2c. The read-only community allows an APC unit manager to read values, but denies any attempt to change values.

R/W community - specify the read-write community that allows an APC unit manager to read and (where possible) change values.

SNMP v3 users have the same access rights as communities but instead of a single community name for all unit managers, user names and passwords must be defined for each APC unit manager. Strong encryption is supported in SNMPv3.

R/O user – specify the user name for read-only SNMPv3 access.

R/O user password – specify the password for read-only SNMPv3 access.

R/W user – specify the user name for read-write SNMPv3 access.

R/W user password – specify the password for read-only SNMPv3 access.

Clock/NTP

Use this section to manage the system time and date on the device automatically, using the Network Time Protocol (NTP), or manually, by setting the time and date on the device.

The NTP (Network Time Protocol) client synchronizes the clock of the device with the defined time server. Choose NTP from the configuration menu, select your location time zone and enter NTP server in order to use the NTP service.

Figure 49 – Device Clock: NTP Configuration

Configuration – choose the system clock configuration mode [NTP/Manual].

Timezone – select the timezone. Time zone should be specified as a difference between local time and GMT time.

Save last known time – select to recall the timestamp that was saved on last reboot. When NTP is enabled, this option will set system clock to last reboot time if no NTP servers are available.

NTP server – specify the trusted NTP server IP or hostname for synchronizing time with [IP address].

To adjust the clock settings manually, choose the configuration mode as Manual and specify the following settings:
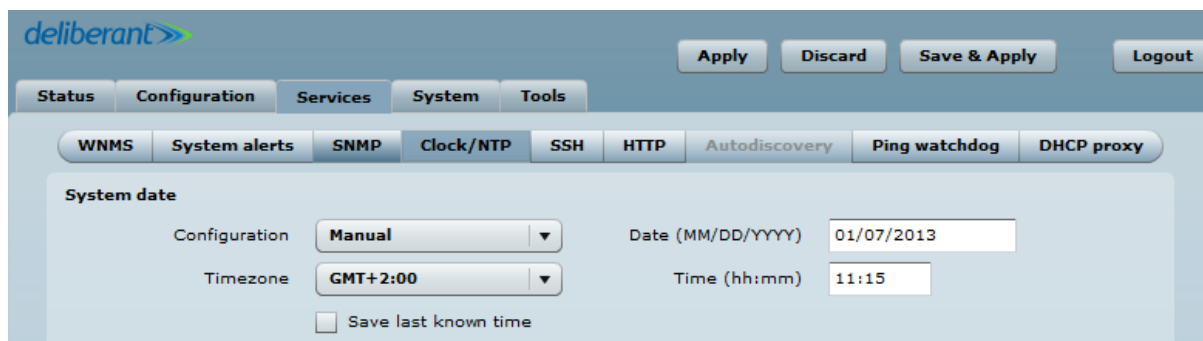

Figure 50 – Device Clock: Manual Configuration

Configuration – choose the system clock configuration mode [NTP/Manual].

Timezone – select the timezone. Time zone should be specified as a difference between local time and GMT time.

Save last known time – select to recall the timestamp that was saved on last reboot.

Date – specify the new date value in format MM/DD/YYYY

Time – specify the time in format hh:mm.

SSH

Use this menu to manage access to the device via SSH port:
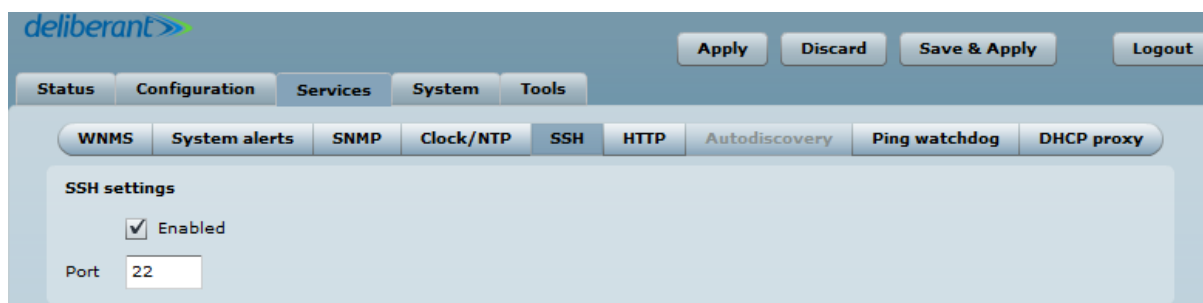

Figure 51 – SSH Port Configuration

Enabled – enable or disable SSH access to device.

Port – the SSH service port. By default SSH port is 22.

HTTP

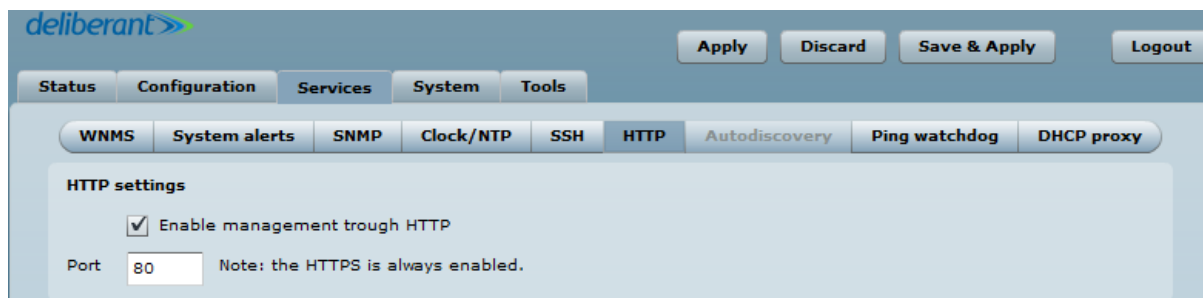Use this menu to control HTTP connection on device web management:

Figure 52 – HTTP Settings

Enable management through HTTP – select tis option to enable or disable HTTP access to the device management.

Port – specify HTTP port. Standard HTTP port is 80.

> **HTTPS** connection via the standard port 8080 is always enabled.

Autodiscovery

> **Autodiscovery** function is available only on **Station** and **Station (auto IPoll)** wireless modes.

Enable this feature to allow the APC unit discovery within reach of a single multicast packet.
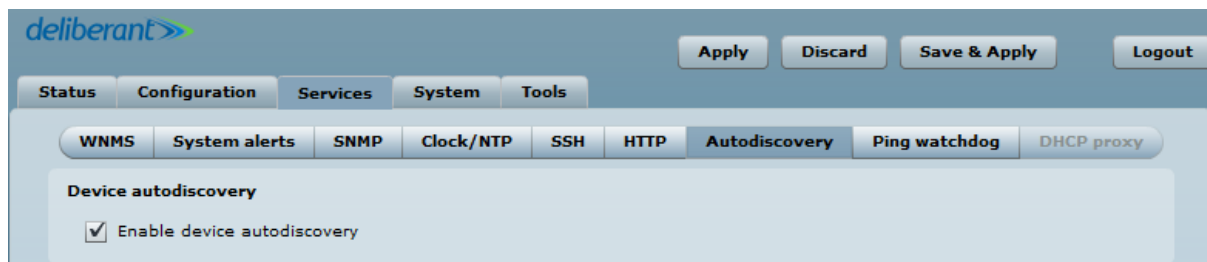
Figure 53 – Device Autodiscovery

Enable device autodiscovery – select to enable Autodiscovery function.

Ping Watchdog

Enable Ping Watchdog for continuous monitoring of the APC unit network connection with the specified trusted host. If enabled, the APC unit will send Ping requests periodically to the host and in case there is no response within a specified time period, the Ping Watchdog will reboot the APC unit.

Figure 54 – APC Ping Watchdog

Enabled – select to enable Ping Watchdog.

IP address - specify the host where the Ping requests will be sent to.

Ping interval - specify the interval in seconds between Ping requests.

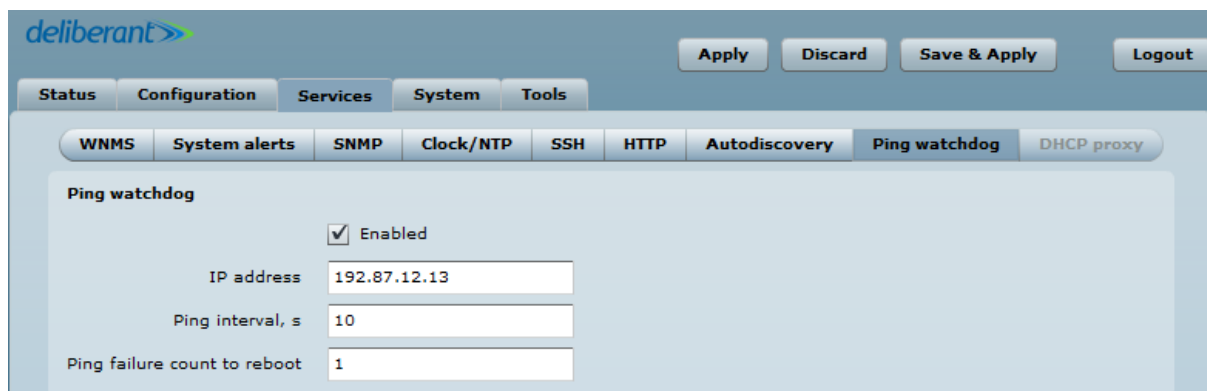**Ping failure count to reboot** - specify the count of failed Ping replies. After specified count of Ping failures, the APC unit will reboot itself.

DHCP Proxy

> **DHCP Proxy** is available only if APC works s bridge in **Access Point** or **Access Point Repeater** wireless modes.

DHCP option 82 enables the AP to act as a DHCP relay agent to prevent DHCP client requests from untrusted sources. If enabled, the additional information will be inserted into DHCP request packets which will be verify by the DHCP server prior to issuing an IP from assigned IP pool.

Select the required SSID on the AP list and the **AP settings** will be ready to enable the DHCP proxy:

Figure 55 – DHCP Proxy Configuration

Option 82 remote-id - specify the remote-id for DHCP proxy requests that will be accepted by DHCP server.

System

Administration

> For security reasons it is recommended to change the default administrator username and password as soon as possible.

System menu allows you to manage main system settings and perform main system actions (reboot, restore configuration, etc.). The section is divided into further three sections: Device settings, Account settings and system functions.

Figure 56 – Device Administration Settings

Device settings

Friendly name – specify name of the APC that will be used to identify the unit.

Device location – describe the location of the device [maximum 255 ASCII characters].

Longitude – specify the longitude coordinates of the device [specific decimal format, e.q. 54.869446].

Latitude – specify the latitude coordinates of the device [specific decimal format, e.q. 23.891058]. Both coordinates helps indicate accurate location of the device.

Account settings

The Administrative Account menu is for changing the administrator's password.

> Default administrator logon settings are:
> Username: **admin**
> Password: **admin01**

Username – change the administrator's username.

Old password – enter the old administrator password.

New password – enter the new administrator password for user authentication.

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

> The only way to gain access to the web management if you forget the administrator password is to reset the unit to factory default settings.

System functions

Reboot device – reboot device with the last saved configuration.

Reset device to factory defaults – click to restore unit's factory configuration.

> Resetting the device is an irreversible process. Current configuration and the administrator password will be set back to the factory default.

Download troubleshooting file – click to download the troubleshooting file. The troubleshooting file contains valuable information about device configuration, routes, log files, command outputs, etc. When using the troubleshooting file, the device quickly gathers troubleshooting information automatically, rather than requiring you to gather each piece of information manually. This is helpful for submitting problems to the support team.

Backup configuration file – click to save the current configuration file. The saved configuration file is useful to restore a configuration in case of a device misconfiguration or to upload a standard configuration to multiple devices without the need to manually configure each device through the web interface.

Restore configuration from file – click to upload an existing configuration file to the device.

Installer radio test mode – select to enable Installer radio test mode. If enabled, responsibility for the compliance of the device performance with the regulatory rules must be taken by the installer.

Log

Use the log tab to configure device to view or save log messages to the local or remote server using standard syslog facility:
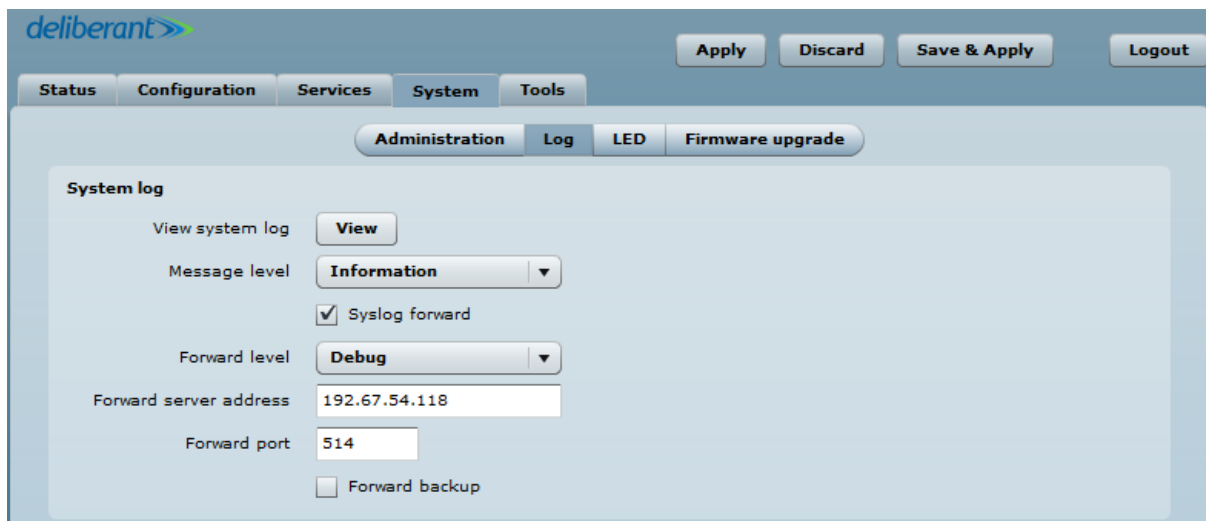

Figure 57 – Device System Log

View system log – click to view current trace messages. The system log viewer utility provides debug information about the system services and protocols. If the device's malfunction occurs recorded messages can help operators to locate misconfiguration and system errors.

Message level – specify system's message tracing level. The level determines the importance of the message and the volume of messages generated by the device. The levels are in increased importance order [emergency, alert, critical, error, warning, notice, information, debug]. Default: info.

The device can be configured to send system log messages to a remote server:

Syslog forward – select to enable remote system logging.

Forward server – specify the remote host IP address or hostname where syslog messages will be sent.

Forward port – specify the port to which syslog messages will be forwarded [0-65535]. Default: 514.

Forward message level – specify the level of the message which will be sent to the remote syslog server. The level determines the importance of the message and the volume of messages generated by the device. The levels are in order of increasing importance [emergency/alert/critical/error/warning/notice/information/debug]. Default: information.

Forward backup – select to enable remote syslog logging backup.

Backup server – specify the backup host IP address or hostname where syslog messages will be send to.

Backup port – specify the port to which syslog messages will be forwarded [0-65535]. Default: 514.

LED Control

The APC is equipped with 6 LEDs: power, LAN and 4 Signal LEDs that indicates the signal strength of current connection. The signal level is classified into 4 levels, thus corresponding 4 LEDs switches on as soon as indicated threshold is reached.
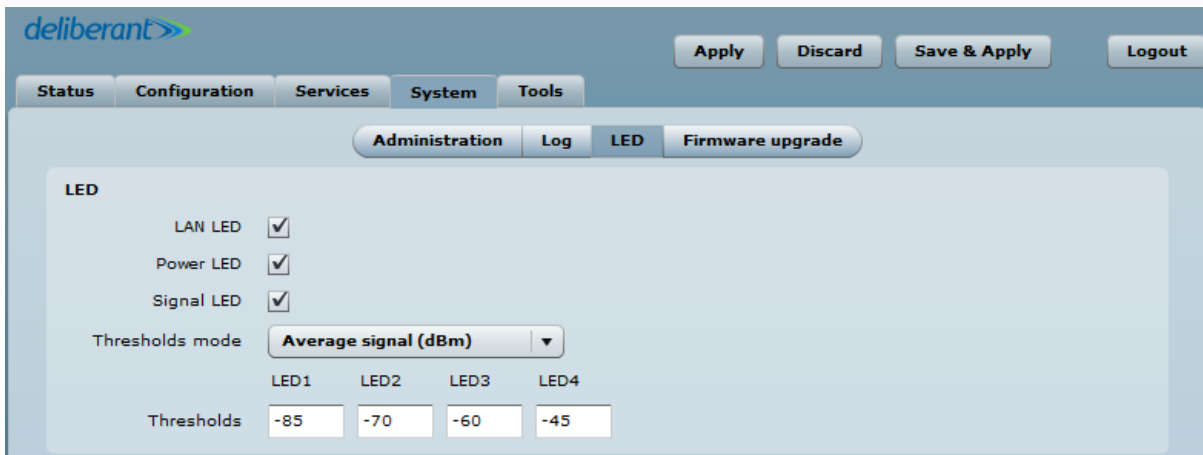
Figure 58 – Device LED Control

LAN LED – select to enable LAN LED. The red LED will be blinking on LAN activity, off – no LAN connection.

Power LED – select to enable Power LED. The steady red LED when power is on, off – no power.

Signal LED – select to enable signal strength indication LEDs:

Thresholds – specify the RSSI threshold at which corresponding LED will switch on.

> The Signal LEDs are working only when the connection is established. Therefore, please make sure all wireless settings are correct and the connection is established.

Firmware Upgrade

To update your device firmware use the **System | Firmware upgrade** menu. Press **Upload firmware**, select the firmware file and click the **Upload firmware** button:
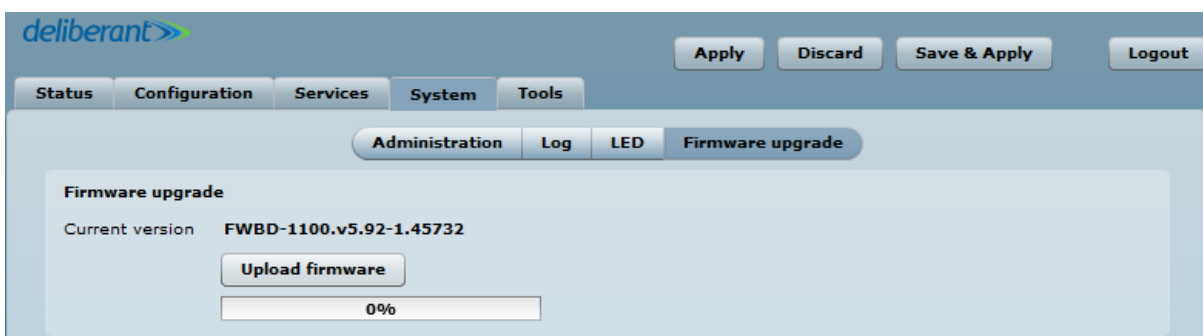
Figure 59 – Firmware Upload

Current version – displays version of the current firmware.

Upload firmware – click the button to select the new firmware image for uploading it to the device.

The device system firmware upgrade is compatible with all configuration settings. When the device is upgraded with a newer version or the same version builds, all the system's configuration will be preserved after the upgrade.

The new firmware image is uploaded to the controller's temporary memory. It is necessary to save the firmware into the device permanent memory. Click the Upgrade button:

Figure 60 – Firmware Upgrade

Upgrade – upgrade device with the uploaded image and reboot the system.

Do not switch off and do not disconnect the device from the power supply during the firmware upgrade process as the device could be damaged.

Tools

Antenna Alignment

The Antenna Alignment tool measures signal quality between the Station and AP. For best results during the antenna alignment tes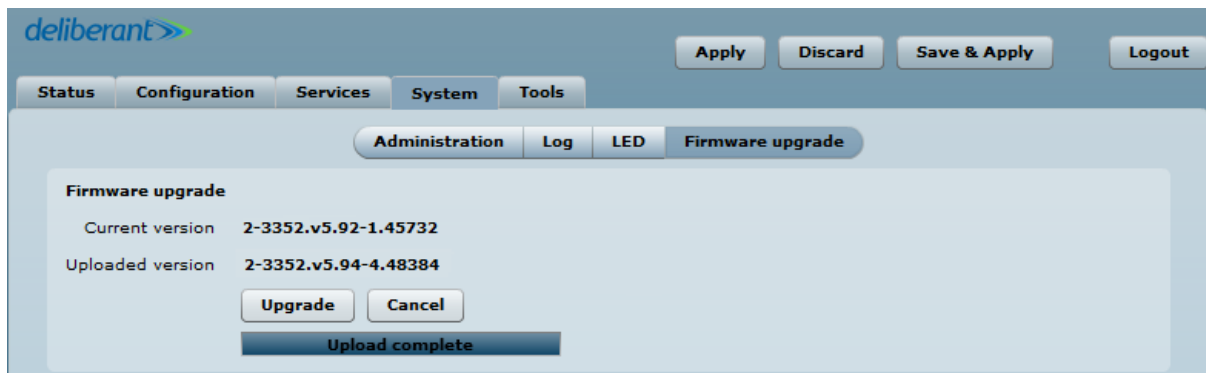t, turn off all wireless networking devices within range of the device except the device(s) with which you are trying to align the antenna. Watch the constantly updated display in the Alignment Test window as you adjust the antenna.

Figure 61 – Antenna Alignment

Start – press this button to start antenna alignment.

Stop – press this button to stop antenna alignment.

Average – if this option selected, the graph will display the average RSSI of both antennas.

Site Survey

The Site Survey tool shows overview information for wireless networks in a local geographic area. Using this test, an administrator can scan for working access points, check their operating channels, encryption and see signal/noise levels.

To perform the Site Survey test currently, click the **Start scan**:
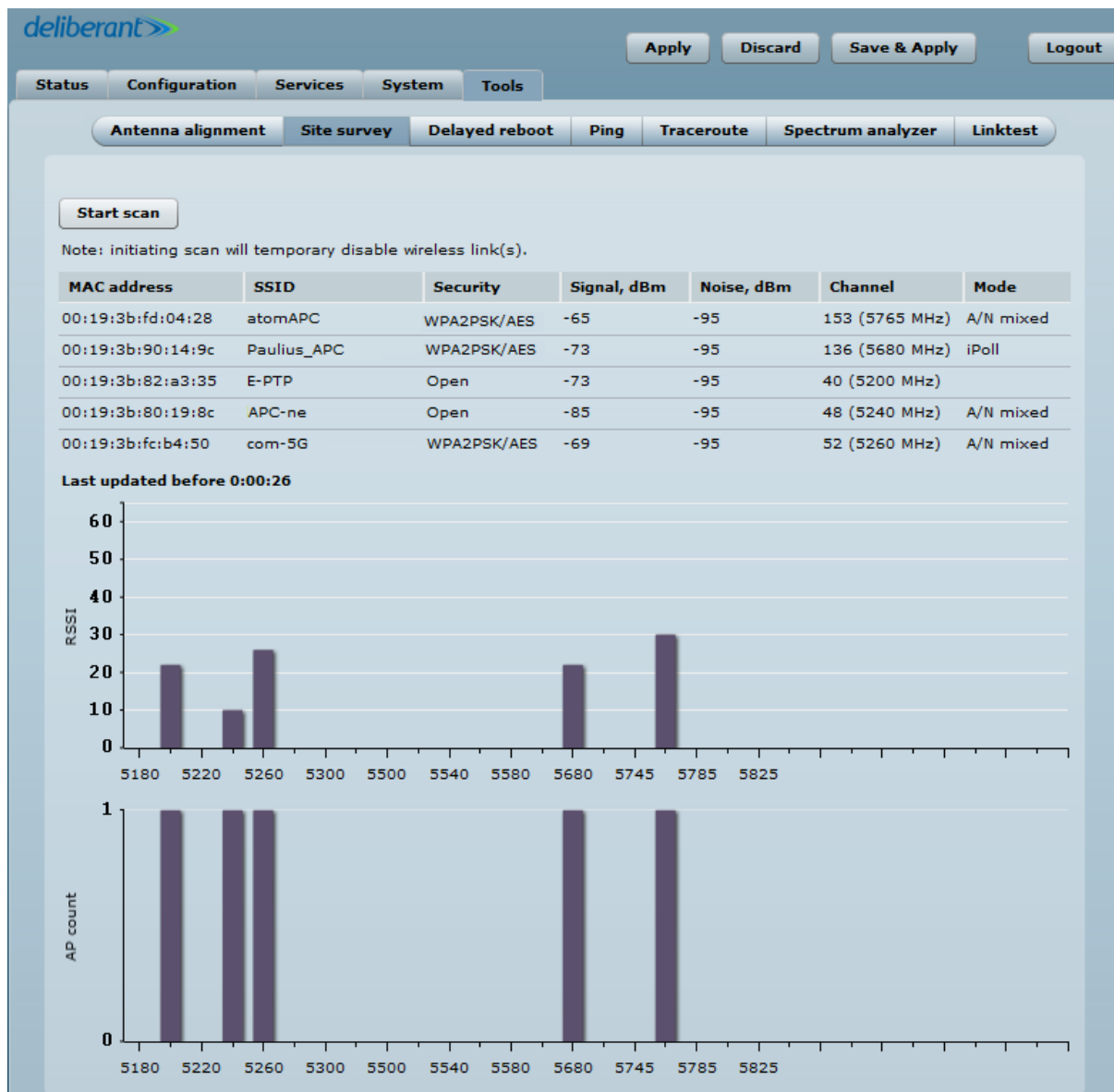
Figure 62 – Site Survey Results

Last updated before – displays when the last scan was performed.

The results of the Site Survey test are converted to handy two graphs: AP count and RSSI. An administrator can use this to identify the best channel for device operation that will not receive interference from adjacent APs.

Delayed Reboot

This tool is extremely useful while tuning radio settings – once you defined hypothetic radio parameters and set them with Apply button (not written to the permanent memory), device starts operating with the new settings, and in case the link fails, device will be rebooted in specified minutes, thus the old settings will be set back.

Figure 63 – Delayed Reboot Configuration

Reboot after – specify time in minutes, after which the device will be rebooted.

Start/Stop – click to start or stop delayed reboot tool.

Ping

This command is used to test whether a particular host is reachable across an IP network. The Ping results will be displayed graphically:
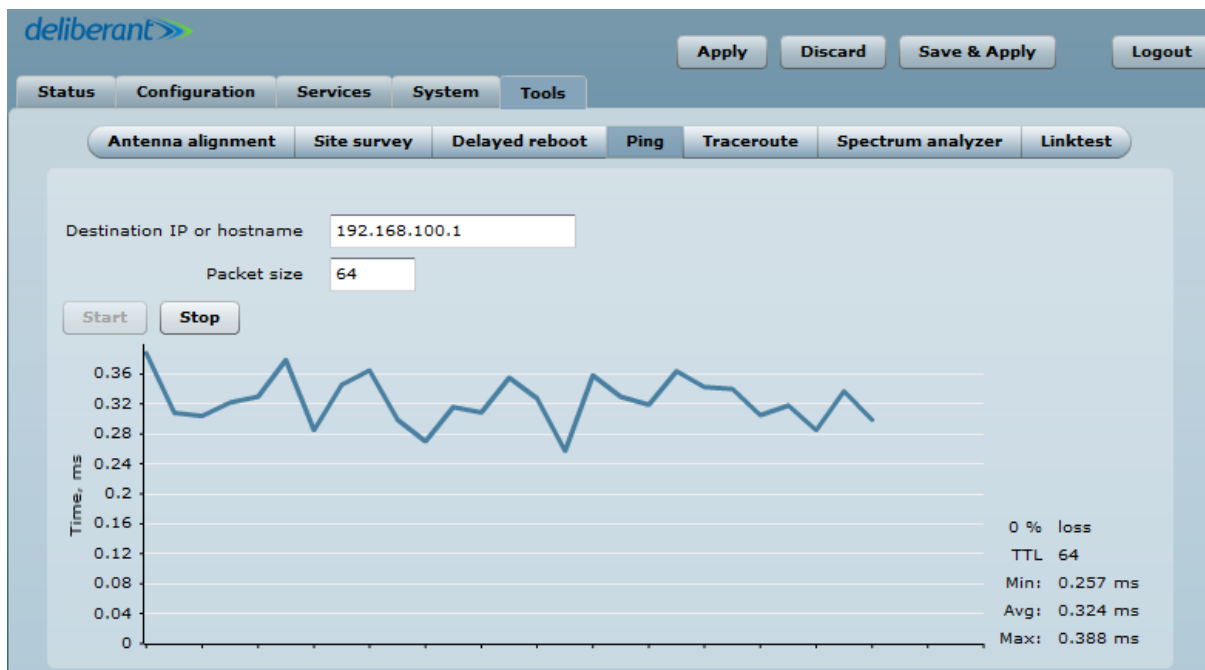
Figure 64 – Ping Results

IP address or Host name – specify the destination IP address or Host name.

Packet size – specify the packet size.

Traceroute

This tool is a route-tracing utility used to determine the path that an IP packet has taken to reach a destination. This is useful when trying to find out why destination is unreachable, as you will be able to see where the connection fails.
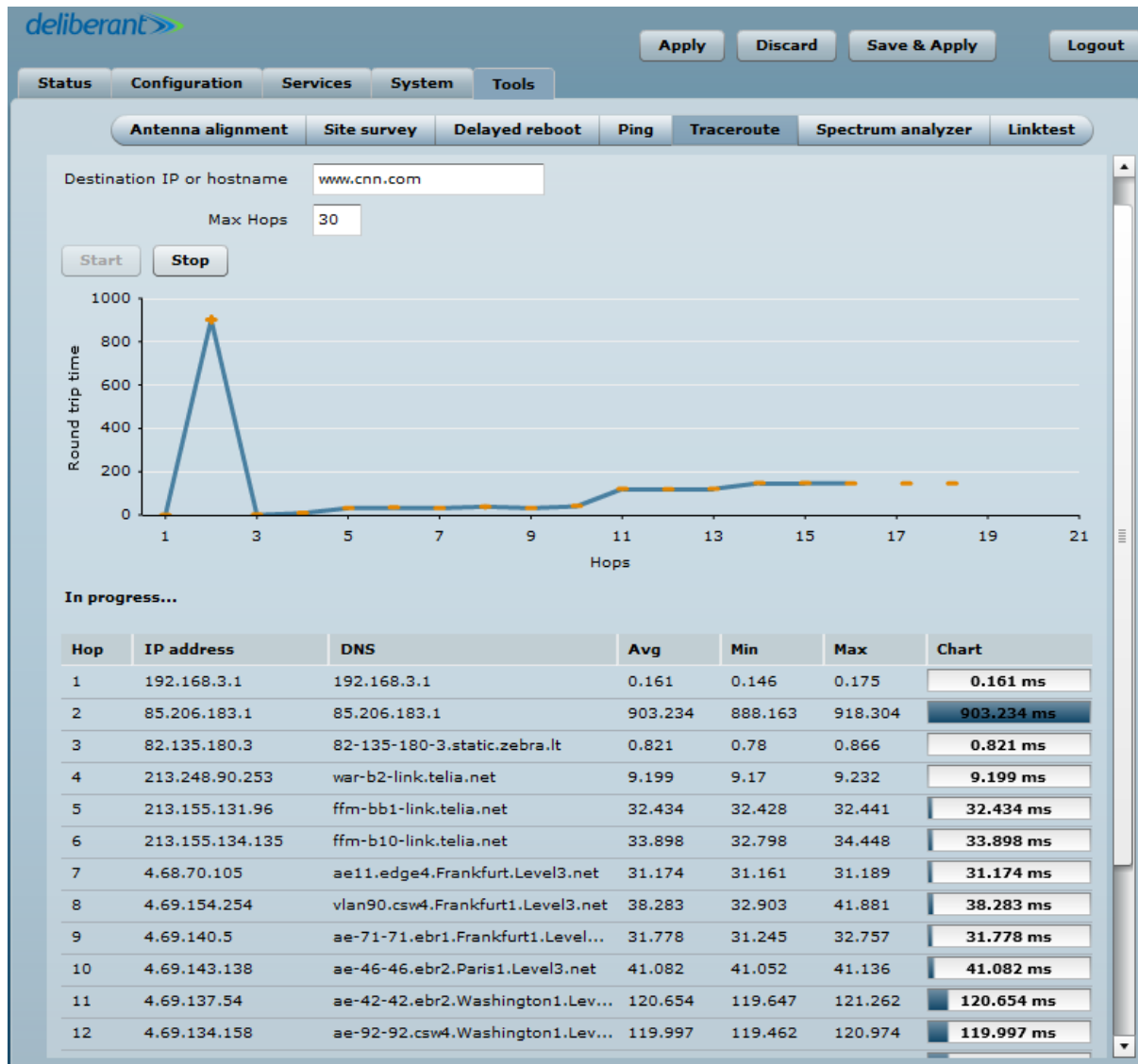
Figure 65 – Traceroute Results

Destination IP or Hostname – specify hostname or IP address of the target host.

Max Hops –Specifies the maximum number of hops to search for target.

Start/Stop – click to start or stop traceroute tool.

Spectrum Analyzer

The **Spectrum analyzer** test displays detailed information about signal level of each APC unit's antenna on each available frequency. This enables administrator choose the best available frequency/channel for the unit operation. The frequency list depends on the Country at which the unit is operating, and chosen channel width.

> ⚠️ Do not use the Spectrum analyzer on the remote unit of the link, as the connection to the device will be lost during the test.

Click **Start** button to perform the test:

Figure 66 – Spectrum Analyzer Results
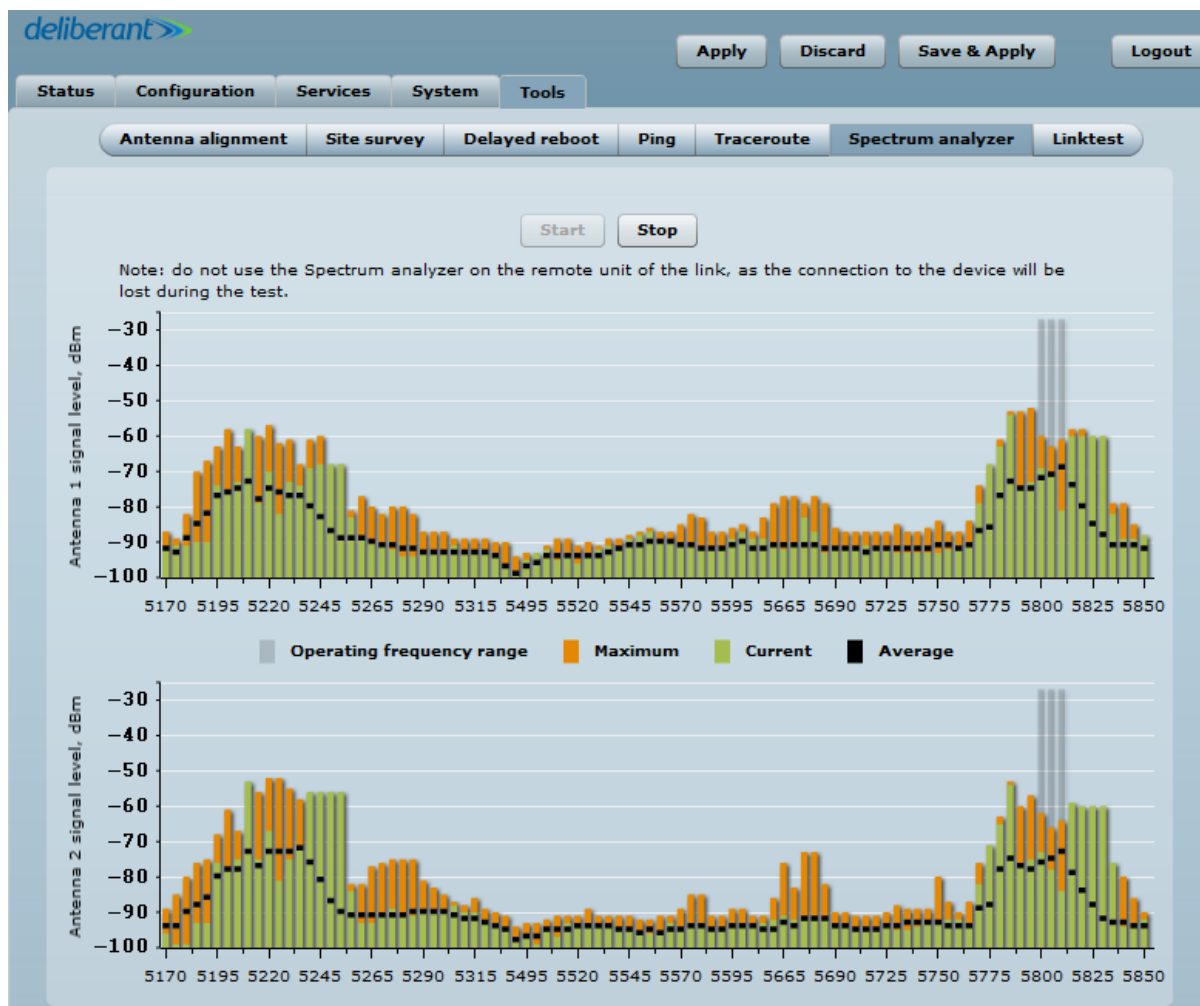
Operating frequency range – displays the channel frequency range at which the APC unit is operating currently.

Maximum – color indicates a the maximum achieved signal level on the appropriate frequency.

Current – color indicates the current signal level on the appropriate frequency.

Average – indicates average of the signal level on the appropriate frequency.

Link Test

> It is recommended to ensure that there is no traffic on the link before running the Link Test as results may not be completely accurate.

Use the Link test tool to check the quality of the established link. This tool tests the throughput at selected packet sizes and iterations. Results represent the maximum, minimum and average value of the performed test.
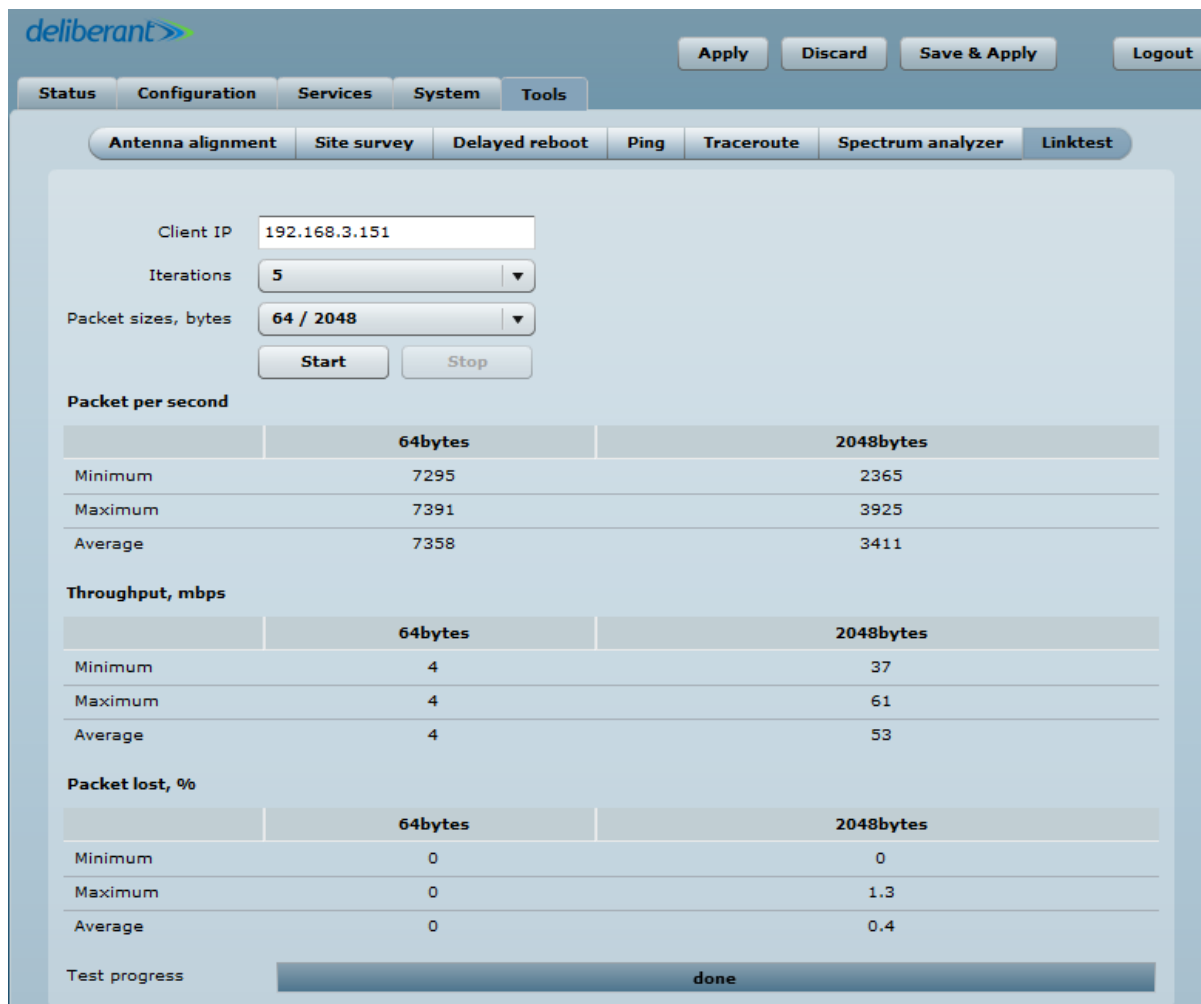
Figure 67 – UAM Login Page

Figure 68 – Linktest Results

Client IP - specify the connected client's IP address.

Iterations - specify number of test iterations.

Packet sizes - specify packet sizes in bytes at which the test will be performed.

Start – click to start the throughput test.

Stop – click to stop the throughput test.

Universal Access Method (UAM)

Universal Access Method (UAM) is a simple Web browser based user authentication method. On initial HTTP request to any Web site, client's browser is redirected to the authentication page for login to the network. The login page can be served by internal Web server or by external Web Application Server.

UAM Overview

When using internal UAM, the **Login** page is the first page a client receives when he starts his Web browser and enters any URL. To get access to the network, the user should enter his authentication settings: **login name** and **password** and click the **login** button:

My HotSpot

Welcome to my HotSpot!

You can use the Internet, but have to login first.
You must also agree to these terms and conditions.

Username [   ]
Password [   ]
[Login & Accept Terms]

Figure 69 – UAM Login Page

The DLB APC could be shared by several Wireless Internet Service Providers (WISP). They are uniquely identified by specifying WISP domain name in addition to subscriber user name when logging in. APC can be configured to send authentication and accounting information to different Authentication, Authorization, and Accounting (AAA) servers associated with different WISP domains.

> Subscriber's login format:
> - username

UAM Configuration

> UAM authentication is available on radio interfaces (including VAPs) only if DLB APC is working as **router** in **Access Point (auto WDS)** wireless mode.

The APC allows user authentication through external or internal Web portal. This authentication method is called UAM. User provides login credentials and then Web portal attempts to authenticate and authorize the client using the provided information. Client will not send any authentication requests directly to the APC, the Web portal will do this. On success, APC will allow access to the Internet; otherwise Web portal will display failure notice.

Use Security section on Wireless or VAP (depending on the interface on which the UAM will be configured) page for UAM configuration: choose the security option UAM:

Figure 70 – UAM Settings

RADIUS Settings

NAS ID – specify the NAS identifier.

RADIUS server 1 – specify the name or IP address of the primary RADIUS server.

RADIUS server 2 – specify the name or IP address of the secondary RADIUS server.

RADIUS secret – specify the RADIUS shared secret.

RADIUS authentication port – specify the UDP port number to use for radius authentication requests, default 1812

RADIUS accounting port – specify the UDP port number to use for radius accounting requests, default 1813

RADIUS WEB page type – choose the authentication Web portal type:

▪ **Internal** – use the built in authentication Web page. If selected, then when a users first tries to access the Internet, they will be blocked, and re-directed to the built-in login page. The logon data will be sent to the Radius Server for authentication.
▪ **External** – specify the external authentication Web page URL and settings. If selected, then when a user first tries to access the Internet, they will be blocked, and re-directed to the URL specified

below.

- **Custom internal** – upload a customized internal page.

Use HTTPS – enable to use the HTTPS protocol for connection and authentication.

- **Key** – upload a PEM formatted private key file.
- **Certificate** – upload a PEM formatted certificate file.

WISPr Settings

    WISPr location name – specify the WISPr location name.

    Operator name – specify the operator's name

    Network name – specify the network name

    ISO country code – specify the country code in ISO standard.

    E.164 country code – specify the country code in E.164 standard.

    E.164 area code – specify the area code in E.164 standard.

WISPr default max bandwidth – specify the default bandwidth limitation for clients. Note that if the external RADIUS server has traffic limitations preconfigured, then RADIUS overrides these settings.

    Download, kbps – specify max download bandwidth in kbps.

    Upload, kbps – specify the max upload bandwidth in kbps.

UAM config auto update - select for automatically UAM configuration update. If enabled, the APC will download and apply the configuration form the specified URL each specified time.

- **UAM config URL** - specify the URL where the UAM configuration will be downloaded from.
- **Update mode** - select the automatic UAM configuration update mode: time or interval.
  - **Interval** - in this mode UAM configuration will be downloaded and set on device each specified period.
  - **Time** - in this mode UAM configuration will be downloaded and set on device at a specified time, daily.
- **Time** - specify time period in hh:ss format.
- **View config** - click to view last downloaded configuration file.

Interface IP address – specify the LAN interface IP address. Note that LAN settings on Network menu will be disabled if UAM is enabled.

DHCP settings – specify the dynamic IP settings for the connected users:

    Network – specify the network for IP address pool.

    Subnet mask – specify the subnet mask for the DHCP.

    DNS server – specify the primary and the secondary DNS servers.

Data encryption settings – choose the data encryption method:

- **Open** – no encryption.
- **Personal WPA** – preshared key encryption with WPA using AES method.
- **Personal WPA 2** – preshared key encryption with WPA2 using AES method.

White/Black List

The white and black access lists control user access to Web content through the APC. The unauthenticated users will be allowed to access sites from white list while access to the sites from black list will be denied even for authenticated users.

Figure 71 – White List and Black List

W/B list auto update - select for automatically White/Black list update. If enabled, the APC will download and apply the White/Black list form the specified URL each specified time.

- **W/B list URL** - specify the URL where the White/Black list will be downloaded from.
- **Update mode** - select the update mode: time or interval.
  - **Interval** - in this mode White/Black list will be downloaded and applied each specified period.
  - **Time** - in this mode White/Black list will be downloaded and applied at a specified time, daily.
- **Time** - specify time period in hh:ss format.
- **View W/B list** - click to view last downloaded White/Black list.

> ℹ️ Example of White/Black list format for auto update:
> ```
> whitelist avp.innity.com,www.tm.com.my,m3.innity.net,pb2.ipass.com,
> avn.innity.com,1.innity-.innity.net,tmpoint.tm.com.my,m4.innity.net
> blacklist
> ```

For manual white/black list configuration, use "**+**" sign to add new entry to the list, and "**–**" sign to remove required one.

White list

Host/IP address – specify the IP addresses or hosts for free access even for unauthenticated users.

Notes – add a description for the specified host or IP address.

Black list

Host/IP address – specify the IP addresses or hosts that will be not accessible even for the authenticated users.

Notes – a description for the specified host or IP address.

AP Keep Alive Monitoring

The AP keep alive function allows checking device availability on a specified remote server.

Figure 72 – AP Keepalive Configuration

Enable monitoring - select to enable AP keep alive monitoring.

Monitor test URL - specify the remote URL for device periodical polling.

Interval - specify polling interval in hh:mm format.

Appendix

A) Resetting Device to Factory Defaults

Device has the capability of being reset to defaults by pinging the device with a certain packet size when the radio is booting. During the startup of the device, when the drivers of the Ethernet interfaces are loaded, the discovery daemon is started. The daemon suspends startup process for 3 seconds and waits for ICMP "`echo request`" packet of length 369 bytes. If the packet received, the discoveryd resets the device to default configuration.

> It is recommended to connect PC to the device via switch, as depending on PC OS settings, the ARP table might be flushed during wired link status change (connecting the device that will be reset).

Steps to reset to default settings:

Step 1.   Power off the APC device.

Step 2.   Obtain the device MAC address.

Step 3.   Connect a PC to the same physical subnet as the device.

Step 4.   Execute 'arp -s' command to assign the IP address (IP address should be from the same subnet as PC) to the device MAC address:

arp -s <IP address to assign> <device MAC address>

> Note that syntax of MAC address differs depending on OS:
> - Linux OS: AA:BB:CC:DD:EE:FF
> - Windows OS: AA-BB-CC-DD-EE-FF

Step 5.   Start ping the device:

> **For Linux users:** ping <IP address> -s 369
>
> **For Windows users:** ping <IP address> -l 369 -t -w 0.2

Step 6.   Power up APC device and wait about 30sec or more (depending on device hardware).

Step 7.   Stop pinging the device, and let the device boot as usual. The device should start up with factory default settings.

B) RADIUS Attributes

The following RADIUS attributes and messages are supported by the DLB APC.

General Attributes

Attribute	Description
User-name (1)	Full username as entered by the user.
User-Password (2)	Used for UAM as alternative to CHAP-Password and CHAP-Challenge.
CHAP-Password (3)	Used for UAM CHAP Authentication
CHAP-Challenge (60)	Used for UAM CHAP Authentication
EAP-Message (79)	Used for WPA Authentication
NAS-IP-Address (4)	IP address of Chilli (set by the *nasip* or *radiuslisten* option, and otherwise "0.0.0.0")
Service-Type (6)	Set to Login (1) for normal authentication requests. The Access-Accept message from the radius server for configuration management messages must also be set to Administrative-User.
Framed-IP-Address (8)	IP address of the user, which is configurable during MAC authentication in the Access-Accept.
Filter-ID (11)	Filter ID pass on to scripts possibly.
Reply-Message (18)	Reason of reject if present.
State (24)	Sent to chilli in Access-Accept or Access-Challenge. Used transparently in subsequent Access-Request.
Class (25)	Copied transparently by chilli from Access-Accept to Accounting-Request.
Session-Timeout (27)	Logout once session timeout is reached (seconds)
Idle-Timeout (28)	Logout once idle timeout is reached (seconds)
alled-Station-ID (30)	Set to the nasmac option or the MAC address of chilli.
Calling-Station-ID (31)	MAC address of client
NAS-Identifier (32)	Set to radiusnasid option if present.
Acct-Status-Type (40)	1=Start, 2=Stop, 3=Interim-Update
Acct-Input-Octets (42)	Number of octets received from client.
Acct-Output-Octets (43)	Number of octets transmitted to client.
Acct-Session-ID (44)	Unique ID to link Access-Request and Accounting-Request messages.
Acct-Session-Time (46)	Session duration in seconds.
Acct-Input-Packets (47)	Number of packets received from client.
Acct-Output-Packets (48)	Number of packets transmitted to client.
Acct-Terminate-Cause (49)	1=User-Request, 2=Lost-Carrier, 4=Idle-Timeout, 5=Session-Timeout, 11=NAS-Reboot
Acct-Input-Gigawords (52)	Number of times the Acct-Input-Octets counter has wrapped around.
Acct-Output-Gigawords (53)	Number of times the Acct-Output-Octets counter has wrapped around.
NAS-Port-Type (61)	19=Wireless-IEEE-802.11
Message-Authenticator (80)	Is always included in Access-Request. If present in Access-Accept, Access-Challenge or Access-reject chilli will validate that the Message-Authenticator is correct.
Acct-Interim-Interval (85)	If present in Access-Accept chilli will generate interim accounting records with the specified interval (seconds).
MS-MPPE-Send-Key (311,16)	Used for WPA
MS-MPPE-Recv-Key (311,17)	Used for WPA

WISPr Attributes

Attribute	Description
WISPr-Location-ID (14122, 1)	Location ID is set to the radiuslocationid option if present. Should be in the format: isocc=, cc≤E.164_Country_Code>, ac≤E.164_Area_Code>, network≤ssid/ZONE>
WISPr-Location-Name (14122, 2)	Location Name is set to the radiuslocationname option if present. Should be in the format: ,
WISPr-Logoff-URL (14122, 3)	Included in Access-Request to notify the operator of the log off URL. Defaults to " http://uamlisten:uamport/logoff".
WISPr-Redirection-URL (14122, 4)	If present the client will be redirected to this URL once authenticated. This URL should include a link to WISPr-Logoff-URL in order to enable the client to log off.
WISPr-Bandwidth-Max-Up (14122, 7)	Maximum transmit rate (b/s). Limits the bandwidth of the connection. Note that this attribute is specified in bits per second.
WISPr-Bandwidth-Max-Down (14122, 8)	Maximum receive rate (b/s). Limits the bandwidth of the connection. Note that this attribute is specified in bits per second.
WISPr-Session-Terminate-Time (14122, 9)	The time when the user should be disconnected in ISO 8601 format (YYYY-MM-DDThh:mm:ssTZD). If TZD is not specified local time is assumed. For example a disconnect on 18 December 2001 at 7:00 PM UTC would be specified as 2001-12-18T19:00:00+00:00.

ChilliSpot Attributes

Attribute	Description
ChilliSpot-Max-Input-Octets (14559, 1)	Maximum number of octets the user is allowed to transmit. After this limit has been reached the user will be disconnected.
ChilliSpot-Max-Output-Octets (14559, 2)	Maximum number of octets the user is allowed to receive. After this limit has been reached the user will be disconnected.
ChilliSpot-Max-Total-Octets (14559, 3)	Maximum total octets the user is allowed to send or receive. After this limit has been reached the user will be disconnected.
ChilliSpot-Bandwidth-Max-Up (14559, 4)	Maximum bandwidth up
ChilliSpot-Bandwidth-Max-Down (14559, 5)	Maximum bandwidth down
ChilliSpot-Config (14559, 6)	Configurations passed between chilli and back-end as name value pairs
ChilliSpot-Lang (14559, 7)	Language selected in user interface
ChilliSpot-Version (14559, 8)	Version of Chilli sending this AccessRequest

Index