Поставщик систем безопасности TELECAMERA.RU

Dahua V-Radio Wireless Transmission Device

User Guide

DH-PFWB2-30n、DH-PFWB2-60n、DHPFWB2-90n、
DH-PFWB5-10n、DH-PFWB5-30n、DH-PFWB5-90n、
DH-PFWB5-10ac、DH-PFWB5-30ac、DH-PFWB5-90ac

July 25, 2018

Copyright

© 2016 Dahua

This user's guide and the software described in it are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Dahua.

Notice

Dahua 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. Dahua 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 Dahua.

Trademarks

Dahua logo is trademark of Dahua LLC.

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

FCC warning

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

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

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

FCC caution

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

FCC radiation exposure statement

To comply with FCC RF exposure requirements in section 1.1307, a minimum separation distance of 3.9 feet is required between the antenna and all occupational persons, and a minimum separation distance of 8.7 feet is required between the antenna and all public persons.

CE mark warning

This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

R&TTE compliance statement

This equipment complies with all the requirements of the Directive 1999/5/EC of the European Parliament and the Council of 9 March 1999 on Radio Equipment and Telecommunication Terminal Equipment and the Mutual Recognition of their Conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this manual and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU countries intended for use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states Iceland, Liechtenstein, Norway and Switzerland.

EU countries not intended for use

None.

Contents

About This Guide

Purpose

This document provides information and procedures on installation, setup, configuration, and management of Dahua wireless device.

Definitions, acronyms and abbreviations

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

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
ACK	Acknowledgement
AES	Advanced Encryption Standard
AMSDU	Aggregated Mac Service Data Unit
AP	Access Point
ATPC	Automatic Transmit Power Control
CCQ	Client Connection Quality
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

Abbreviation	Description
LAN	Local Area Network
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabits per second
MCS	Modulation and Coding Scheme
MHz	Megahertz
MIMO	Multiple Input, Multiple Output
MSCHAPv2	Microsoft version of the Challenge-handshake authentication protocol, CHAP.
NAS	Network Access Server
NAT	Network Address Translation
NTP	Network Time Protocol
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
RADIUS	Remote Authentication dial In User Service
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
SSH	Secure Shell
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
WACL	Wireless Access Control List
WDS	Wireless Distribution System
WEP	Wired Equivalent Privacy
WISPr	Wireless Internet Service Provider roaming
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia

Abbreviation	Description
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Device Access

First connection via Ethernet

By default device obtains the IP address from the DHCP server.

In case the device is unable to obtain IP address from a DHCP server, it fallback to the default static IP 192.168.1.36.

First access to web management interface

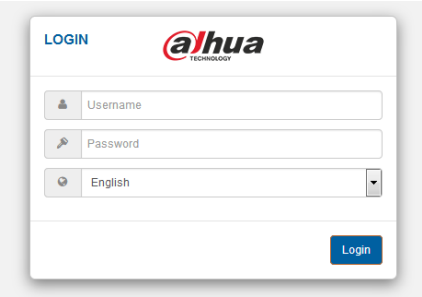
The default administrator login settings are:
Login: **admin**
Password: **admin**

Follow the steps for first connection to the device web management interface:

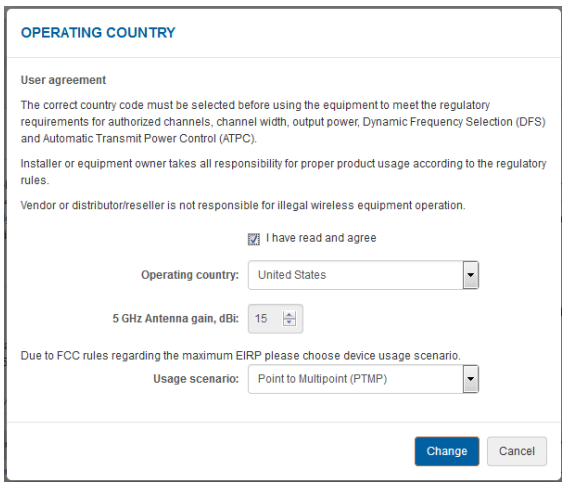
Step 1. Start your Web browser.

Step 2. Enter the device IP address in the web browser's IP field and specify default login settings **admin/admin**.

The initial login screen looks as follow:



Step 3. **Confirm the user agreement.** 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. Usage scenario should be chosen according to actual scenario the device will be used in.



If you choose Point to Point(PTP) as Usage scenario and click Change, the device will not allow more than 1 client unit to connect to it, and Usage scenario can not be changed until you reset the device to factory defaults.

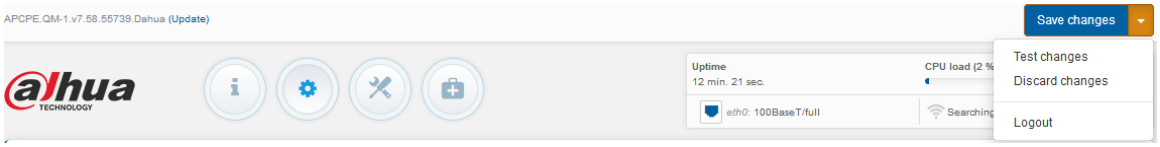
Step 4. After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

Configuration

This document contains powerful web management interface configuration description allowing setups ranging from very simple to very complex.

Saving configuration changes

There is one general button containing three actions located on the right top corner of the WEB GUI allowing managing device configuration:



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

Test changes – if pressed the device will start operating with newly set configuration settings for 3 minutes. During this test time the administrator is able to gauge if device is working properly, and then Save changes. In case wrong settings were chosen (or even after faulty settings administrator have lost connection with the device), the device automatically reverts back configuration to an old one.

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

It is not required to press **Save changes** 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.

Status

After login, the main Web management page displays Status Information page. The header of Web management displays main information about device: Firmware version, Product name, Uptime, CPU load, Ethernet port(s) status, Connected client count on each radio.

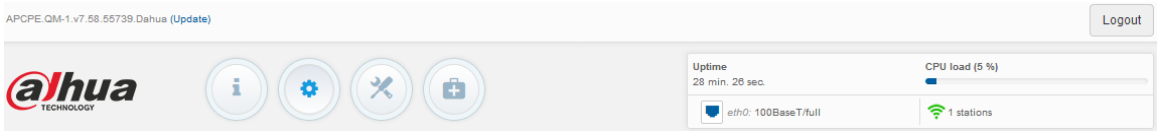


Figure 1 - Web Management Interface

Information

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

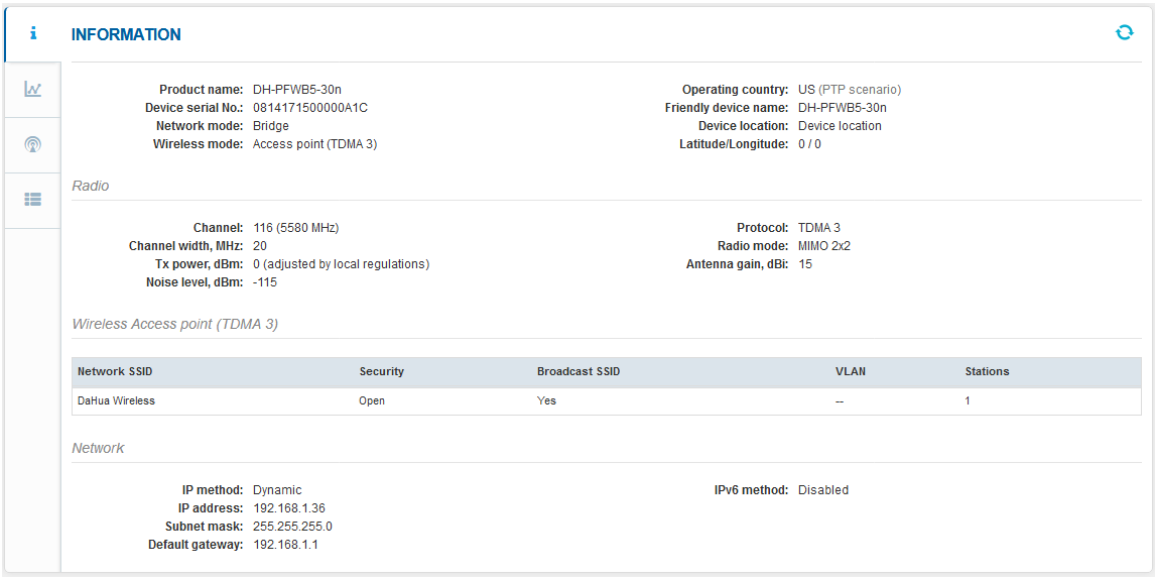


Figure 2 – Device Information Page

If wireless device is dual-band, then **Radio** section on Information page will be divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate information.

Radio – displays summary of the radio interface configuration.

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

- **Access point (autoWDS),** and **(Access Point (TDMA 3)** – displays access point operating information: SSID, Security type, SSID Broadcast status, VLAN and number of connected clients.
- **Station (WDS /TDMA 3)** and **Station (ARPNAT)** – displays settings at which the station is connected to the access point: SSID, Security type, Peer's MAC address, Tx/Rx rate, Protocol.

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

Click the refresh icon, on the upper right corner, to update information.

Statistics

The **Statistics** sections id divided into two sections and displays network interface counters, wireless traffic optimization and traffic graphs of wired and wireless interfaces:

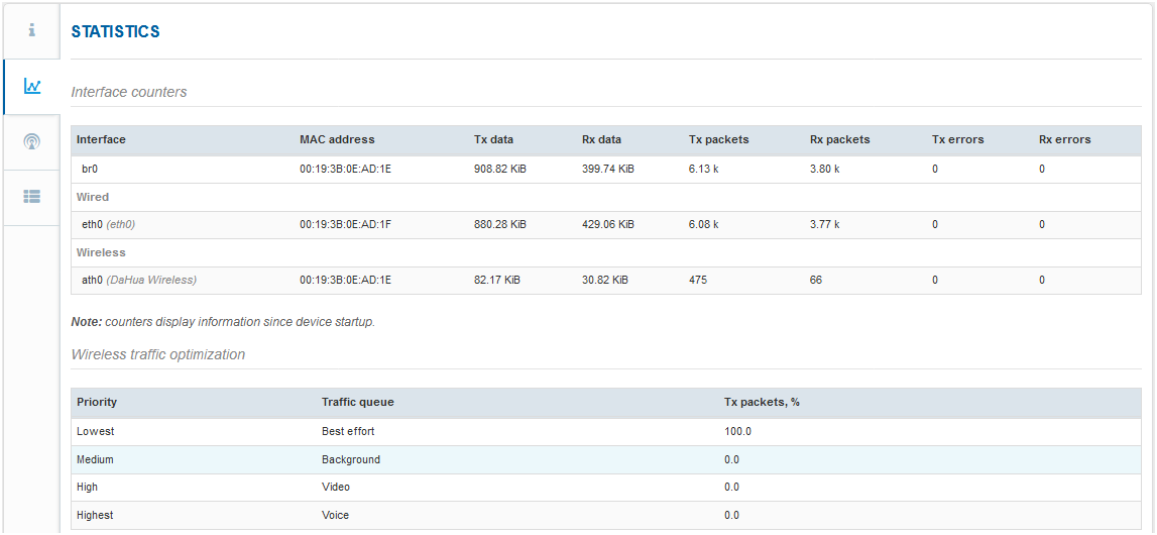


Figure 3 – Device Network Statistics

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

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

Tx data – displays the transmitted data.

Rx data – displays the received data.

Tx packets – displays the number of transmitted packets.

Rx packets – displays the number of received packets.

Tx errors – displays the number of the TX errors.

Rx errors – displays the number of the RX errors.

Wireless traffic optimization – represents QoS prioritized traffic statistics if *Traffic Management* is enabled.

The wired and wireless interface graphs display real-time data traffic.

Figure 4 – Network Statistics: Graphs

If device is working as a Station, the additional graph of the signal and noise levels will be displayed.

Wireless Networks

Status Wireless section is not available if device is operating as Station (WDS/ TDMA3) or Station (ARPNAT). In this case all necessary information about wireless connection with AP unit will be on *Information* page, wireless table.

The Wireless page displays the receive/transmit statistics between AP and successfully associated wireless clients (click **Counters** tab, if necessary to view information of connected clients in Rx/Tx numerical expressions):

Figure 5 – Access Point's Wireless Statistics

If device is dual-band, then Wireless page will be divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate information.

Station – displays MAC address and Friendly name of the successfully connected wireless client.

IP address – displays wireless client IP address.

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

Tx/Rx rate – displays transmit/receive data rates in Mbps.

Tx/Rx CCQ, % - displays the wireless Client Connection Quality (CCQ), the value in percent that shows how effective the bandwidth is used regarding the theoretically maximum available bandwidth.

Protocol – displays the protocol at which the access point communicates with the particular station.

Link uptime – displays the duration of the particular session.

Kick selected – select to end the connection to this station.

Click the refresh icon, on the upper right corner, to update statistics.

Network

The **Network** page displays networking information: routing table, ARP table (Address Resolution Protocol) table currently recorded on the device and DHCP lease table:

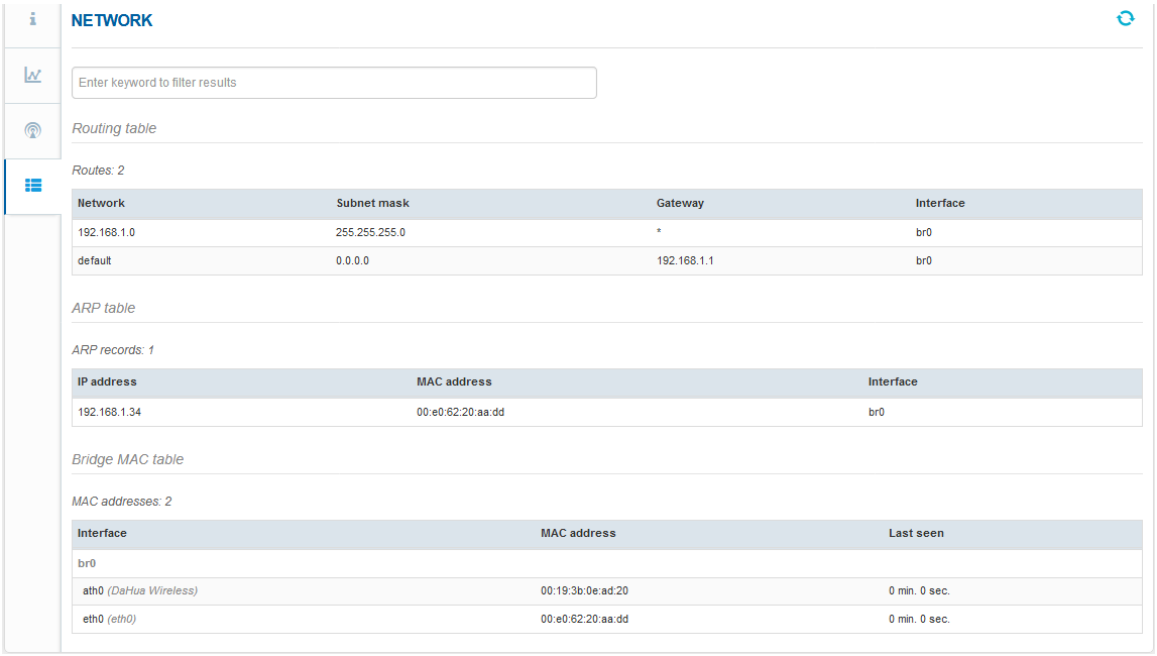
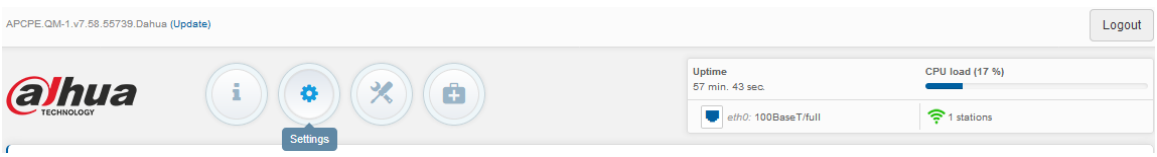


Figure 6 – Networking Tables

DHCP client table is displayed only if unit operates in Router mode with DHCP server enabled.

Settings



Network configuration

The **Settings | Network Configuration** page allows you to control the network configuration of the device. First, the device operation mode must be defined to work as a bridge or router (IPv4 or IPv6). The content of the window varies depending on your selection:

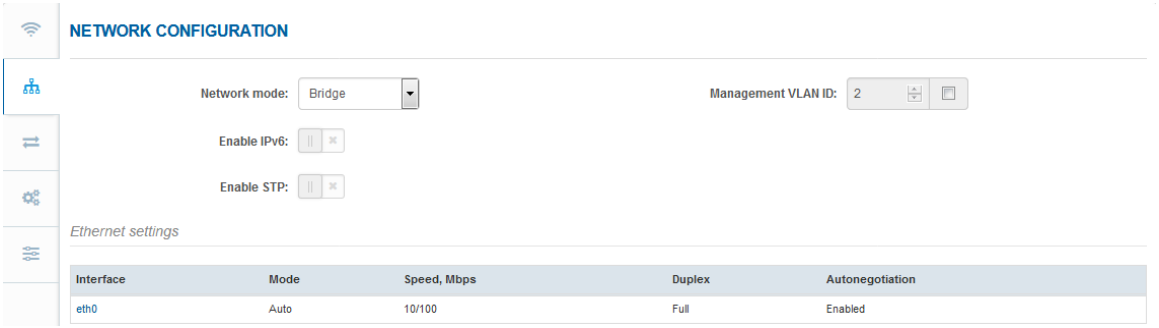


Figure 7 – Network Mode Options

Network mode – choose the device operating mode. Network settings will vary according to the selected Network mode. The Bridge mode allows configuring device IPv4 and IPv6 LAN IP settings, while the Router mode requires more parameters such as LAN network settings, WAN network settings, LAN DHCP settings.

Ethernet settings

The **Ethernet settings** table allows configuring the ETH interface settings

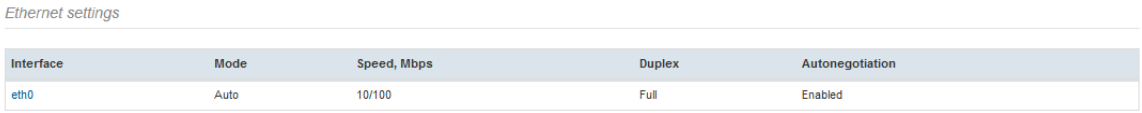


Figure 8 – Ethernet Settings Table

Click on the required Ethernet interface name and configure parameters:

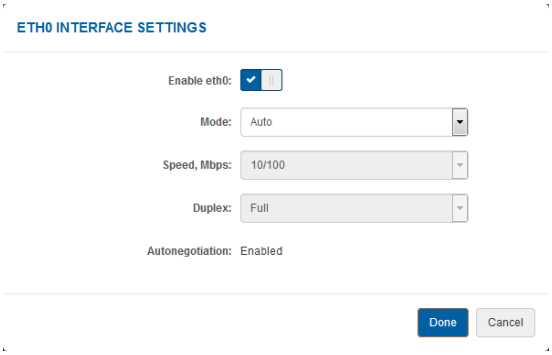


Figure 9 – Ethernet Interface Configuration

Mode – select the Ethernet port configuration mode:

- Auto
- Fixed
- Advanced

Speed, Mbps – select the Ethernet link speed of the particular Ethernet port.

Duplex – select the duplex mode of the particular Ethernet port.

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

Bridge

When device is configured to operate in Bridge mode, only device LAN settings should be configured on the **Network configuration** page:

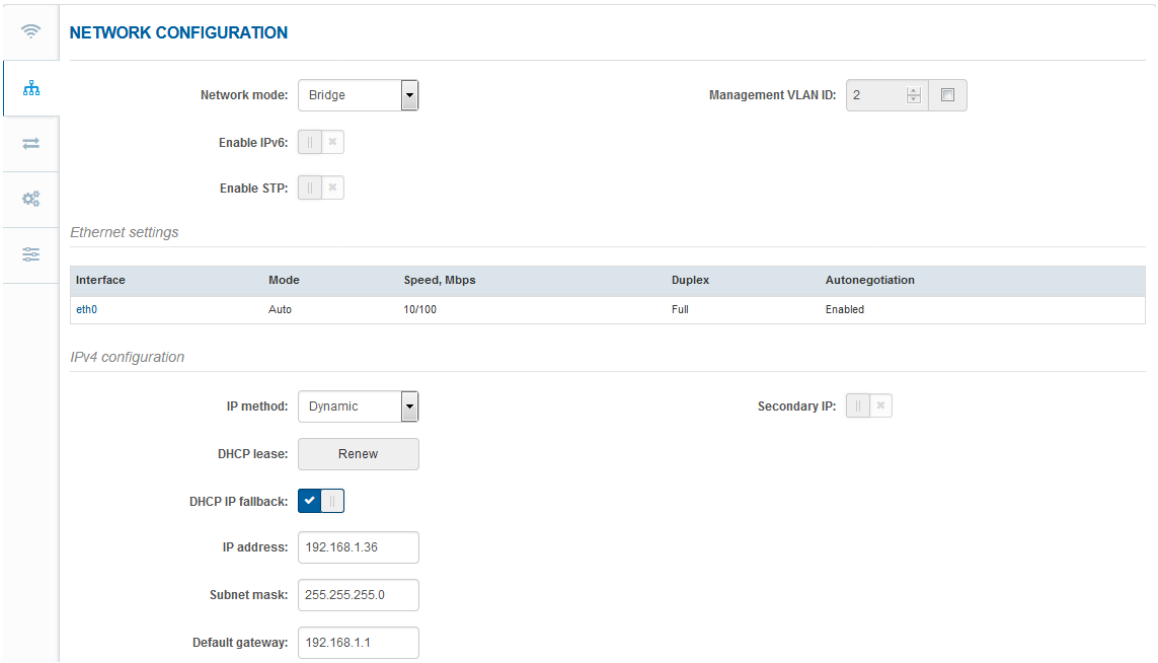


Figure 10 – Bridge Mode Settings

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

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.

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.

IPv4 Configuration

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.

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

- **Static** – the IP address must be specified manually.
- **Dynamic** – 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.

Secondary IP – specify the alternative IP address and the netmask for device management.

IPv6 Configuration

Click the **IPv6** slide to enable IPv6 configuration. IPv6 settings will appear under the **IPv6 configuration** section:

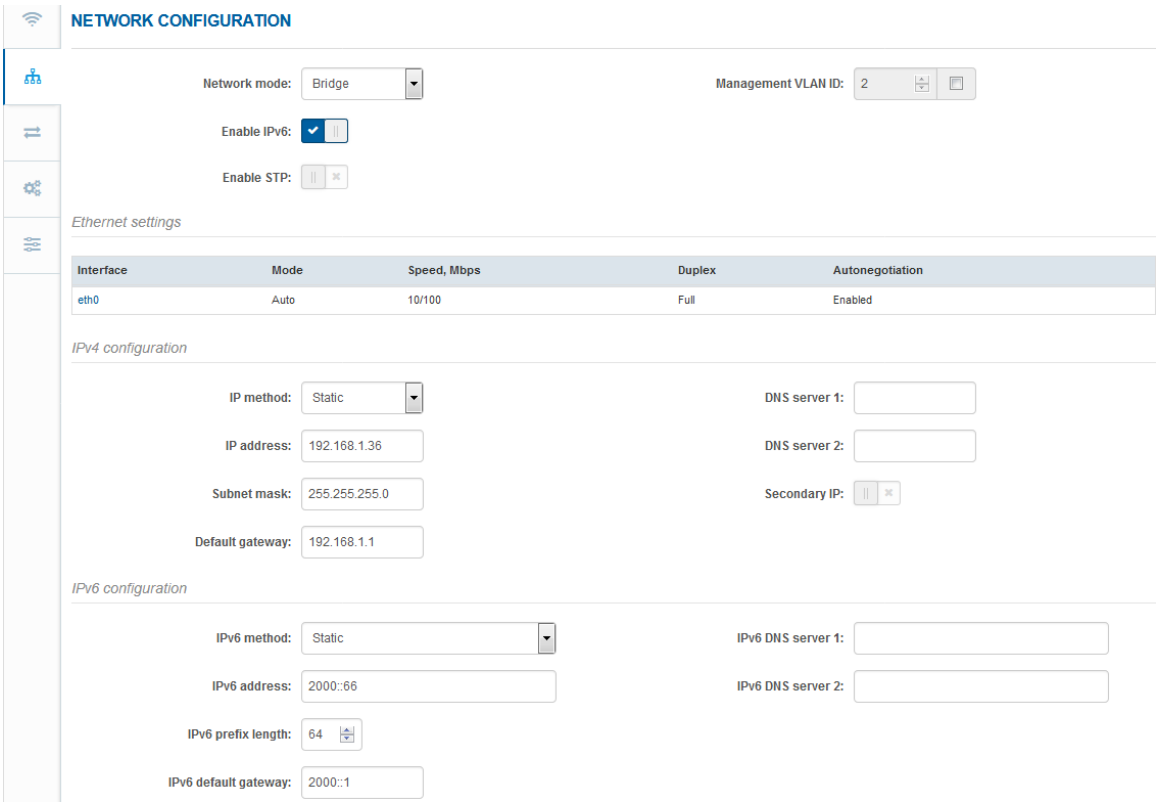


Figure 11 – Bridge IPv6 Settings

IPv6 method – specify IPv6 reception method: IPv6 addresses can either be retrieved from a DHCPv6 server or configured manually:

- **Dynamic stateless IP** – the DHCPv6 client only obtains network parameters other than IPv6 address
- **Dynamic stateful IP** – the DHCPv6 clients require IPv6 address together with other network parameters (e.g. DNS Server, Domain Name, etc.).
- **Static** – the IPv6 address must be specified manually.
  - **IPv6 address** – specify the **IPv6 Address** for the interface.
  - **IPv6 prefix length**– enter the **Prefix Length** for the address.
  - **IPv6 default gateway** – specify IPv6 address for default gateway.
  - **IPv6 DNS server** – specify the Domain Naming Server IPv6 addresses.

Router IPv4

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

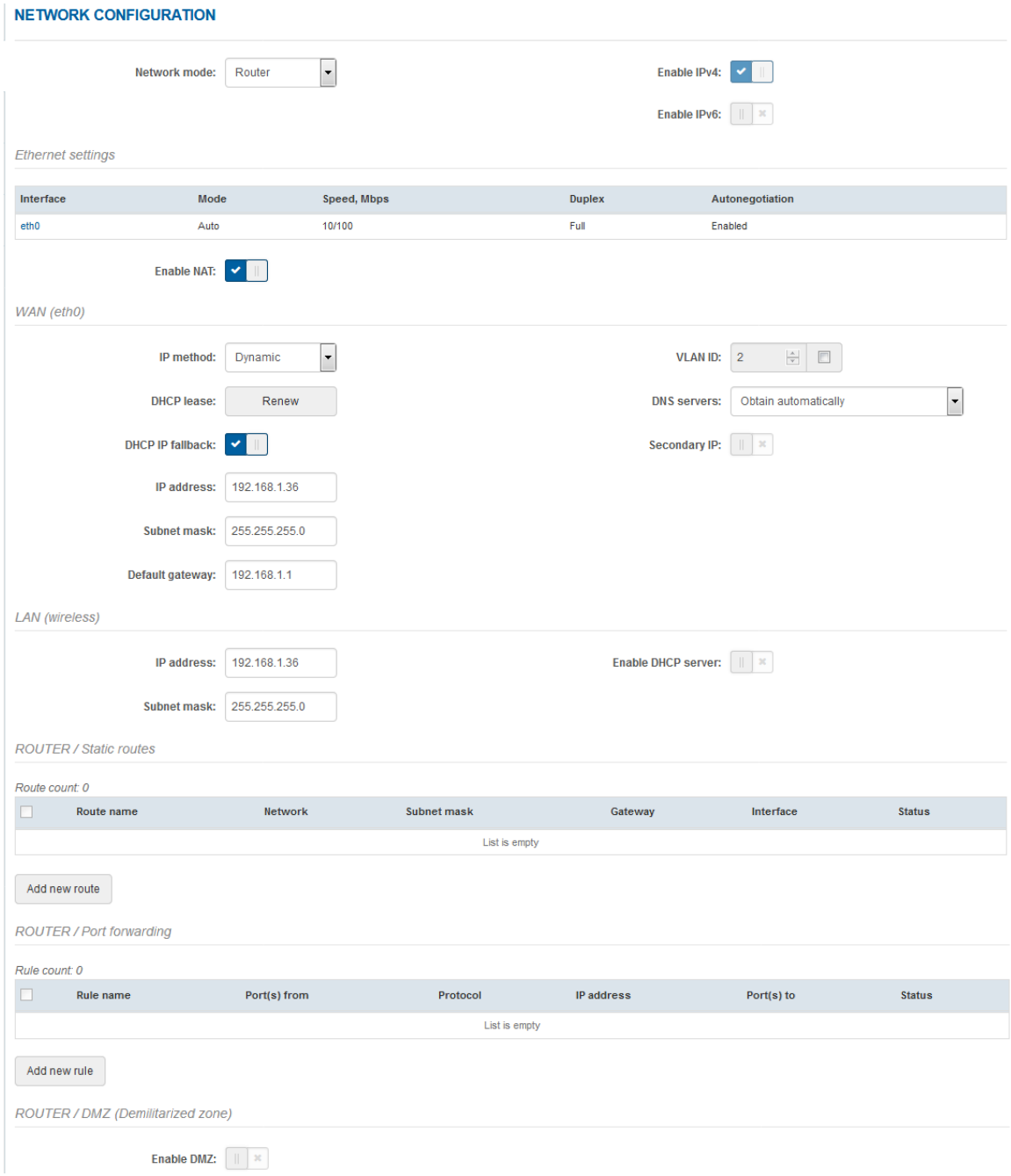


Figure 12 – Router IPv4 Settings

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.

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.

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

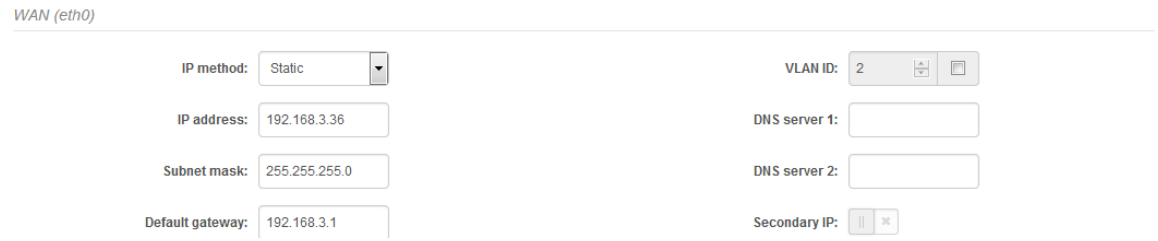


Figure 13 – Router IPv4 WAN Settings: Static IP

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

Secondary IP – enable to specify the alternative IP address and the netmask for device management.

WAN mode – choose **Dynamic** to enable DHCP client on the WAN side and get IP address from the running DHCP server:

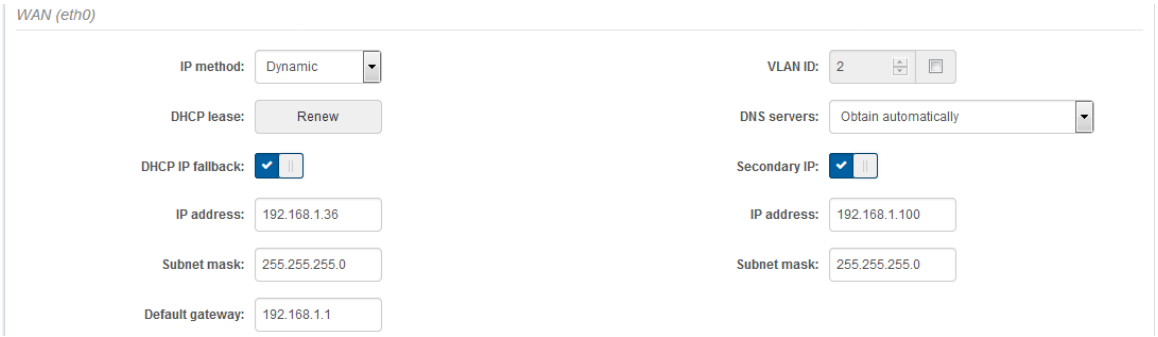


Figure 14 – Routers IPv4 WAN Settings: Dynamic IP

DHCP fallback setting – specify IP address, Subnet mask, Default gateway and optionally DNS server for DHCP fallback. In case the device 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 device management.

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

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

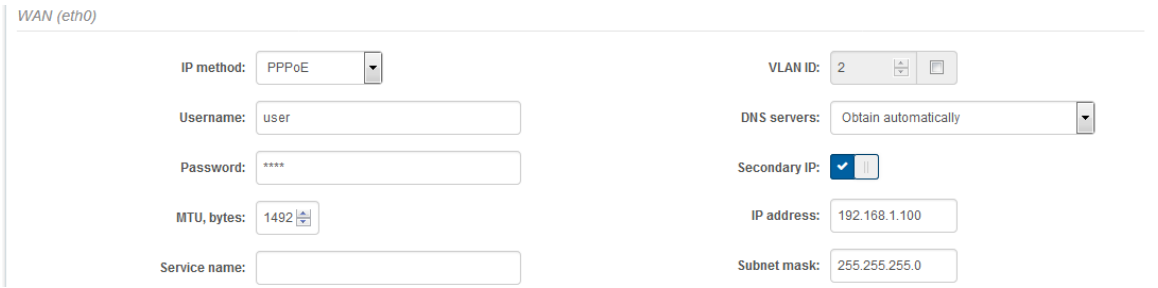


Figure 15 – Routers IPv4 WAN Settings: PPPoE client

User name – specify the user name for PPPoE.

Password – specify the password for PPPoE.

MTU – specify the MTU (Maximum Transmission Unit) in bytes.

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

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

LAN Network Settings

LAN configuration include settings related to the LAN interface.

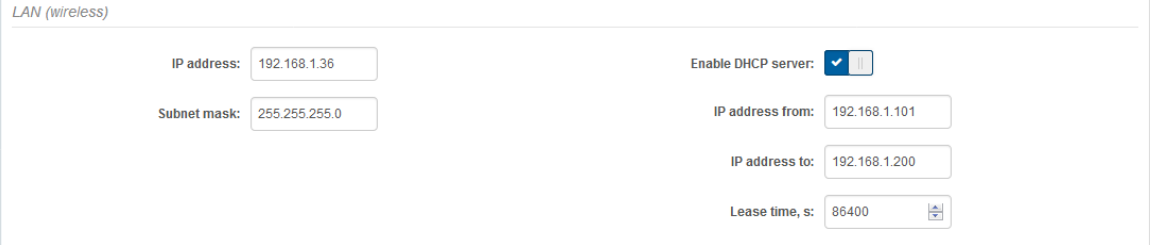


Figure 16 – Router LAN Settings

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

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

Enable DHCP server – select to enable DHCP server on LAN interface.

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

Static Routes

Static routes is active only in Router IPv4 network mode.

Use **Settings | Network Configuration** page for configuring Static routes. Routing rule is defined by the destination subnet (Destination IP address and netmask) and gateway where to route the target traffic.

To add a new static route, click on **Add new route** button under the Routing table and specify the following parameters:

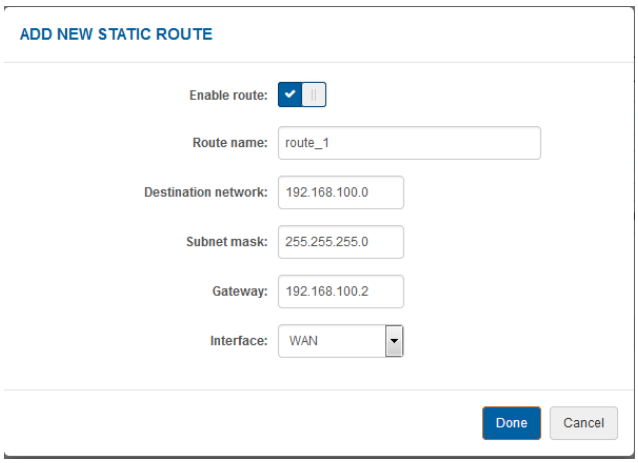


Figure 17 - Static Route Configuration

Enable route – slide to enable or disable route. This option allows disable particular route without deleting it.

Route name – specify a name for the particular route.

Destination network – specify the destination network IP address.

Subnet mask – specify destination netmask.

Gateway – specify the gateway address for the route.

Interface – select the routing interface from the drop-down.

After saving the route settings, the new route will be added in the routing table on **Settings| Network configuration** page:

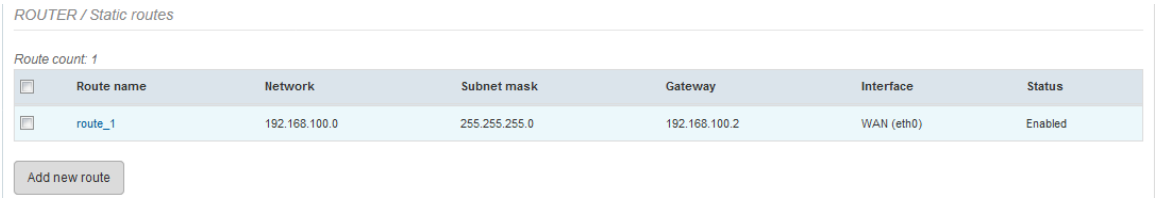


Figure 18 - Static Route Table

Port Forwarding

Port Forwarding is available only in Router IPv4 network mode.

Use **Settings | Network Configuration** page for configuring Port forwarding. 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 it is possible to pass traffic through to these private IP addresses.

To add a new Port forwarding rule, click on **Add new rule** button under the Port forwarding table and specify the following parameters:

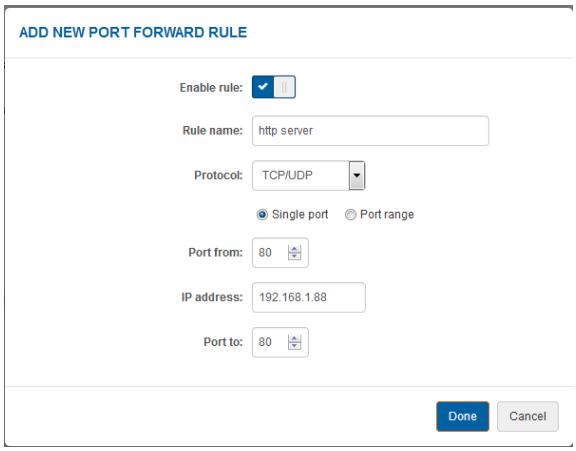


Figure 19 - Port Forward Configuration

Enable rule – slide to enable or disable Port forwarding rule. This option allows disable particular rule without deleting it.

Rule name – specify a name for the particular Port forwarding rule.

Port from– specify the TCP/UDP port from which the selected traffic should be forwarded.

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

IP address – specify the IP address that specified traffic will get forwarded to.

Port to – specify TCP/UDP port to which the selected traffic shall be forwarded.

After saving the new Port forwarding rule, it appears in the routing table on **Settings| Network configuration** page:

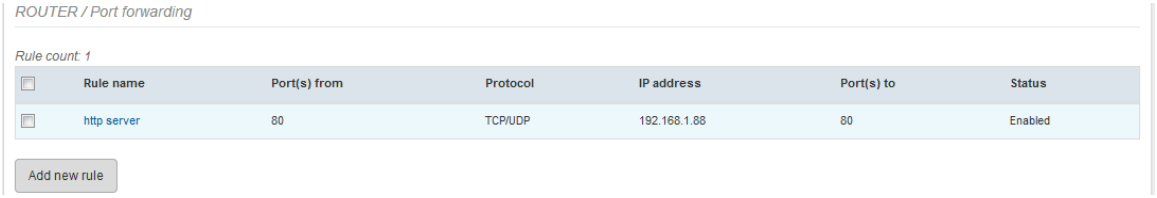


Figure 20 - Port Forward Table

Router IPv6

To setup IPv6 router, select the **Network mode** as **Router IPv6** and specify the required WAN and LAN settings.

IPv6 WAN (wired) settings: Dynamic Stateless

With Dynamic stateless IPv6, device generates its own IP address by using a combination of locally available information and router advertisements, but receives DNS server information from a DHCPv6 server. The IP address is a dynamic address.

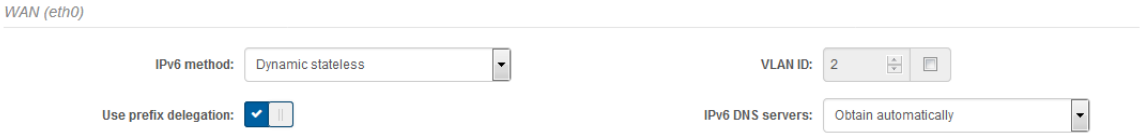


Figure 21 – IPv6 Router WAN Settings: Dynamic Stateless IP

Use prefix delegation – if enabled, a prefix (IP address block) is delegated from Internet service provider to customer's network (LAN).

IPv6 DNS servers – choose the DNS servers for IPv6 connection:

- **Obtain automatically** – if selected, the DNS servers will be used automatically from ISP.
- **Use following** – specify IPv6 DNS servers manually.

IPv6 WAN (wired) settings: Dynamic Stateful

With Dynamic stateful IP, device obtains an interface address, configuration information such as DNS server information, and other parameters from a DHCPv6 server. The IP address is a dynamic address.

Figure 22 – IPv6 Router WAN Settings: Dynamic Stateful

Use prefix delegation – if enabled, a prefix (IP address block) is delegated from Internet service provider to customer's network (LAN).

IPv6 DNS servers – choose the DNS servers for IPv6 connection:

- **Obtain automatically** – if selected, the DNS servers will be used automatically from ISP.
- **Use following** – specify IPv6 DNS servers manually.

IPv6 WAN (wired) settings: Static

With this IPv6 method selected, LAN and WAN settings must be specified manually:

Figure 23 – IPv6 Router WAN Settings: Static IPv6

IPv6 address – specify the **IPv6 address** for the interface.

IPv6 prefix length– enter the **prefix length** for the address (default is 64).

IPv6 default gateway – specify IPv6 address for default gateway.

IPv6 DNS server – specify the Domain Naming Server IPv6 addresses.

IPv6 WAN (wired) settings: PPPoE

With this method device will get WAN interface IPv6 address via PPPoE.

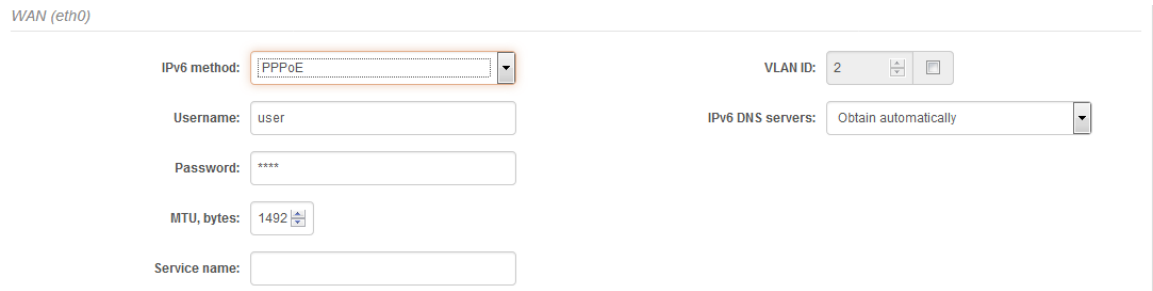


Figure 24 – IPv6 Router WAN Settings: PPPoE

Username – enter the login information for PPPoE.

Password – enter the password for PPPoE.

MTU – specify the MTU (Maximum Transmission Unit) in bytes.

IPv6 DNS servers – choose the DNS servers for IPv6 connection:

- **Obtain automatically** – if selected, the DNS servers will be used automatically.
- **Use following** – specify IPv6 DNS servers manually.

LAN (wireless) settings

LAN configuration includes settings related to the LAN interface.

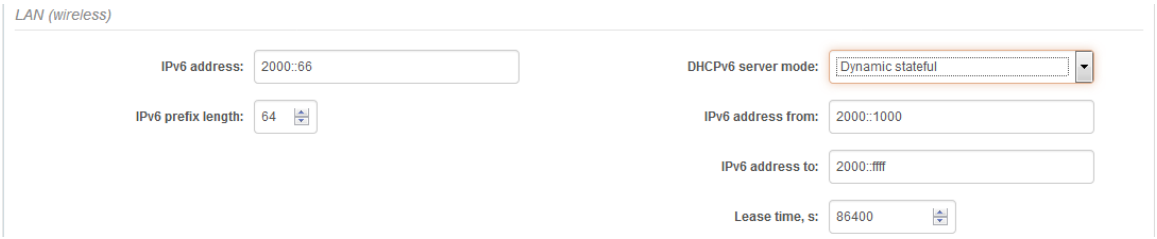


Figure 25 – IPv6 Router LAN Settings

IPv6 address – enter the IPv6 LAN address.

IPv6 prefix length – specify the IPv6 prefix length, or keep the default prefix length (64).

DHCPv6 server mode – select from the drop-down required DHCPv6 mode:

- **Disabled** – select to disable DHCPv6 server. No IPv6 addresses will be assigned for clients.
- **Dynamic stateless IP** – select for automatic IPv6 address configuration.
- **Dynamic stateful IP** – select to configure stateful DHCPv6 server for the LAN by specifying local DHCP IPv6 address pools so the DHCPv6 server can control the allocation of IPv6 addresses in the LAN:
  - **IPv6 address from** - enter the start IP address. This address specifies the first of the contiguous addresses in the IP address pool.
  - **IPv6 address to** – enter the end IP address. This address specifies the last of the contiguous addresses in the IP address pool.
  - **Lease time** – specify the expiration time in seconds for the IP address assigned by the DHCPv6 server.

Wireless

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 device can operate in four wireless modes: Access Point (autoWDS), Access Point (TDMA 2), Access Point (TDMA 3), Station (WDS/TDMA 2/TDMA 3) and Station (ARPNAT).

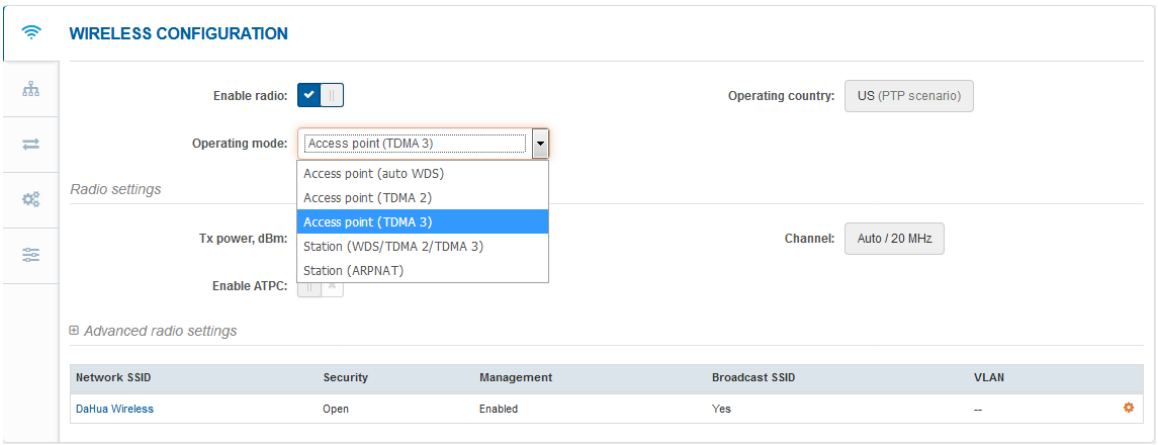


Figure 26 – Device Wireless Operating Mode

If device is dual-band, then Wireless Configuration page will be divided into two tabs (for 2.4GHz and 5GHz radio), each containing appropriate wireless settings.

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

Operating mode – select wireless operation mode:

- **Access Point (auto WDS)** – enables the 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 (TDMA 2)** – enables the radio function as access point for point-to-multipoint solution. The Access Point communicates with Station in TDMA 2 protocol, other clients requests will be not accepted.
- **Access Point (TDMA 3)** – enables the radio function as access point for point-to-multipoint solution. The Access Point communicates with Station in TDMA 3 protocol, other clients requests will be not accepted.
- **Station (WDS/TDMA 2/TDMA 3)** – with this wireless mode the device will act as Station and will automatically turn on TDMA 2 or TDMA 3 mode if detects that selected AP is operating in TDMA 2 or TDMA 3 protocol accordingly.
- **Station (ARPNAT)** – with this wireless mode the device is configured act as client and to connect to other radio functioning as an access point. Station (ARPNAT) is available only if device is operating in Bridge network mode.

Operating modes differs according product:

802.11n:

Access Point (autoWDS),
Access Point (TDMA 2)
Access Point (TDMA 3)
Station (WDS/TDMA 2/TDMA 3)
Station (ARPNAT)

802.11ac:

Access Point (autoWDS)
Access Point (TDMA3)
Station (WDS/TDMA 3)
Station (ARPNAT)

Wireless mode: Access Point (auto WDS)

The Access Point and Stations must operate on the same frequency channel, use the same channel width and the same security settings.

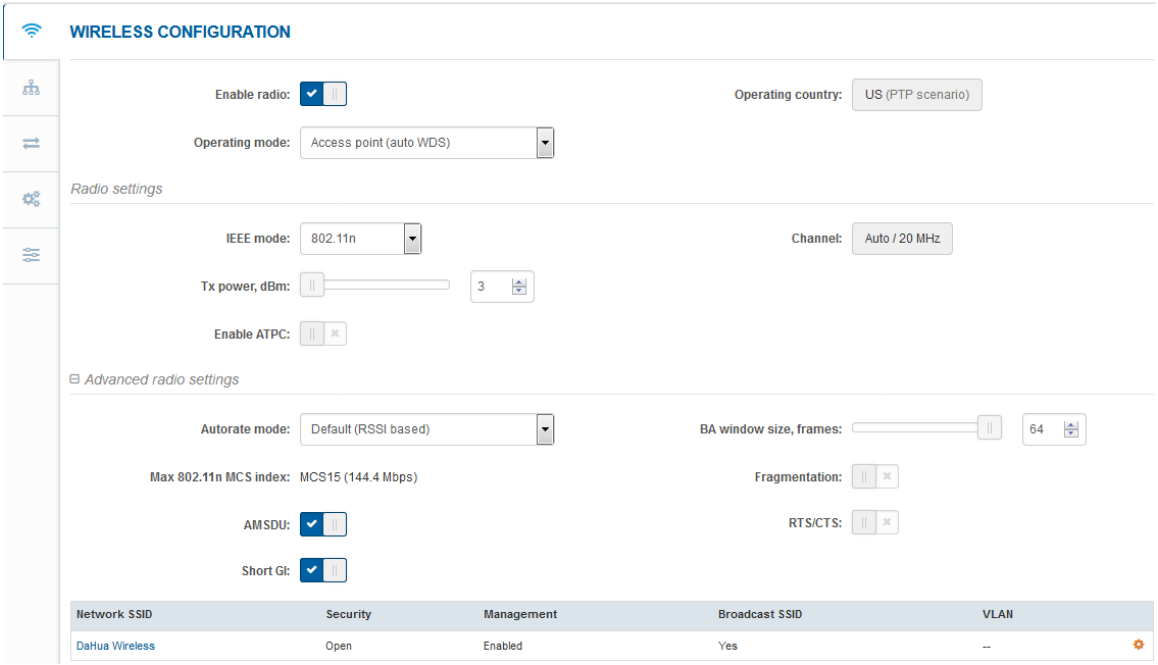


Figure 27 – Access Point Wireless Settings

Enable radio – use slide to enable or disable radio.

Operating country – displays 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 unit's installation, though can be updated if required.

IEEE mode – specify the wireless network mode [802.11a, 802.11n, 802.11a/n]. There is no option IEEE mode on 802.11ac products.

Tx power (dBm) – 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.

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

Channel – displays the channel at which the AP is operating, or indicates that autochannel function is used. Click the button and the channel selection window will be displayed:

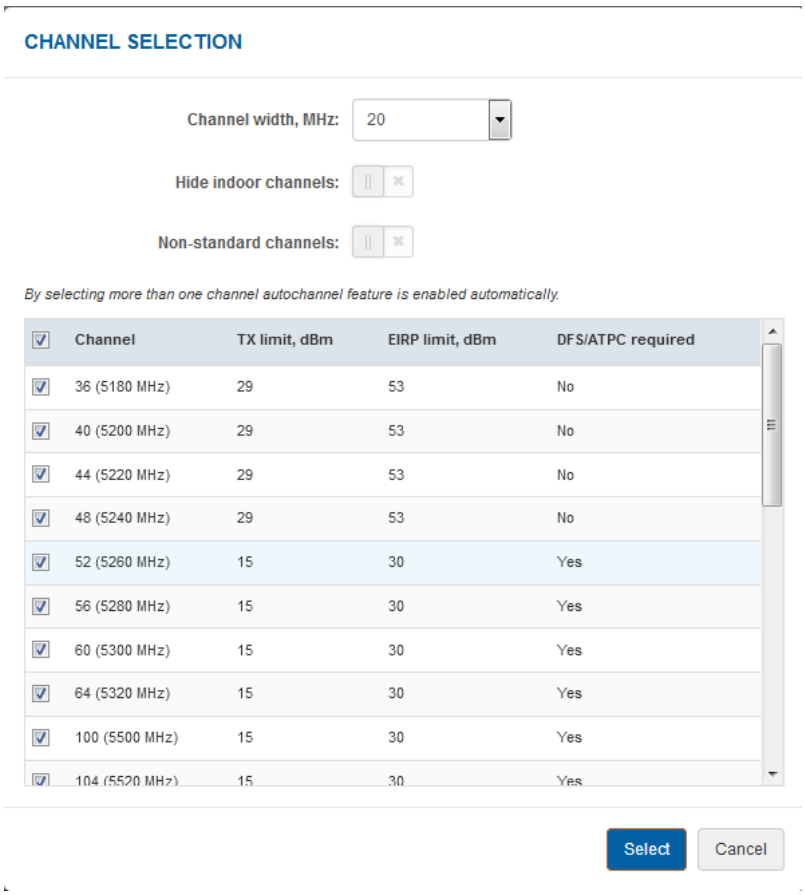


Figure 28 – Channel List Table

Channel width – select the width of the operating radio channel. We supports 5, 10, 20 and 40MHz channel widths.

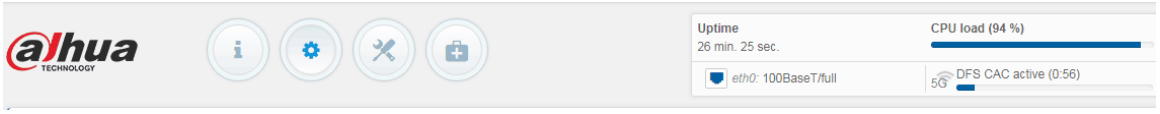
Hide indoor channels – use slide to display only outdoor channels.

Non-standard channels – select to enable non standard channels. Non-standard channels have 5MHz channel step, therefore some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all a/n standard clients or Access Points.

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

Channel table – select the channel(s) at which the Access Point 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: TX limit, EIRP limit and DFS or ATPC.

The DFS CAC (Channel Availability Check) indicator will be visible on the web management page header, in case device is operating on CAC waiting period:



Advanced Radio Settings

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

Radio mode – this option is only on 802.11ac products. Choose the device 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 2x2** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission. Available only on 802.11n or 802.11a/n IEEE modes.

Max legacy data rate – choose the maximum data rate in Mbps at which AP should transmit packets. The AP will attempt to transmit data at the highest data rate set. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission. Available only on 802.11a or 802.11a/n IEEE modes.

Max data rate, Mbps – displays automatically calculated maximum data rate. Available on 802.11ac products.

WMM – enable to support quality of service for traffic prioritizing. Available on 802.11ac products.

AMSDU – enable the AMSDU packet aggregation. If enabled, the maximum size of the 802.11 MAC frames will be increased. Available only on 802.11n or 802.11a/n IEEE modes and on Dahua 802.11ac products.

Short GI – enable short guard interval. If selected, then 400ns value will be used, else 800ns. Available only on 802.11n or 802.11a/n IEEE modes and on Dahua 802.11ac products.

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/CTS – 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.

Basic AP Wireless Settings

Figure 29 - Wireless Settings

The wireless table allows configure main AP parameters, such as SSID, Security, WACL, etc.

Click on the icon for editing basic AP wireless settings:

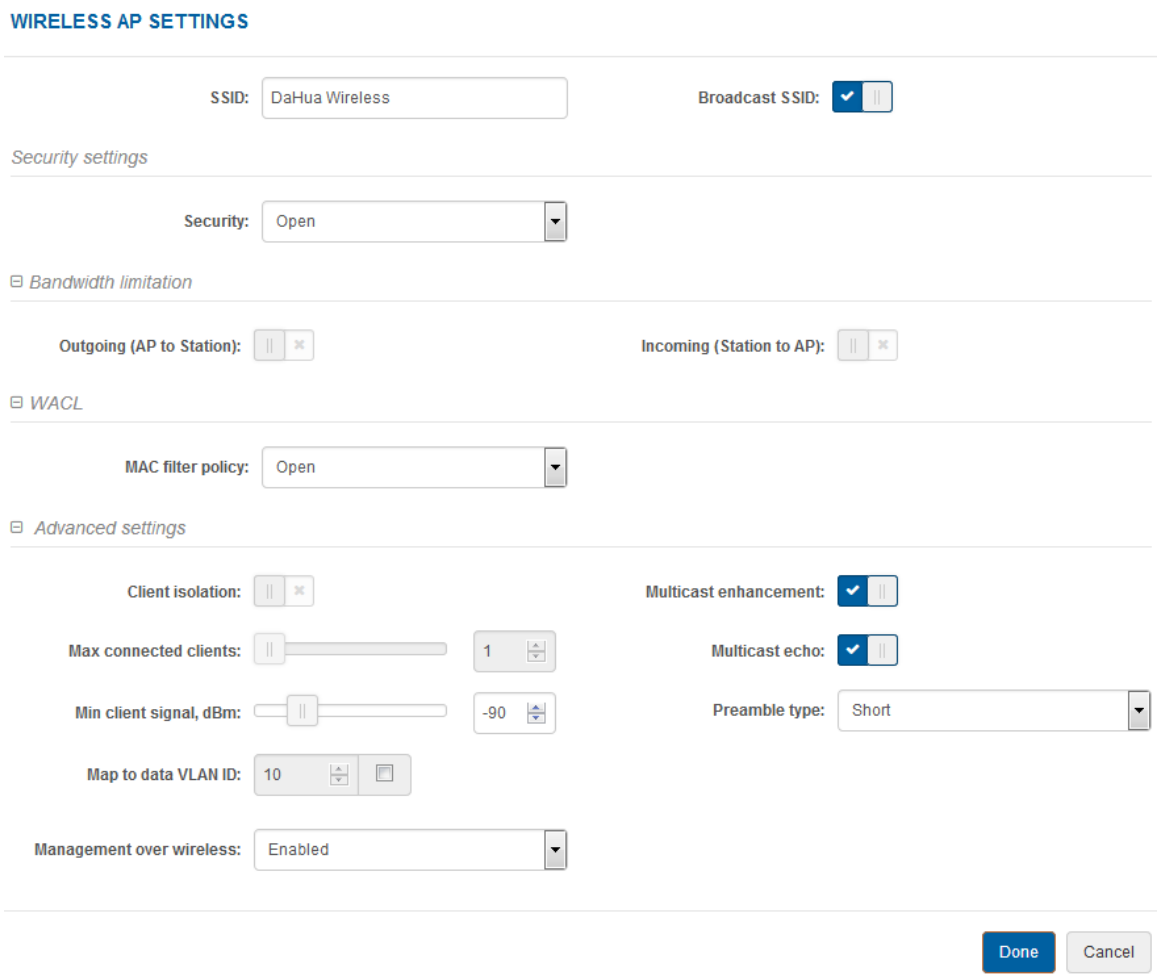


Figure 30 – Wireless AP/Virtual AP Settings

SSID – specify the unique name of the wireless network device. The device will broadcast messages to all stations within range, advertising this SSID.

Broadcast SSID – if this option disabled, the device will not broadcast it's SSID to station devices.

For detailed information about **Security settings** and **WACL** refer at the respective sections *Wireless security* and *Wireless ACL*.

.

Bandwidth limitation:

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

Advanced settings:

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other.

Map to data VLAN ID – specify the VLAN ID for traffic tagging on particular VAP interface. The devices that associate using the particular SSID will be grouped into this VLAN. Map to data VLAN ID is not available if device is operating in Router network mode.

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

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

Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to device. Management over wireless is not available if device is operating in Router network mode.

Multicast enhancement – If clients do not send IGMP (Internet Group Management Protocol) messages, then they are not registered as receivers of your multicast traffic. Using IGMP snooping, the Multicast Enhancement option isolates multicast traffic from unregistered clients and allows the device to send multicast traffic to registered clients using higher data rates. This lessens the risk of traffic overload on PtMP links and increases the reliability of multicast traffic since packets are transmitted again if the first transmission fails. If clients do not send IGMP messages but should receive multicast traffic, then you may need to disable the Multicast Enhancement option. By default this option is enabled.

Wireless mode: Access Point (TDMA 2)

The TDMA 2 wireless mode is designed for point to multipoint wireless solutions. The TDMA 2 Access Point establishes a connection only with TDMA 2 Stations thus creating a reliable network.

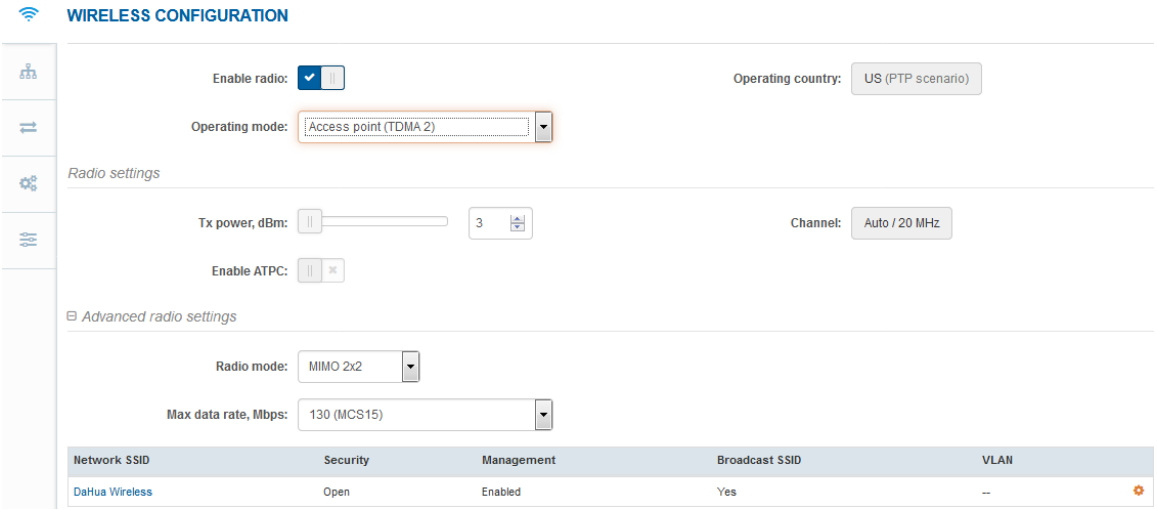


Figure 31 – TDMA Access Point's Wireless Settings

Enable radio – use slide to enable or disable radio.

Operating country - displays device 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 unit's installation, though can be updated if required.

Tx power (dBm) – 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.

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

Channel – displays the channel at which the AP is operating, or indicates that autochannel function is used. Click the button and the channel selection window will be displayed:

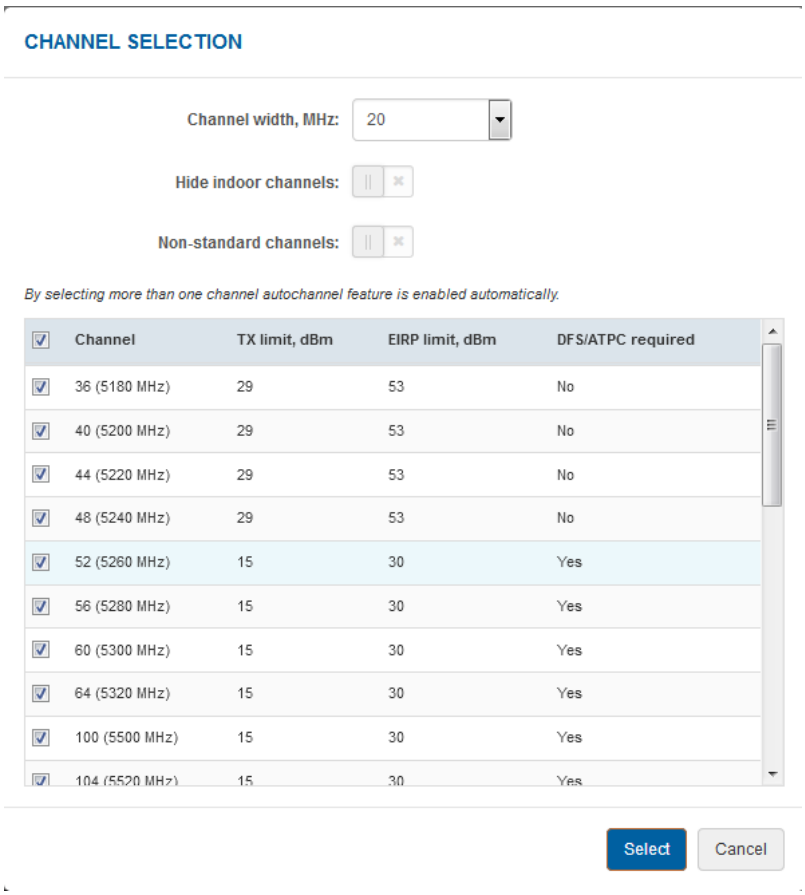


Figure 32 – Channel List Table

Channel width – select the width of the operating radio channel. We supports 5, 10, 20 and 40MHz channel widths.

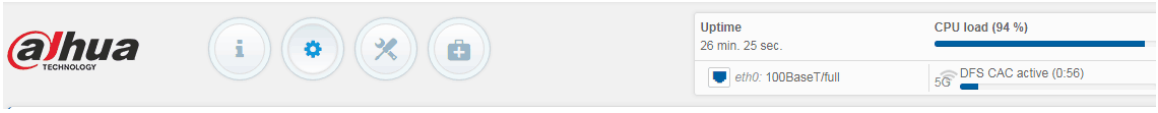
Hide indoor channels – use slide to display only outdoor channels.

Non-standard channels – select to enable non standard channels. Non-standard channels have 5MHz channel step, therefore some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all a/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.

Channel table – select the channel(s) at which the Access Point TDMA 2 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: TX limit, EIRP limit and DFS or ATPC.

The DFS CAC (Channel Availability Check) indicator will be visible on the web management page header, in case the unit is operating on CAC waiting period:



Advanced Radio Settings

Max data rate (Mbps) – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

Basic Wireless Settings (AP)

The wireless AP table allows configure main AP TDMA2 parameters, such as SSID, Security, WACL, advanced settings.

Figure 33 - Wireless Settings

Click on the edit icon and the wireless settings window will be displayed:

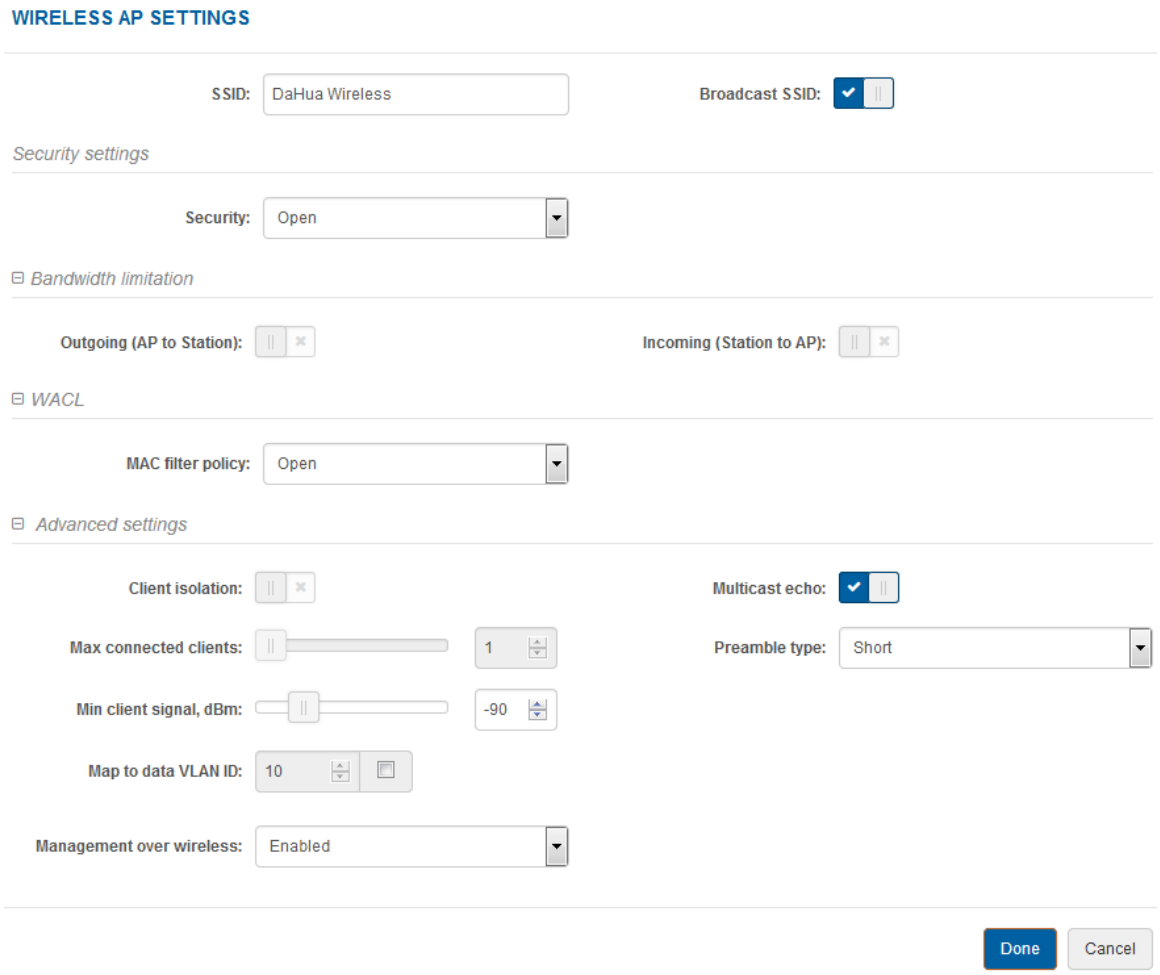


Figure 34 – Wireless AP Settings

SSID – specify the unique name of the wireless network. The device will broadcast messages to all stations within range, advertising this SSID.

Broadcast SSID – if this option disabled, the Dahua device will not broadcast its SSID to station devices.

For detailed information about **Security settings** and **WACL** refer at the respective sections *Wireless security* and *Wireless ACL*.

Bandwidth limitation:

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

Advanced settings:

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other.

Map to data VLAN ID – specify the VLAN ID for traffic tagging on particular VAP interface. The devices that associate using the particular SSID will be grouped into this VLAN. Map to data VLAN ID is not available if device is operating in Router network mode.

Max connected clients - specify the maximum number of associated wireless clients on the Dahua AP radio.

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

Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to device. Management over wireless is not available if device is operating in Router network mode.

Multicast enhancement – If clients do not send IGMP (Internet Group Management Protocol) messages, then they are not registered as receivers of your multicast traffic. Using IGMP snooping, the Multicast Enhancement option isolates multicast traffic from unregistered clients and allows the device to send multicast traffic to registered clients using higher data rates. This lessens the risk of traffic overload on PtMP links and increases the reliability of multicast traffic since packets are transmitted again if the first transmission fails. If clients do not send IGMP messages but should receive multicast traffic, then you may need to disable the Multicast Enhancement option. By default this option is enabled.

Wireless mode: Access Point (TDMA 3)

The TDMA 3 wireless mode is designed for point to multipoint wireless solutions and it is a newer improved version of TDMA2 protocol. The TDMA 3 Access Point establishes a connection only with TDMA 3 Stations thus creating a reliable network.

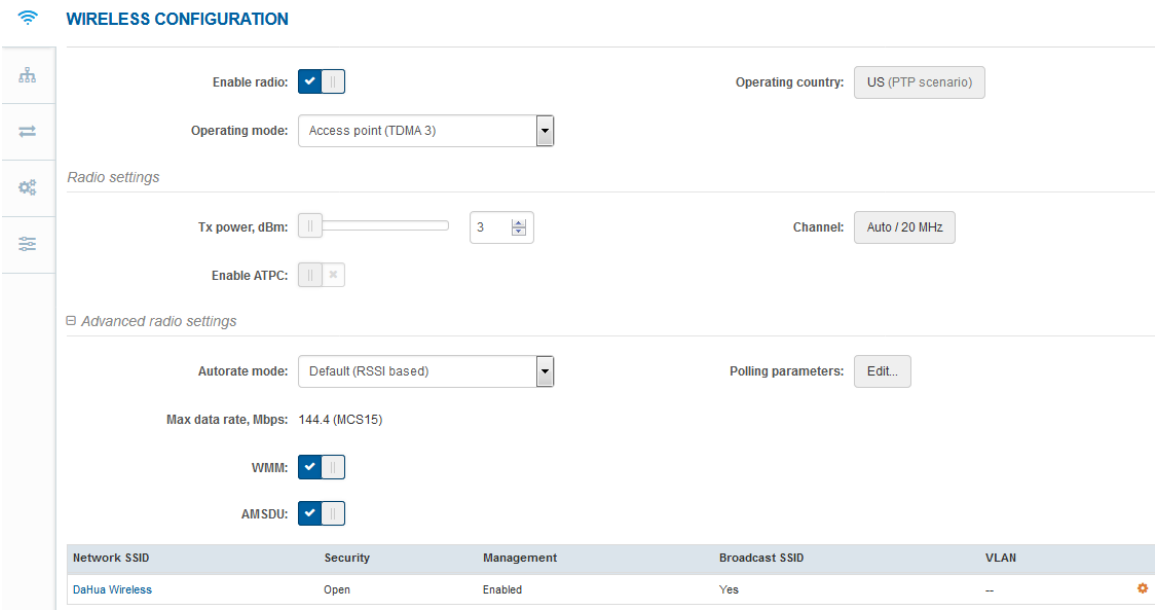


Figure 35 – TDMA 3 Access Point's Wireless Settings

Enable radio – use slide to enable or disable Dahua radio.

Operating country - displays the 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 Dahua unit's installation, though can be updated if required.

Tx power (dBm) – 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.

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

Channel – displays the channel at which the AP is operating, or indicates that autochannel function is used. Click the button and the channel selection window will be displayed:

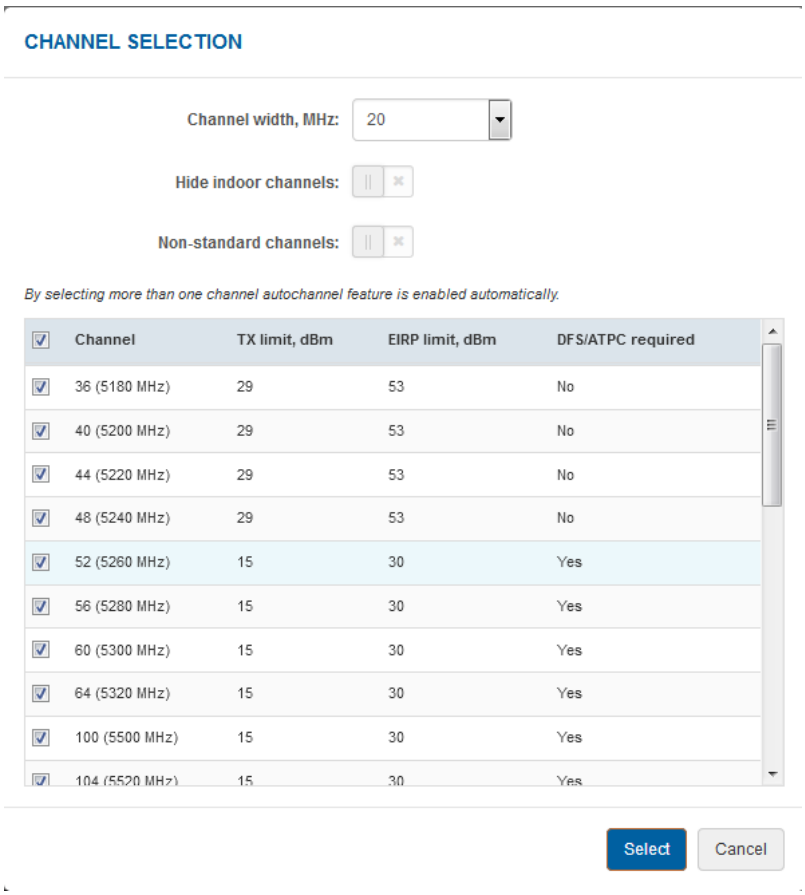


Figure 36 – Channel List Table

Channel width – select the width of the operating radio channel. Dahua supports 5, 10, 20 and 40MHz channel widths.

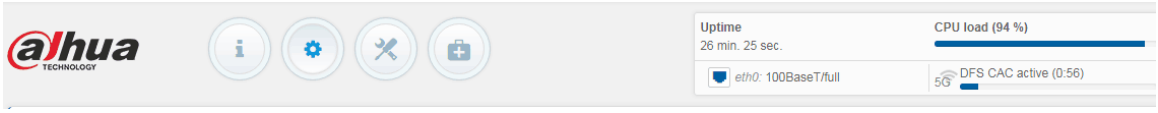
Hide indoor channels – use slide to display only outdoor channels.

Non-standard channels – select to enable nonstandard channels. Non-standard channels have 5MHz channel step, therefore some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all a/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.

Channel table – select the channel(s) at which the Access Point TDMA 2 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: TX limit, EIRP limit and DFS or ATPC.

The DFS CAC (Channel Availability Check) indicator will be visible on the web management page header, in case the unit is operating on CAC waiting period:



Advanced Radio Settings

Advanced parameters allow configuring the device to get the best performance/capacity of the TDMA 3 link.

Radio mode – this option is only on Dahua 802.11ac products. Choose the device 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 2x2** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

Max data rate, Mbps – displays automatically calculated maximum data rate. Available on Dahua 802.11ac products.

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/CTS – 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.

Basic Wireless Settings (AP)

The wireless AP table allows configure main AP TDMA 3 parameters, such as SSID, Security, WACL, advanced settings.

Figure 37 - Wireless Settings

Click on the edit icon and the wireless settings window will be displayed:

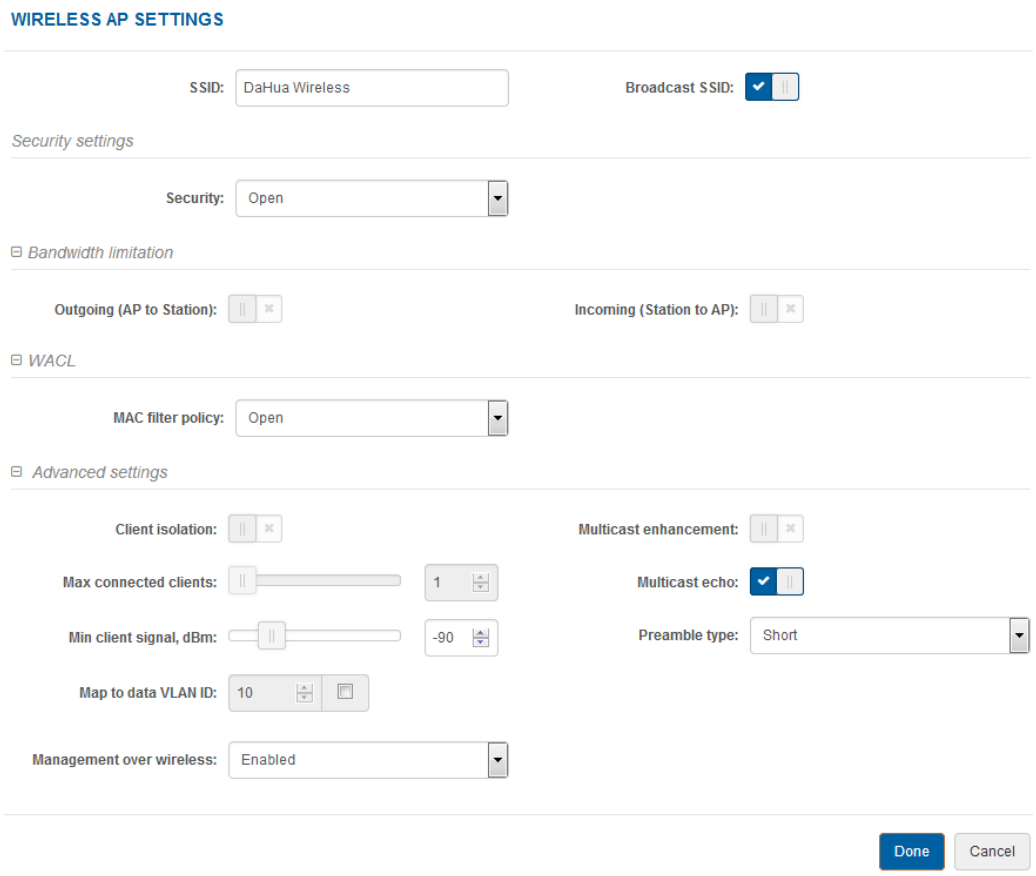


Figure 38 – Wireless AP Settings

SSID – specify the unique name of the wireless network. The device will broadcast messages to all stations within range, advertising this SSID.

Broadcast SSID – if this option disabled, the Dahua device will not broadcast its SSID to station devices.

For detailed information about **Security settings** and **WACL** refer at the respective sections *Wireless security* and *Wireless ACL*.

Bandwidth limitation:

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

Advanced settings:

Client isolation – select to enable the layer 2 isolation that blocks clients from communicating with each other.

Map to data VLAN ID – specify the VLAN ID for traffic tagging on particular VAP interface. The devices that associate using the particular SSID will be grouped into this VLAN. Map to data VLAN ID is not available if device is operating in Router network mode.

Max connected clients - specify the maximum number of associated wireless clients on the Dahua AP radio.

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

Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to device. Management over wireless is not available if device is operating in Router network mode.

Multicast enhancement – If clients do not send IGMP (Internet Group Management Protocol) messages, then they are not registered as receivers of your multicast traffic. Using IGMP snooping, the Multicast Enhancement option isolates multicast traffic from unregistered clients and allows the device to send multicast traffic to registered clients using higher data rates. This lessens the risk of traffic overload on PtMP links and increases the reliability of multicast traffic since packets are transmitted again if the first transmission fails. If clients do not send IGMP messages but should receive multicast traffic, then you may need to disable the Multicast Enhancement option. By default this option is enabled.

Wireless mode: Station (WDS/TDMA 2/TDMA 3)

With this wireless mode, the device will operate as wireless Station, though it automatically switches on the TDMA 2 or TDMA 3 mode if the specified access point will be detected as an AP TDMA 2 or AP TDMA 3 accordingly. In case the Station finds two networks with the same SSID, where one is TDMA 3, another 11n, the connection priority will be TDMA 3.

Use Wireless Configuration to setup radio interface of the device.

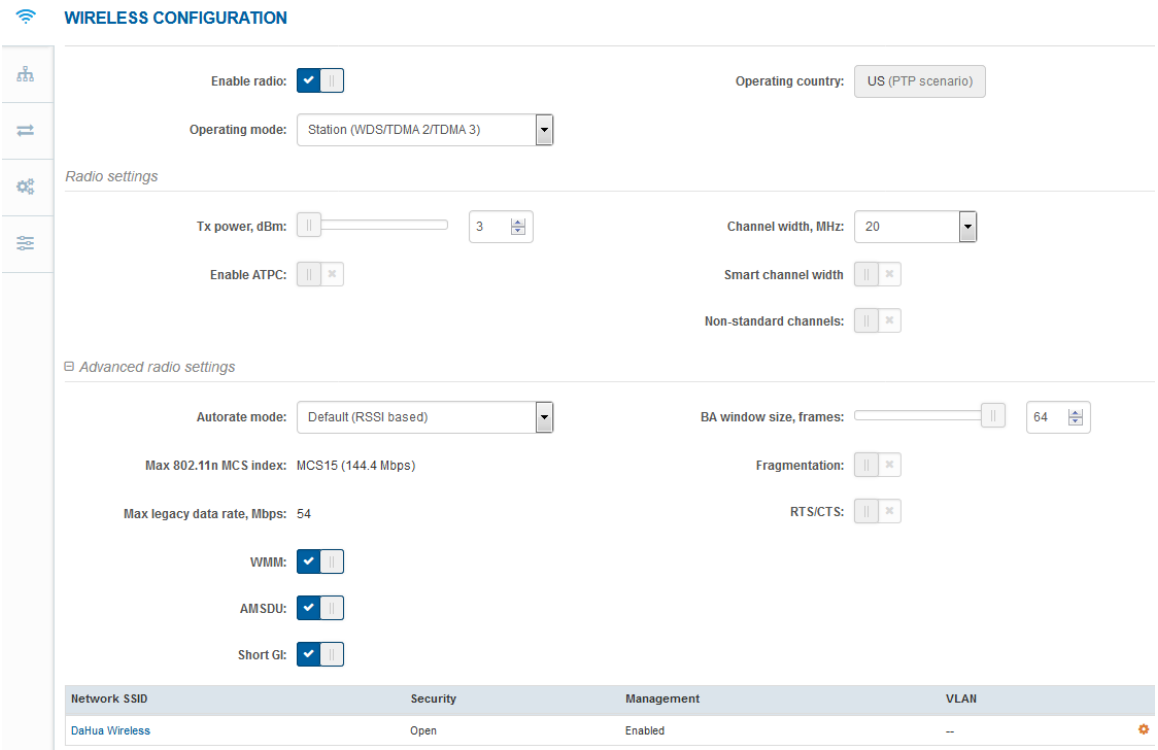


Figure 39 – Station Wireless Settings

Enable radio – use slide to enable or disable Dahua radio.

Operating country - displays the 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 Dahua unit's installation, though can be updated if required.

Tx power (dBm) – 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.

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

Channel width - select the width of the operating radio channel. Dahua device supports 5, 10, 20 and 20/40MHz channel widths.

Non-standard channels – select to enable non standard channels. Non-standard channels have 5MHz channel step, therefore some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all a/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.

Smart channel width – select to enable smart channel width on station. This option enabled allows Dahua station to change the channel width automatically in case of unsuccessful connection to AP as long as the connection to AP is established.

Advanced Radio Settings

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

Radio mode – this option is only on Dahua 802.11ac products. Choose the device 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 2x2** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

Max data rate, Mbps – displays automatically calculated maximum data rate. Available on Dahua 802.11ac products.

WMM – enable to support quality of service for traffic prioritizing. Available on Dahua 802.11ac products.

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

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

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/CTS – 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.

Basic SSID Settings

The wireless table allows configure main station parameters, such as SSID settings, Security and advanced settings.

Network SSID	Security	Management	VLAN	
DaHua Wireless	Open	Enabled	--	

Figure 40 - Wireless Settings

Click on the edit icon and the wireless settings window will be displayed:

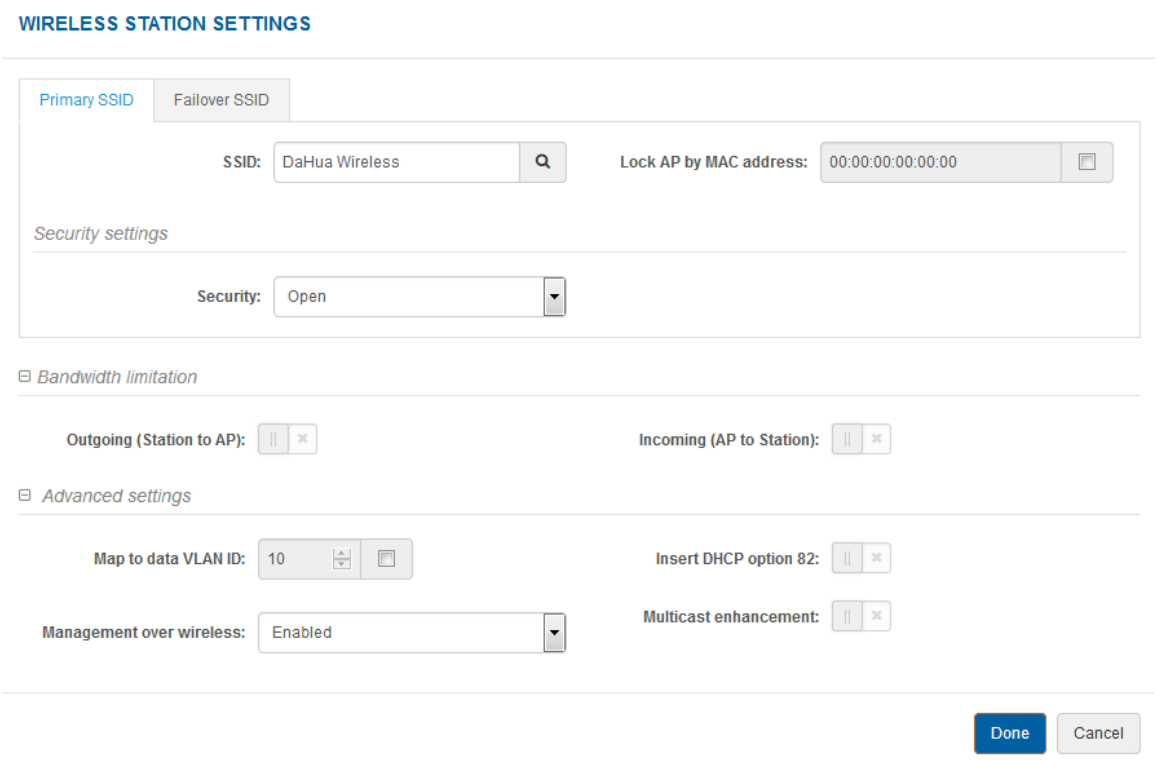
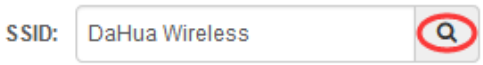


Figure 41 – Station SSID Settings

Primary SSID – specify the SSID of the wireless network device manually, or scan for Access Points automatically:



If auto scan for SSID is used, the results will be displayed in the Search SSID table, thus simply click on the required AP and SSID will be selected:

Lock AP by MAC address – select the check-box and specify the MAC address of the required access point, thus preventing the roaming between access points with the same SSID.

For detailed information about **Security settings** refer at the respective sections *Wireless security*.

Bandwidth Limitation

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

Advanced SSID Settings

If device is operating in Router network mode, this section will be hidden, as VLAN and Management over wireless are not available on Router.

Wireless VLAN ID – specify the VLAN ID for traffic tagging on particular radio interface. The Station devices that associate using the particular SSID will be grouped into this VLAN.

Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to device.

Failover SSID

Dahua units have possibility to connect to preconfigured failover SSID, in case the connection to the primary SSID is lost.

In case the Station is operating on failover SSID and then loses this connection, the Station will try to connect to primary SSID first, and only then will try to attempt to connect to the failover SSID. Reboot will result in the same sequence.

Use the **Failover SSID** tab to enable SSID failover function:

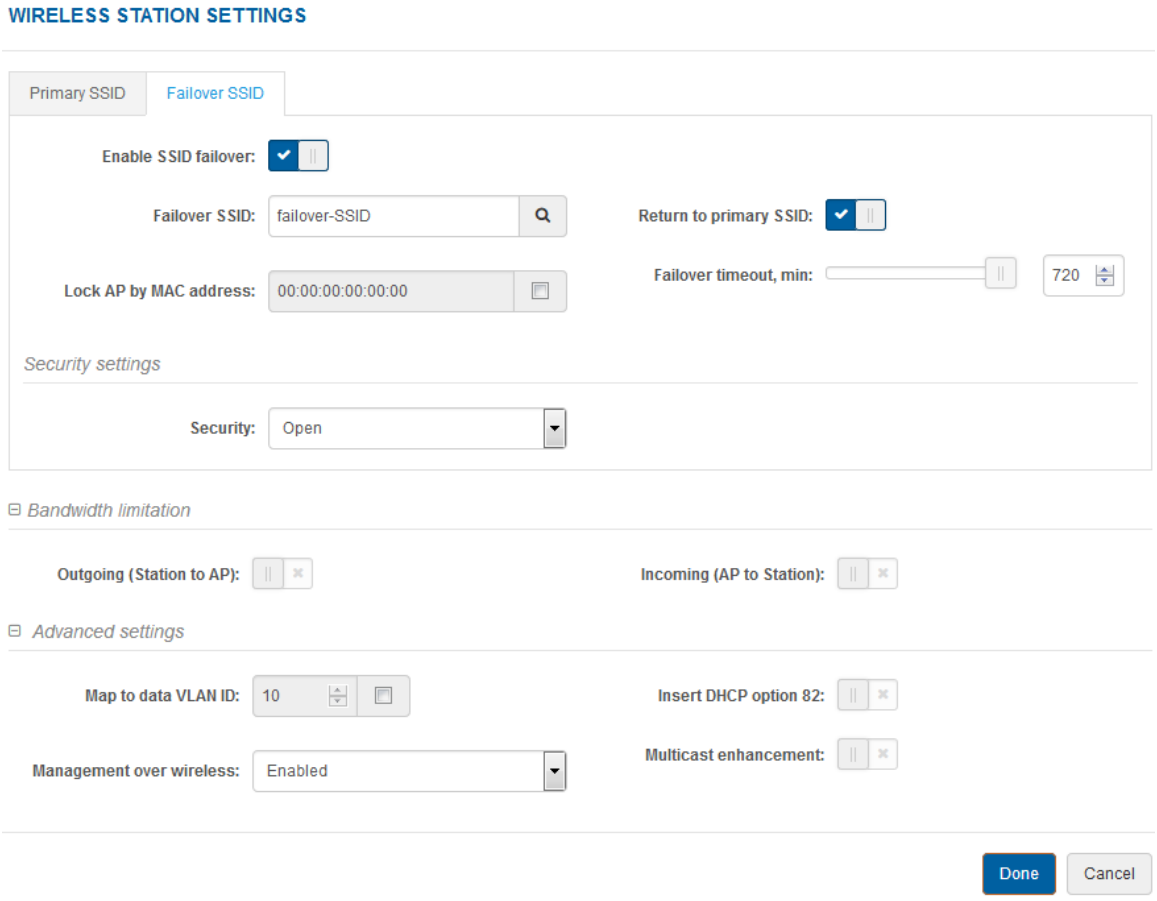


Figure 42 - SSID Failover Configuration

Failover SSID – specify the secondary SSID where the Dahua Station will try to connect.

Return to primary SSID – when enabled the Dahua unit tries to connect continuously to the primary SSID in the intervals preset.

Failover timeout – specify the amount of time in minutes, the station will attempt to connect to primary SSID.

Bandwidth limitation:

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

For detailed information about **Security** and **Advanced** settings refer at the respective sections *Wireless security* and *Bandwidth Limitation.*

Wireless mode: Station (ARPNAT)

The wireless mode Station (ARPNAT) is available only if the Dahua device is operating in *Bridge* network mode.

With this wireless mode, the device will operate as wireless Station with ARPNAT. Use Wireless Configuration to setup radio interface:

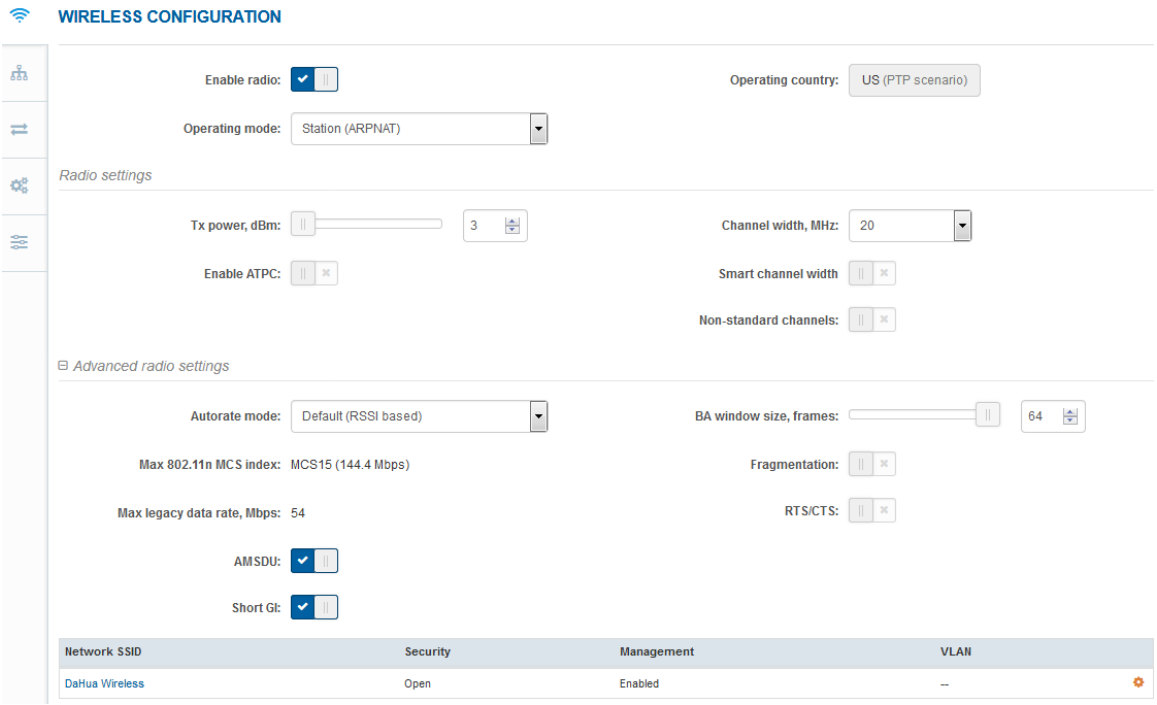


Figure 43 – Station Wireless Settings

Enable radio – use slide to enable or disable Dahua radio.

Operating country - displays Dahua 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 unit's installation, though can be updated if required.

Tx power (dBm) – 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.

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

Channel width - select the width of the operating radio channel. Dahua supports 5, 10, 20 and 40MHz channel widths.

Non-standard channels – select to enable non standard channels. Non-standard channels have 5MHz channel step, therefore some center frequencies will not be valid with 802.11 specification. This feature may interfere with other networks and may not support all a/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.

Smart channel width – select to enable smart channel width on station. This option enabled allows Dahua station to change the channel width automatically in case of unsuccessful connection to AP as long as the connection to AP is established.

Advanced Radio Settings

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

Radio mode – this option is only on Dahua 802.11ac products. Choose the device 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 2x2** – multiple input multiple output. The device will use two antennas for data transfer (two simultaneous streams).

Max 802.11n MCS index – choose the maximum rates to specify the modulation and coding scheme (MCS) rates at which data can be transmitted between the access point and the client. If there will be an interference encountered, the device will step down to the highest rate that allows data transmission.

Max data rate, Mbps – displays automatically calculated maximum data rate. Available on Dahua 802.11ac products.

WMM – enable to support quality of service for traffic prioritizing. Available on Dahua 802.11ac products.

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

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

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/CTS – 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.

SSID Settings

The wireless table allows configure main station parameters, such as SSID of the AP unit, Security, advanced settings.

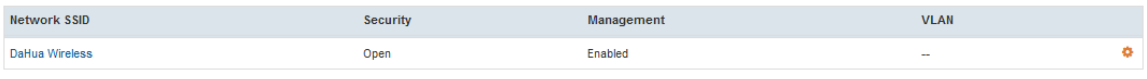


Figure 44 - Wireless Settings

Click on the edit icon and the wireless settings window will be displayed:

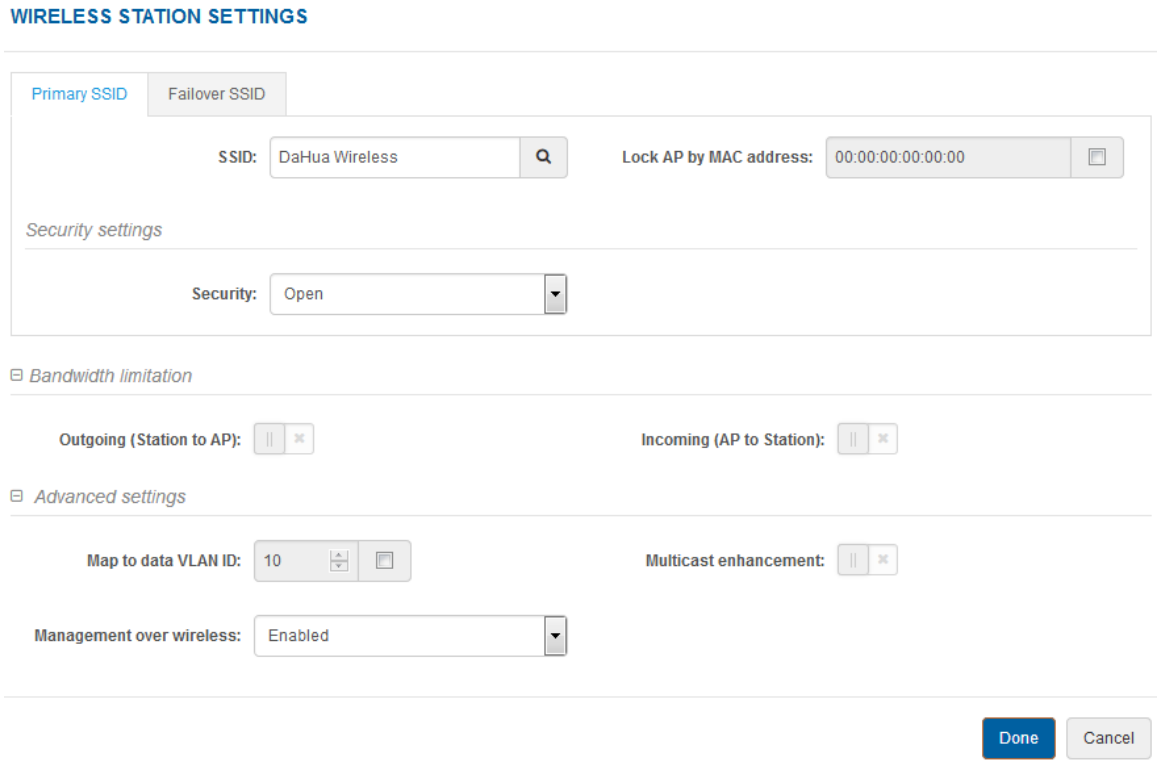
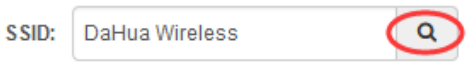


Figure 45 – Wireless AP Settings

Primary SSID – specify the SSID of the required wireless network device manually, or scan for Access Points automatically:



If auto scan for SSID is used, the results will be displayed in the Search SSID table, thus simply click on the required AP and SSID will be selected:

Lock AP by MAC address – select the check-box and specify the MAC address of the particular access point, thus preventing the roaming between access points with the same SSID.

For detailed information about **Security settings** refer at the respective sections *Wireless security*.

Bandwidth Limitation

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

Advanced SSID Settings

If device is operating in Router network mode, this section will be hidden, as VLAN and Management over wireless are not available on Router.

Wireless VLAN ID – specify the VLAN ID for traffic tagging on particular radio interface. The Station devices that associate using the particular SSID will be grouped into this VLAN.

Management over wireless – controls the wireless administrative access. For security reasons, it is recommended disable wireless access and instead requires a physical network connection using an Ethernet cable for administrative access to device.

Failover SSID

Dahua units have possibility to connect to preconfigured failover SSID, in case the connection to the primary SSID is lost.

In case the Station is operating on failover SSID and then loses this connection, the Station will try to connect to primary SSID first, and only then will try to attempt to connect to the failover SSID. Reboot will result in the same sequence.

Use the **Failover SSID** tab to enable SSID failover function:

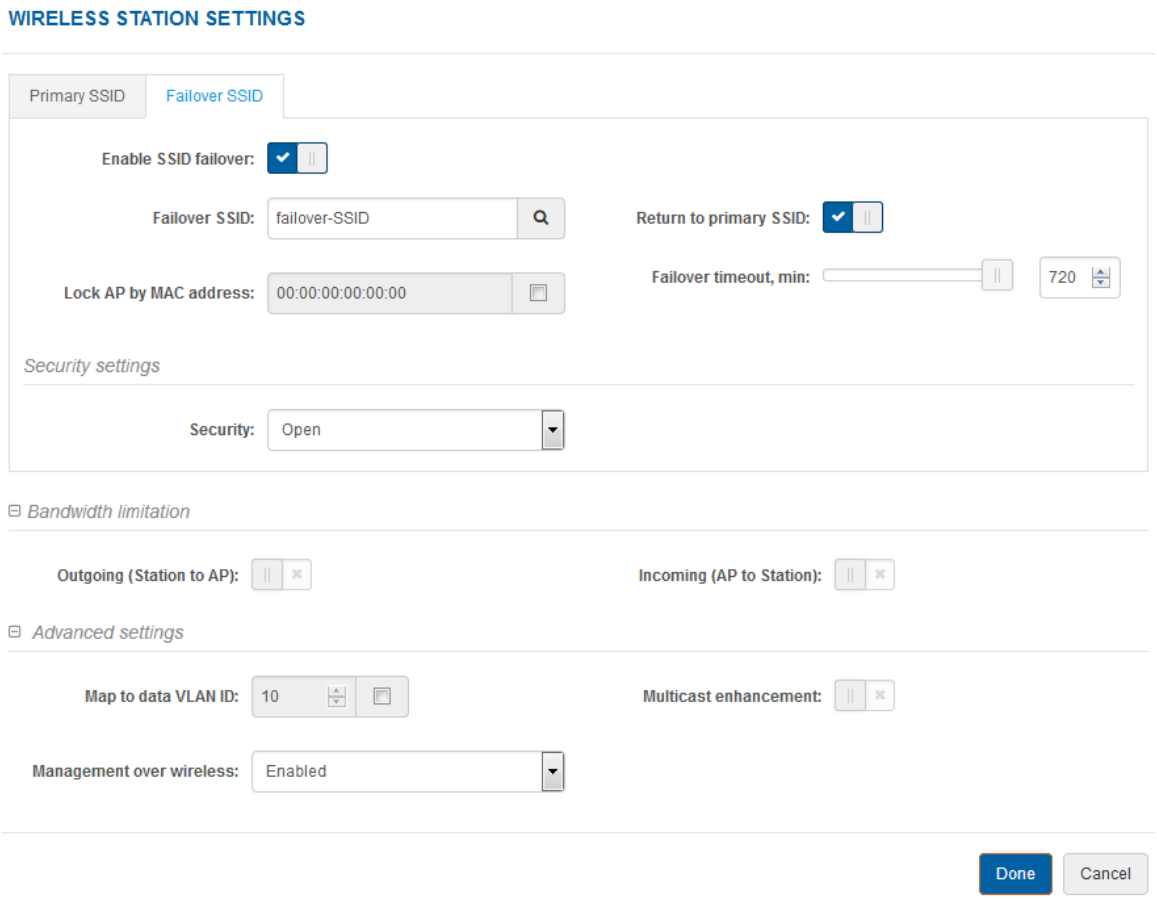


Figure 46 - SSID Failover Configuration

Failover SSID – specify the secondary SSID where the Dahua Station will try to connect.

Return to primary SSID – when enabled the Dahua unit tries to connect continuously to the primary SSID in the intervals preset.

Failover timeout – specify the amount of time in minutes, the station will attempt to connect to primary SSID.

Bandwidth limitation:

Outgoing (AP to Station) – specify the maximum speed in Mbps of the outgoing traffic.

Incoming (Station to AP) – specify the maximum speed in Mbps of the incoming traffic.

For detailed information about **Security** and **Advanced** settings refer at the respective sections *Wireless security* and *Bandwidth Limitation*.

Wireless security

The configuration of wireless security is made on Settings | Wireless Configuration page:

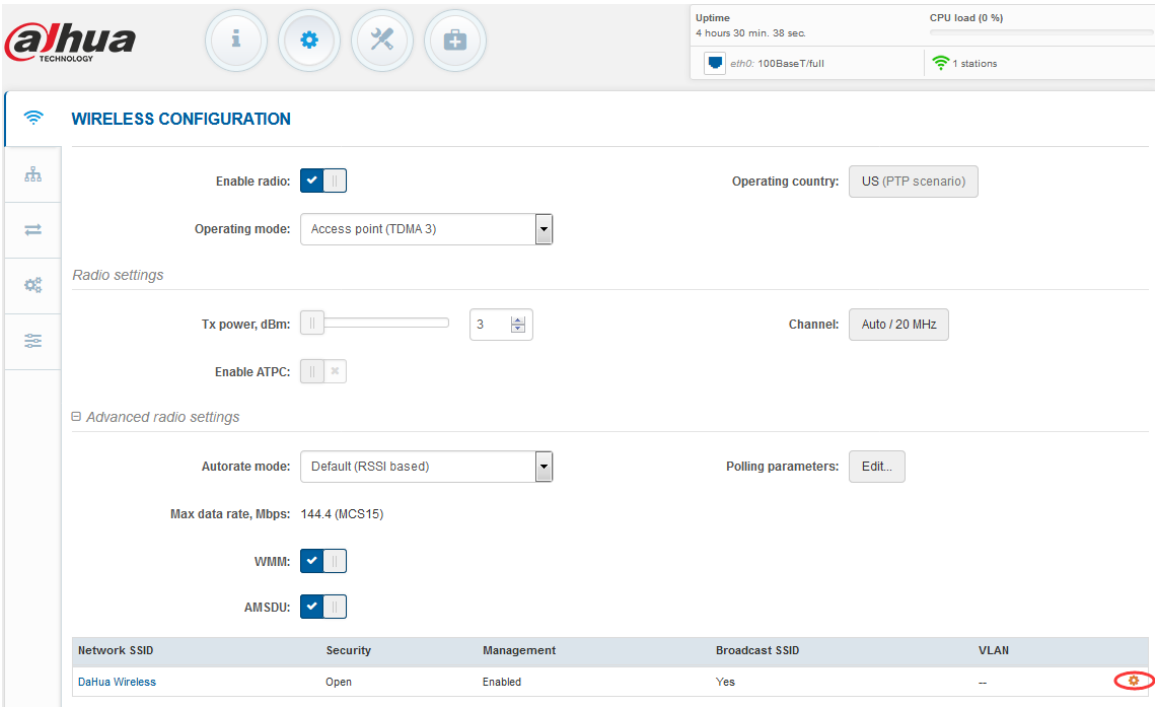


Figure 47 - Wireless Security Navigation

If device acts as an Access Point (auto WDS), Access Point (TDMA 2) or Access Point (TDMA 3) 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.

Dahua devices supports various authentication/encryption methods and they are different for Stations and Access Points.

Access Point security methods:

- **Open** – no encryption.
- **WPA/WPA2 Personal** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals using mixed WPA and WPA2 securing methods.
- **WPA2 Personal** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals using WPA2 securing method.
- **WPA/WPA2 Enterprise**– RADIUS server based authentication (requires configured RADIUS server) using mixed WPA and WPA2 securing methods.
- **WPA2 Enterprise**– RADIUS server based authentication (requires configured RADIUS server) using WPA2 securing method.

Station security methods:

- **Open** – no encryption.
- **WEP 64bit** – WEP encryption with 64bit key algorithm.
- **WEP 128bit** – WEP encryption with 128bit key algorithm.
- **WPA/WPA2 Personal** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals using mixed WPA and WPA2 securing methods.
- **WPA/WPA2 Enterprise**– RADIUS server based authentication (requires configured RADIUS server) using mixed WPA and WPA2 securing methods.

Open

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

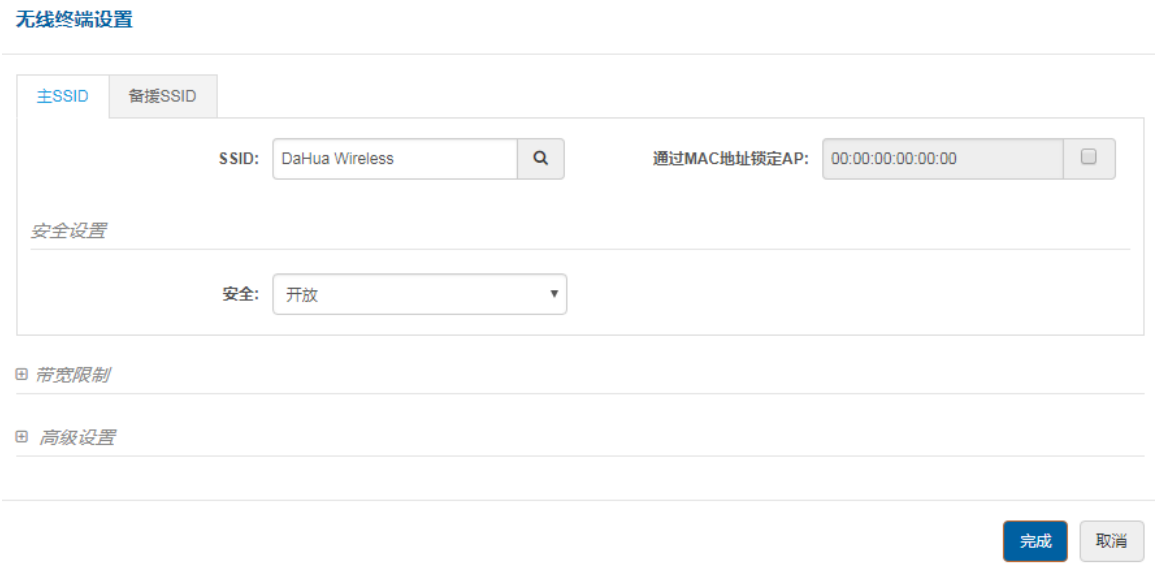


Figure 48 – Wireless Security: Open

WPA/WPA2 Personal

Use the same sequence for the **WPA2 Personal** security configuration.

To setup WPA/WPA2 Personal encryption, need to select appropriate security type and specify the passphrase:

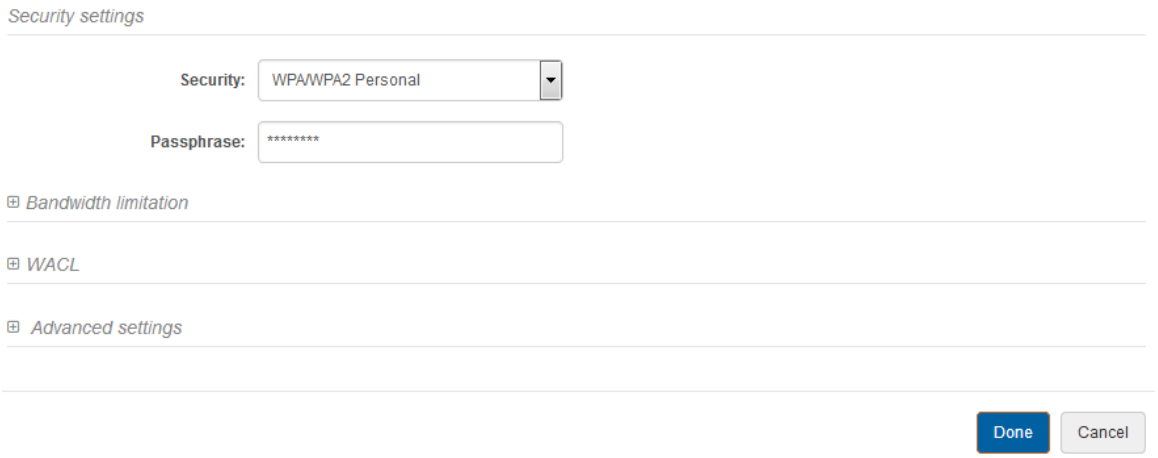


Figure 49 –Wireless Security: Personal WPA/WPA2 Security

Passphrase – specify WPA or WPA2 passphrase [8-63 characters].

WPA/WPA2 Enterprise for Access Points

Use the same sequence for the **WPA2 Enterprise** security configuration

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

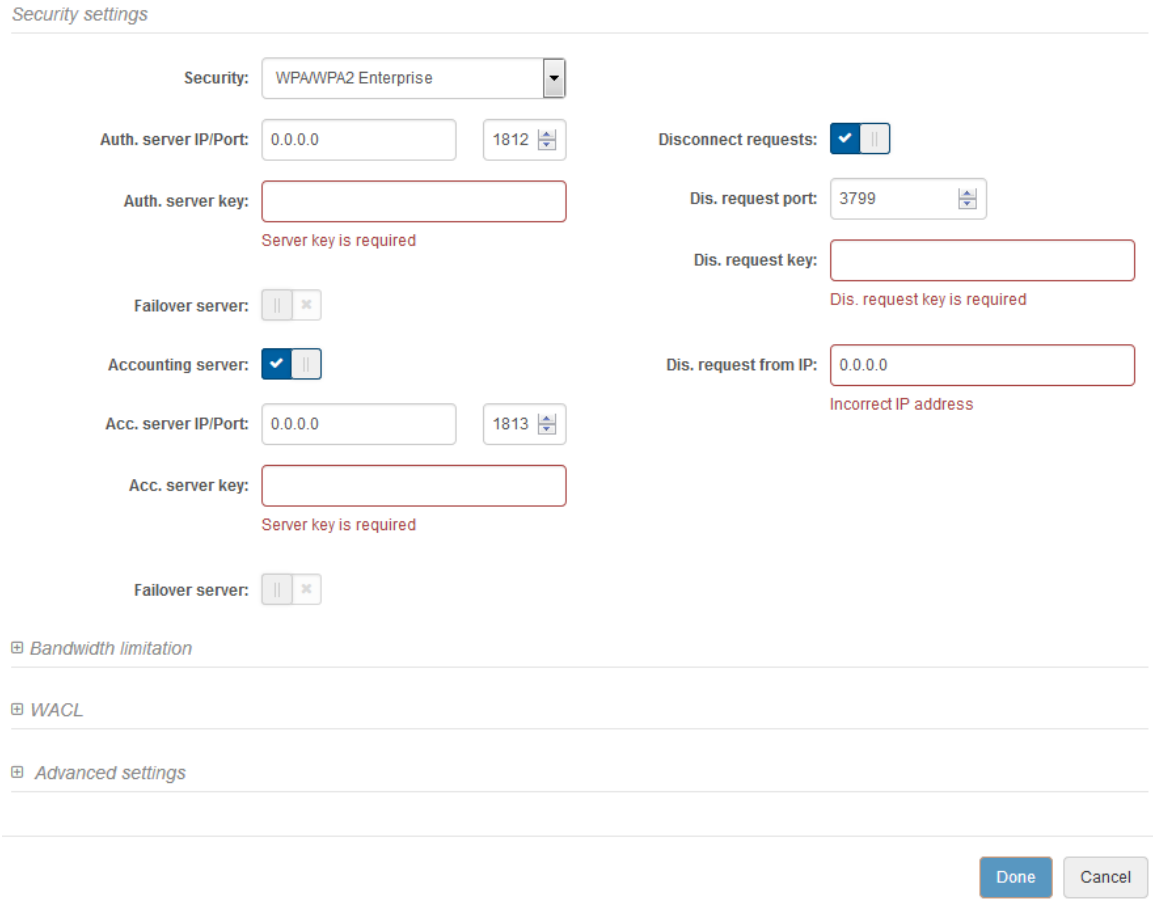


Figure 50 –Wireless Security: Enterprise WPA/WPA2 Security for AP

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

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

Auth. server key – enter the key for the authentication on specified RADIUS server.

Accounting server – use slide to enable accounting RADIUS server, if required.

- **Accounting server IP/Port** – specify the IP address and the port of the accounting RADIUS server where the accounting stats will be send to.
- **Accounting server key** – enter the key for the authentication on specified accounting RADIUS server.

Disconnect requests – select to enable the Disconnect Request message that is sent to a NAS (Network Access Server) in order to terminate a user session and discard all associated session context.

- **Disconnect request Port** – specify the NAS port number where the disconnect request packets

will be sent to (default: 3799).

- **Disconnect request key** – specify the key in text string that is shared between the network access server and the device.
- **Disconnect request from IP** – specify the requestors IP address.

WPA/WPA2 Enterprise for Stations

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

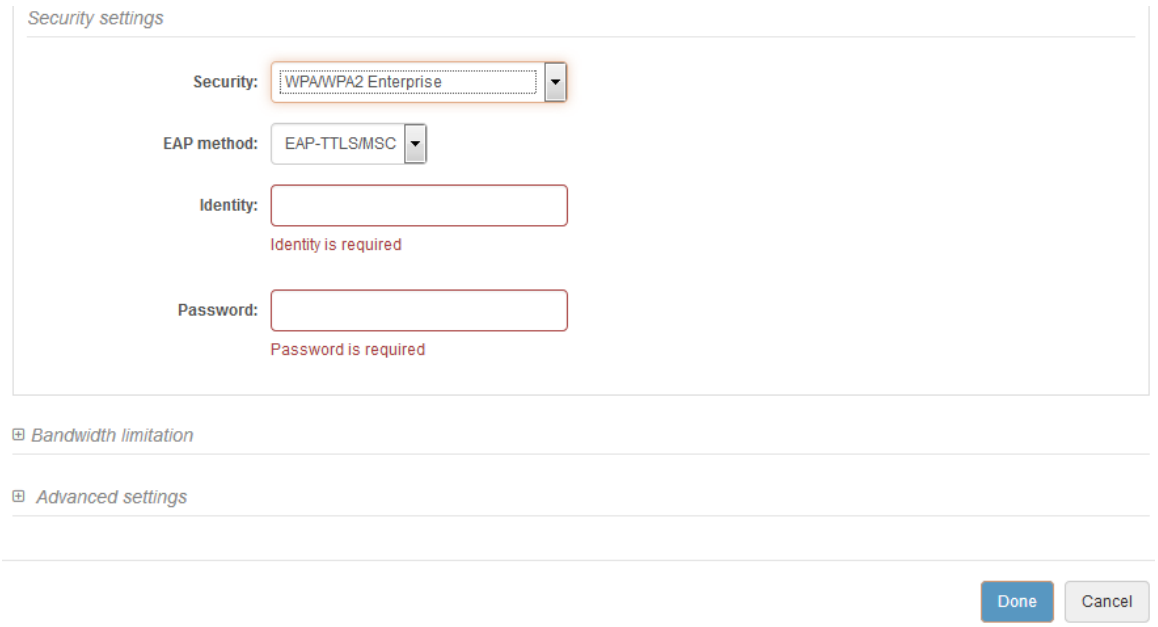


Figure 51 –Wireless Security: Enterprise WPA/WPA2 Security for Stations

EAP method – choose EAP method:

- EAP-TTLS
- PEAP

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 Station must match the identity and password running on the RADIUS server's user list.

WEP 64bit/128bit encryption

WEP encryption is available only for Station (not recommended for it's security flaws).

To configure the WEP encryption, select the WEP key algorithm (64bit or 128bit) and enter the pre-shared key:

Figure 52 - WEP Encryption Configuration

Key index – select a value between 1 and 4, that refers to the position of the matching key stored on the Access Point.

Key – WEP keys are entered as a series of colon-separated HEX (0-9, A-F, and a-f) pairs:

- 5 pairs for 64-bit (e.g. 00:AC:01:35:FF)
- 13 pairs for 128-bit (e.g. 00:11:22:33:44:55:66:77:88:99:AA:BB:CC)

Wireless ACL

Wireless ACL is active only in **Access Point (auto WDS), Access Point (TDMA 2)** and **Access Point (TDMA 3)** wireless modes.

Wireless 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.

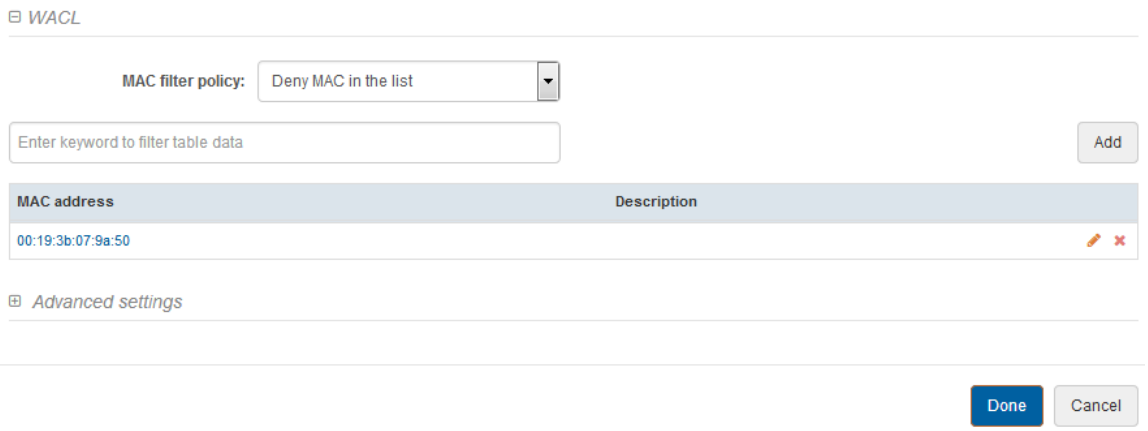


Figure 53 – Wireless ACL Configuration

MAC filter 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, click the **Add** button, specify MAC address and click verification icon ✔.

To remove the rule, click the delete icon ✖ next to required record.

To edit the rule, click the pencil icon next to required record.

Traffic Management

Traffic Management can be performed by configuring Traffic Optimization and/or Traffic Control:

Traffic Optimization – for L2 (802.1p) and L3 (DSCP) data classification in order to prioritize incoming traffic for the best performance.

Traffic Control – for downstream or upstream bandwidth control.

The availability of traffic management methods per Dahua device's operating mode is given in the table below:

Operating mode	Traffic Optimization	Traffic Control
Access point (autoWDS)	–	–
Access point (TDMA 2)	–	×
Access point (TDMA 3)	×	–
Station (WDS/TDMA 2/TDMA 3)	×	×
Station (ARPNAT)	–	×

Traffic Optimization

Traffic optimization is available only on:

- Access Point (TDMA3) and Station (WDS/TDMA 2/TDMA 3) wireless modes on Dahua 802.11n products.
- Access Point (TDMA3) and Station (WDS/TDMA 3) wireless modes on Dahua 802.11ac products.

The incoming traffic has to be marked according to 802.1p or DSCP values to match one of the four queues, before reaching Dahua device.

The QoS on the device automatically detects and classifies incoming traffic according 802.1p or DSCP values to match one of the four queues (Lowest->Highest), as given in the following table:

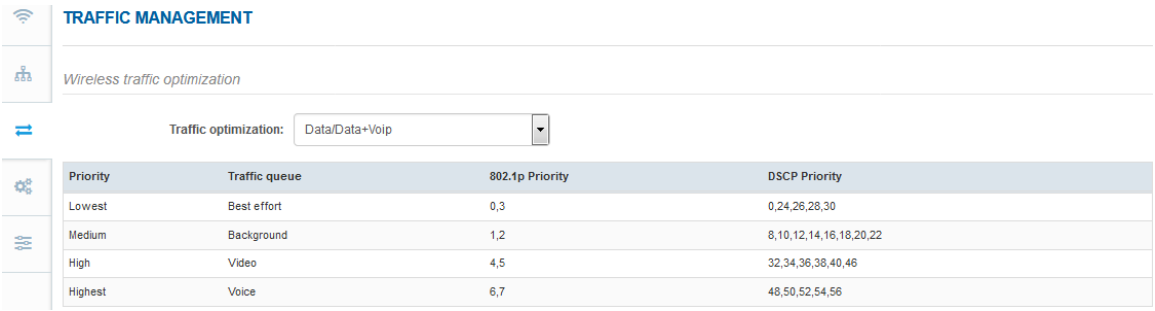


Figure 54 – 801.p and DSCP Traffic Classification on Dahua device

QoS mapping precendence is always 802.1p.

Traffic optimization – select the transmitting traffic type for the best data optimisation and performance:

- **Data/Data+Voip** – for data and data+Voip traffic.
- **Data+Video+Voip** – for data, video and Voip traffic.

Traffic Control: Access Point

Traffic control is available only on Access Point (TDMA2) and both Station (WDS/TDMA 2/TDMA 3) and Station (ARPNAT) wireless modes.

Traffic control is not available on 802.11ac products.

The Traffic Control on Access Point is made by assigning the pre-configured profile for each station. Initially the Default traffic management profile is created on system. All newly connected stations to the Dahua unit will appear under the **Station list** table and then the Default profile will be assigned to them by default automatically.

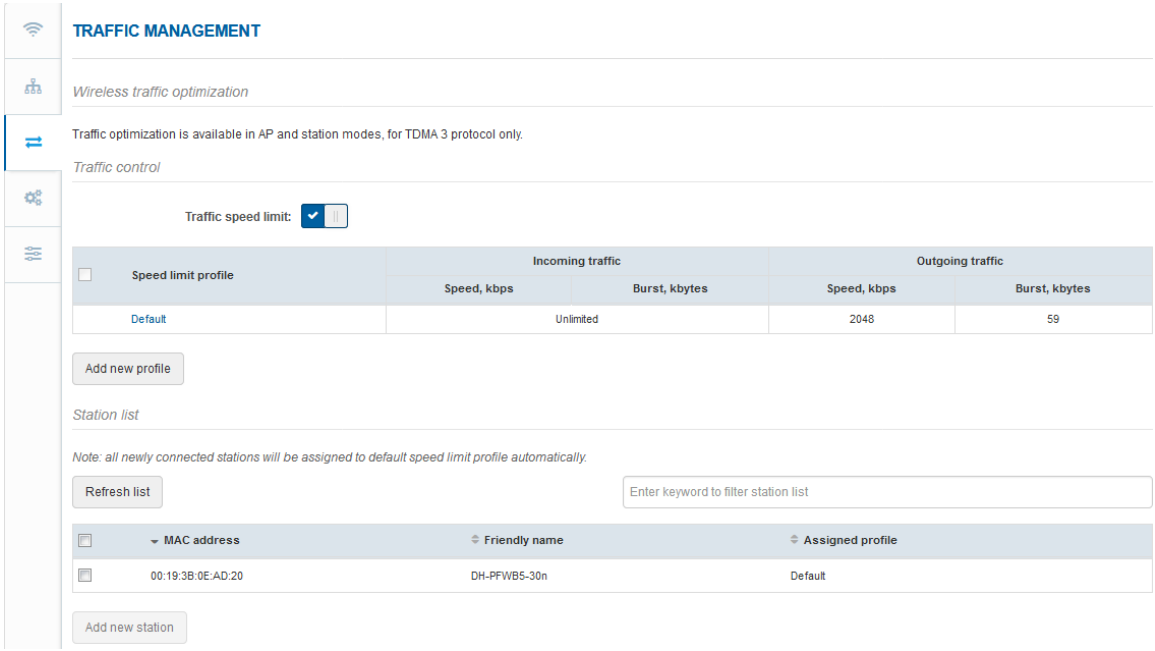


Figure 55 - Traffic Management Page

Up to 32 Speed Limit Profiles can be created on GUI.

Click on the profile name for editing, or click the **Add new profile** button for creating a new profile:

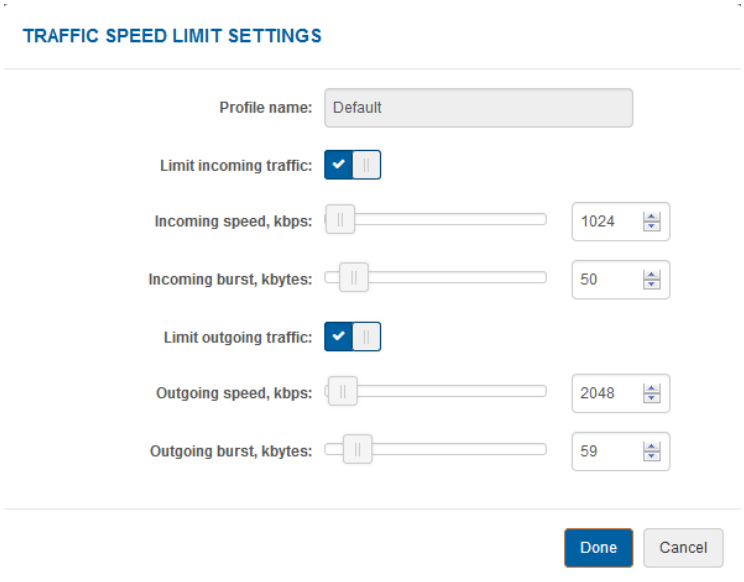


Figure 56 - Traffic Management Profile Configuration

Profile name – assign a name for the particular Speed Limit Profile.

Limit incoming traffic – select to enable limitation of the incoming traffic:

- **Incoming speed, kbps** – specify the maximum incoming bandwidth value for traffic in kbps
- **Incoming burst, kbytes** – specify data volume in kbytes of Incoming traffic, that allows users to exceed their assigned limit in a "burst" for a short period of time.

Limit outgoing traffic – select to enable limitation of the outgoing traffic:

- **Outgoing speed, kbps** – specify the maximum outgoing bandwidth value for traffic in kbps.
- **Outgoing burst, kbytes** – specify data volume in kbytes of Outgoing traffic, that allows users to exceed their assigned limit in a "burst" for a short period of time.

All newly connected stations will be assigned to default Speed Limit Profile automatically.

If custom Speed Limit Profiles are configured, it is available to change profile for the connected station. Select station that requires changes and choose the action that can be performed:

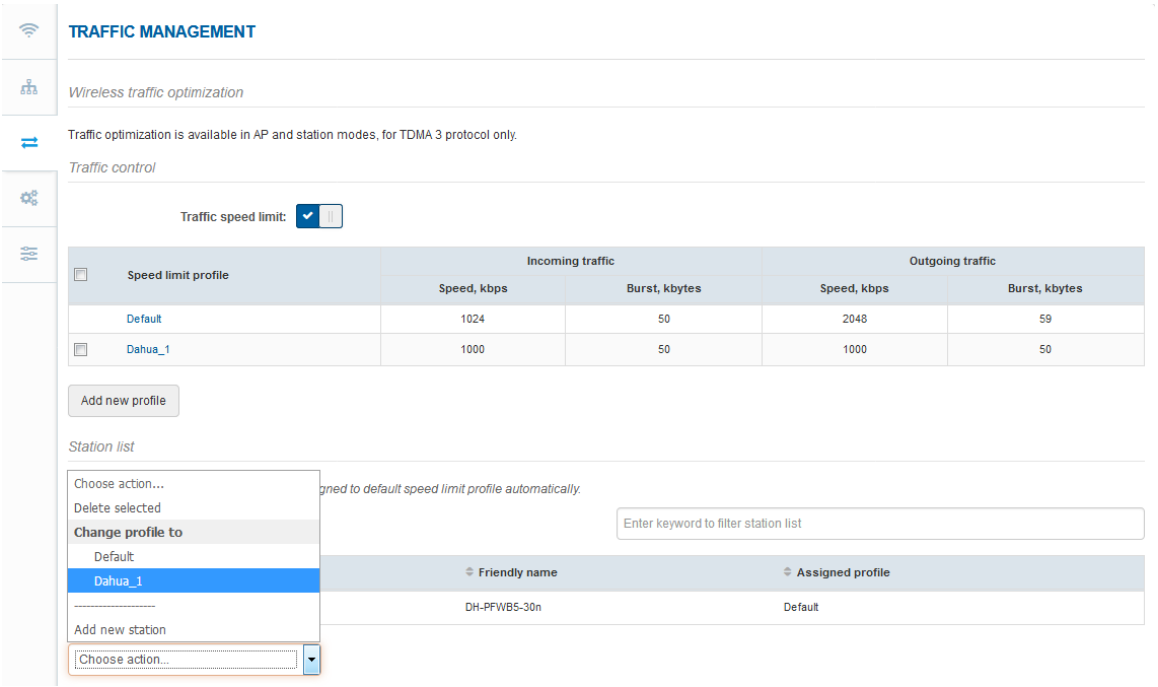


Figure 57 - Traffic Management Stations List

Delete selected – choose to delete particular station. Note that station that will reconnect, will appear under this table with assigned default profile automatically.

Change profile to – select profile that will be assigned to the particular station.

It is possible to assign a custom profile for new, not connected yet station, and then as soon as it connects to the AP, the custom profile (not default) will be assigned for it. Click **Add new station** under the Station list table, specify the station MAC address and the profile that will be assigned:

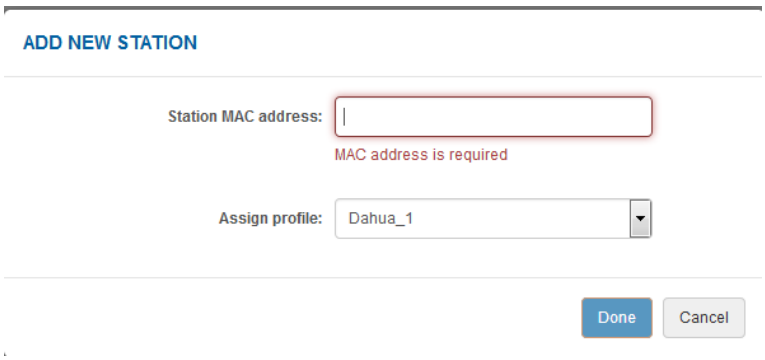


Figure 58 - Assign Profile for the New Station

Traffic Control: Stations

The configuration of the Traffic Control is the same on both Station wireless modes: **Station (WDS/TDMA 2/TDMA 3)** and **Station (ARPNAT)**.

In case the Station is connected to the Access Point and the traffic speed limit is enabled on AP, then traffic speed limit is managed from the AP side, thus all Traffic Control section will be hided on Station.

The Traffic Control on Stations can by performed by limiting incoming and outgoing traffic on the station wireless interface.

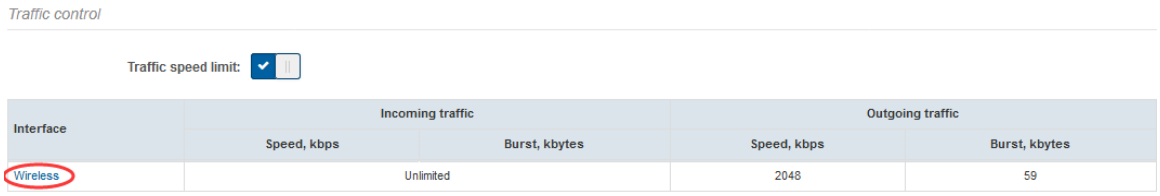


Figure 59 - Traffic Speed Limitation on Station

Click on **Wireless** interface name to edit traffic limitation settings:

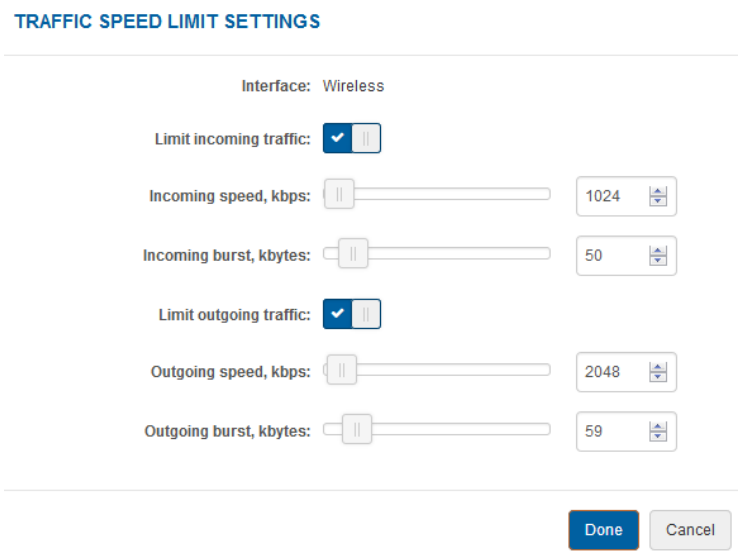


Figure 60 - Traffic Speed Limit Settings

Limit incoming traffic – select to enable limitation of the incoming traffic:

- **Incoming speed, kbps** – specify the maximum incoming bandwidth value for traffic in kbps
- **Incoming burst, kbytes** – specify data volume in kbytes of Incoming traffic, that allows users to

exceed their assigned limit in a "burst" for a short period of time.

Limit outgoing traffic – select to enable limitation of the outgoing traffic:

- **Outgoing speed, kbps** – specify the maximum outgoing bandwidth value for traffic in kbps.
- **Outgoing burst, kbytes** – specify data volume in kbytes of Outgoing traffic that allows users to exceed their assigned limit in a "burst" for a short period of time.

Services configuration

Use **Services** menu is divided into further five sections:

- Date & time
- Remote management
- SNMP
- Ping watchdog
- WNMS

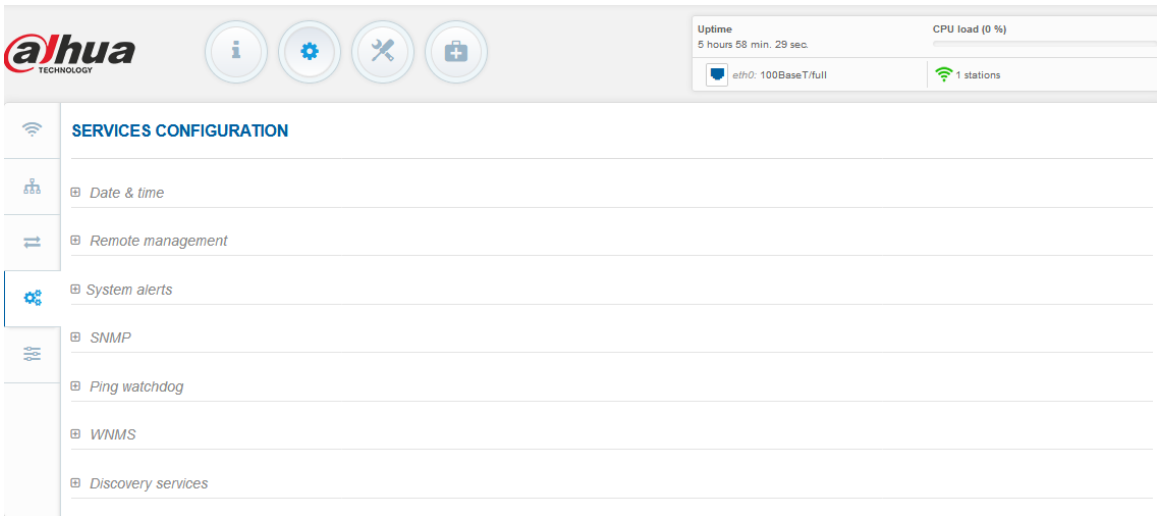


Figure 61 - Services Menu

Date & time

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.

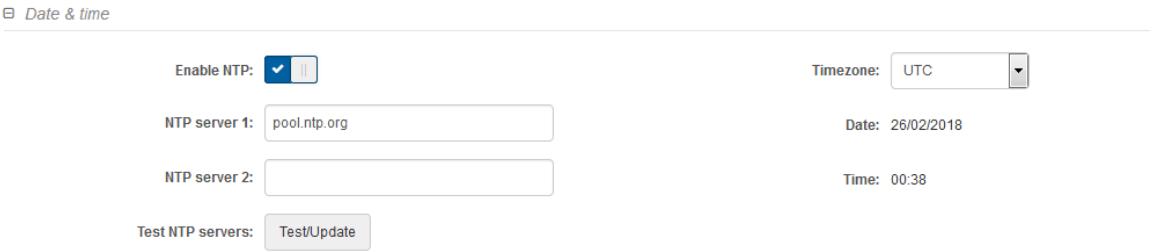


Figure 62 – Date&time: NTP Configuration

Enable NTP – select this option as enabled to configure NTP.

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

NTP server – specify the trusted NTP server IP or hostname for time synchronization.

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

To adjust the clock settings manually, disable NTP option and specify the following settings:

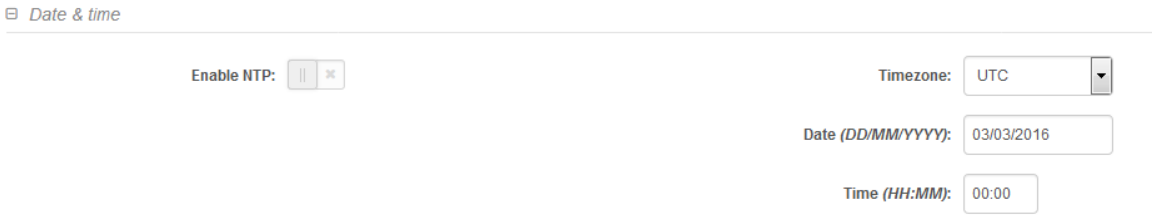


Figure 63 – Date&time: Manual Configuration

Enable NTP – disable this option to set date&time manually.

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

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

Time – specify the time in format HH:MM.

Remote management

Use this menu to manage access to the device via SSH, Telnet and HTTP:

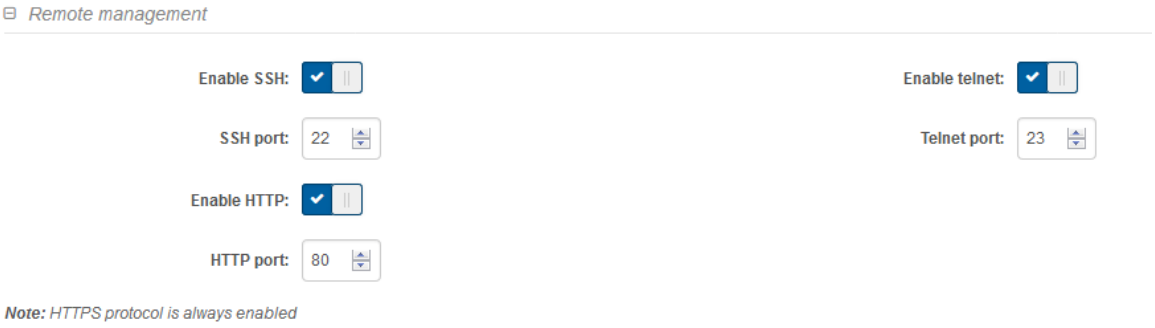


Figure 64 – Remote Management Configuration

Enable SSH – enable or disable SSH access to device.

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

Enable telnet – enable or disable telnet access to device.

Telnet port – specify the telnet port. By default, telnet port is 23.

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

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

HTTPS connection via the standard port 443 is always enabled.

System Alerts

Dahua unit is able to send external alerts via SNMP Traps when there are system errors.

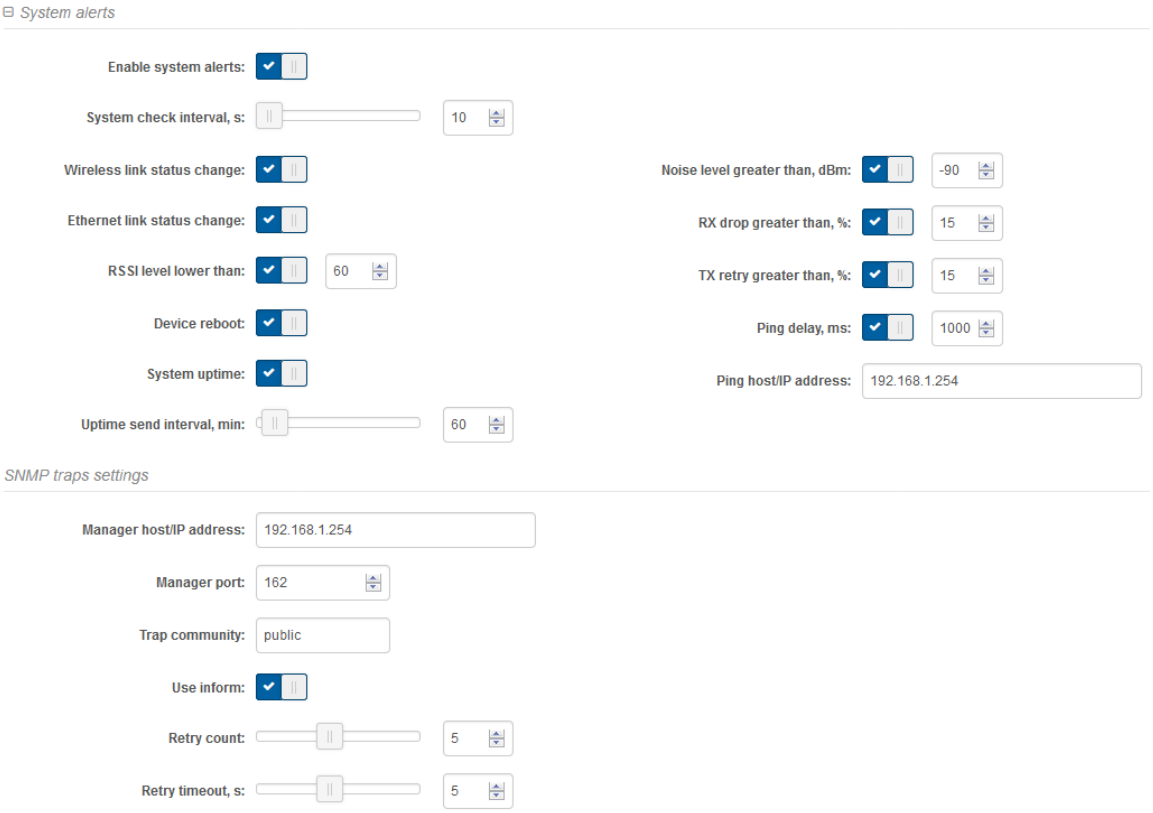


Figure 65 - System Alerts Configuration

Enable system 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

Device reboot – system will send notification about unexpected or administrator initiated device reboot.

System uptime – system will send notification about unit's uptime on preset time interval.

Uptime send interval – set the time interval, at which the information about device uptime will be send.

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.

Ping delay – if enabled, system will send continuously ping requests to the host, specified below, and in case ping delay will reach presetted interval, the notification will be sent.

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

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: 5.

SNMP

SNMP is the standard protocol that is widely used for remote network management over the Internet. With the SNMP enabled, the Dahua device will act as SNMP agent. SNMP Agent provides an interface for device monitoring using the Simple Network Management Protocol, thus the network administrator is able to monitor network performance, find and solve network problems.

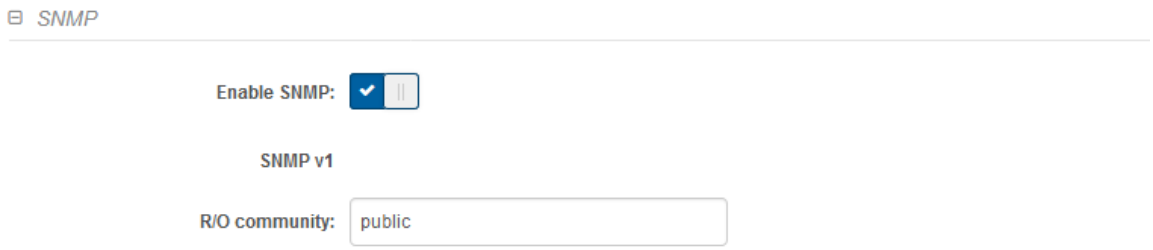


Figure 66 – SNMP Service Settings

Enable SNMP – specify the SNMP service status.

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

Ping watchdog

Enable Ping Watchdog for continuous monitoring of the Dahua unit network connection with the specified trusted host. If enabled, the 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 unit.

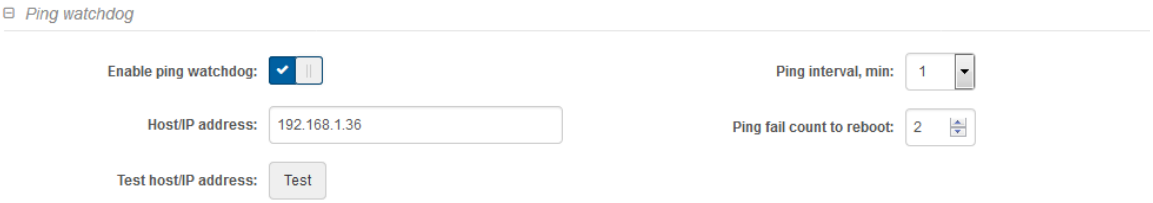


Figure 67 –Ping Watchdog

Enable ping watchdog – click to enable Ping Watchdog function.

Host/IP address – specify the host where the Ping requests will be sent to.

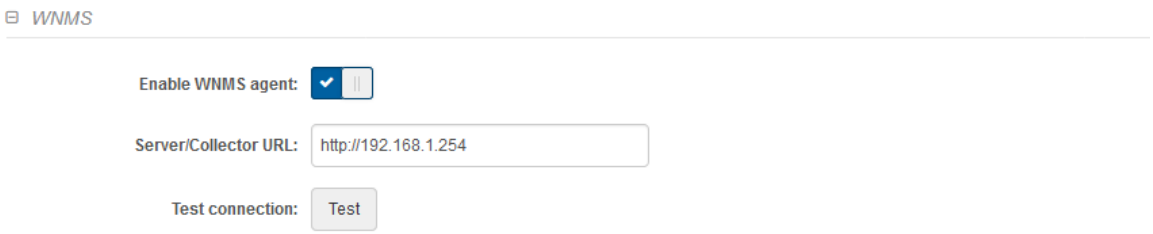
Test host/IP address - click this button to check if the specified host responses successfully.

Ping interval - specify the interval, in minutes, between Ping requests.

Ping fail count to reboot - specify the count of failed Ping replies. After specified count of Ping failures, the unit will reboot itself automatically.

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

System configuration

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

- Device settings
- System functions
- User accounts
- LED settings
- Advanced settings

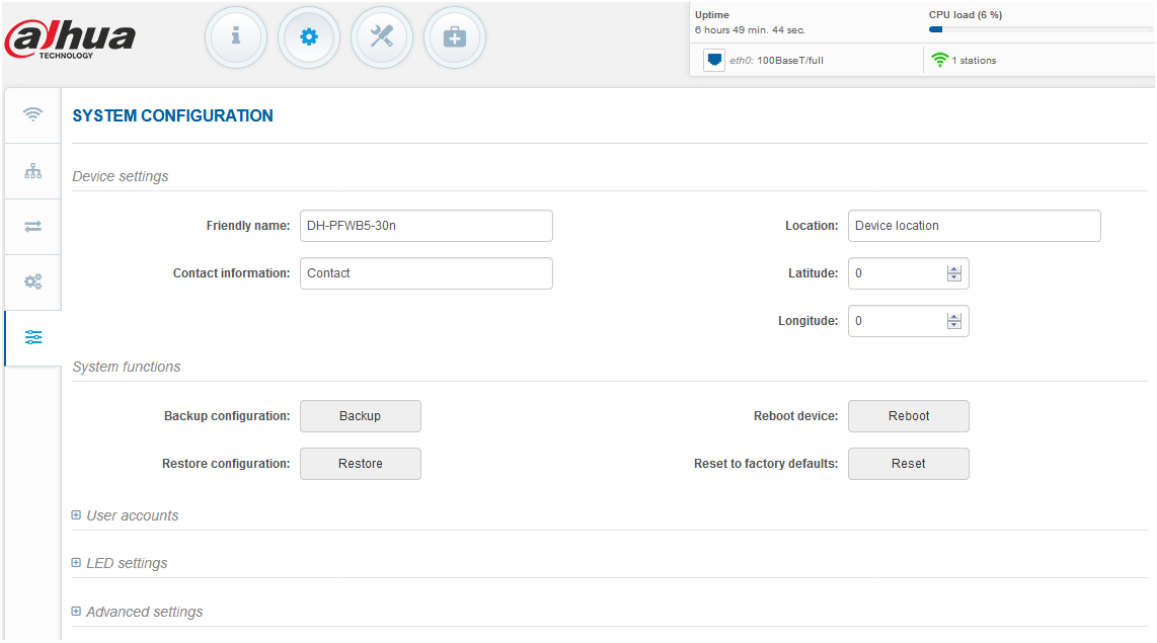


Figure 68 - System Menu

Device settings

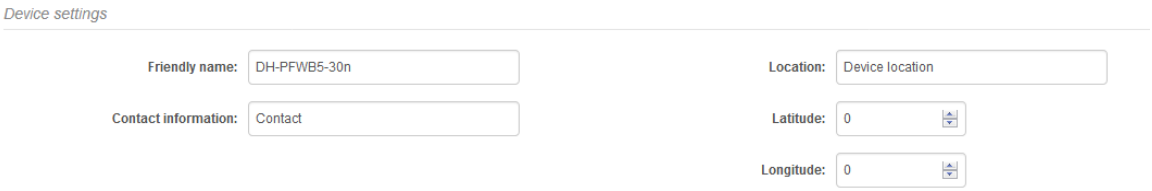


Figure 69- Device Settings

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

Contact information – specify the name of the contact person, such as a network administrator, for the unit.

Location – describe the physical location of the device.

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.

System functions

Figure 70 - System Functions

Backup configuration – 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 – click to upload an existing configuration file to the device. After the configuration file is uploaded, the new configuration will be effective after the *Save changes* button is pressed.

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.

User accounts

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

Use this section to modify device user access credentials, to prevent unit from unauthorized configuration.

Figure 71 – User Accounts

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

Click **Edit** button next to user for changing credentials:

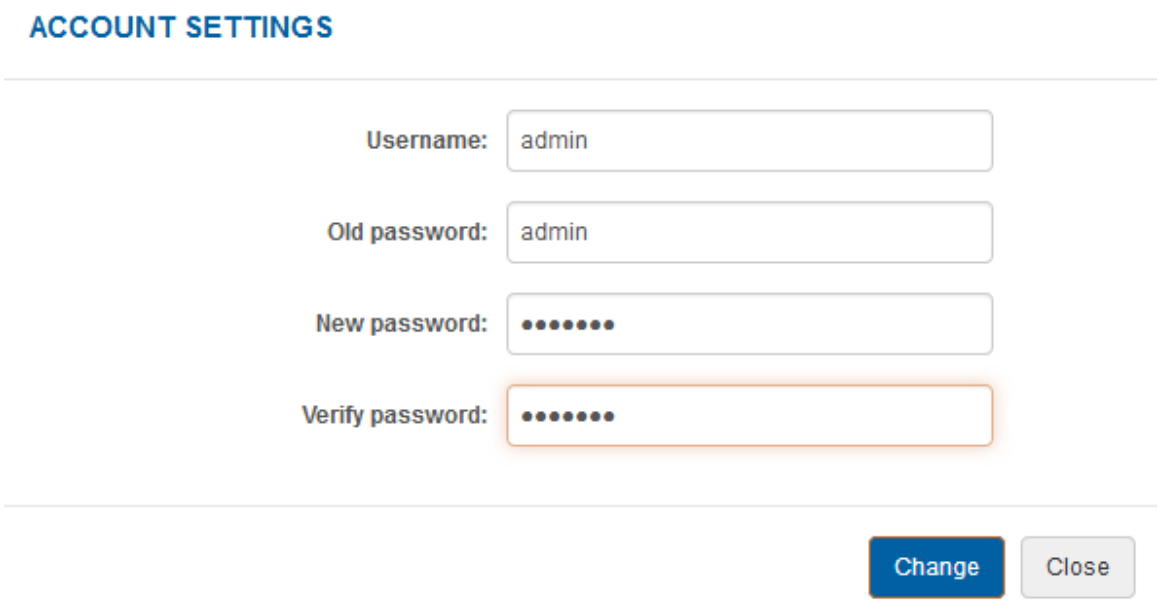


Figure 72 – User Account Settings

Username – change the administrator's username.

Old password – enter the current administrator password.

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

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.

LED settings

The device has possibility to control LEDs.

Figure 73 – Device LED Control

LED status – use the slide to disable or enable LED signals on the unit.

Advanced settings

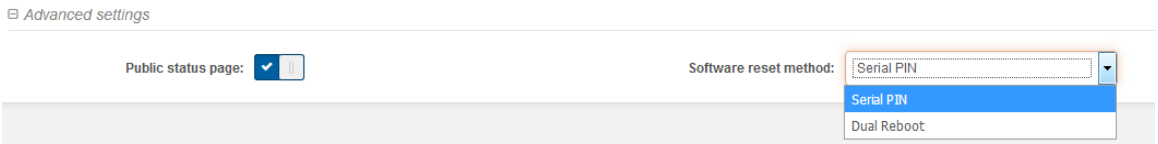


Figure 74 – Device discovery

Public status page –enable or disable the permission for not logged users to view the Status page.

Software reset method – select what reset method to use.

Firmware upgrade

The current version of the device firmware is shown on the upper left corner of the Web interface.

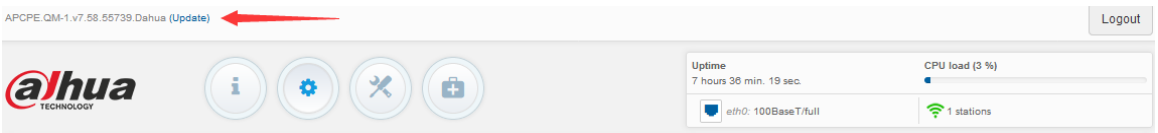


Figure 75 – Firmware Version

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.

Click the **(Update)** link near the running firmware name and select the proper firmware image in the Firmware Update pop-up window, then click **Upload** button:

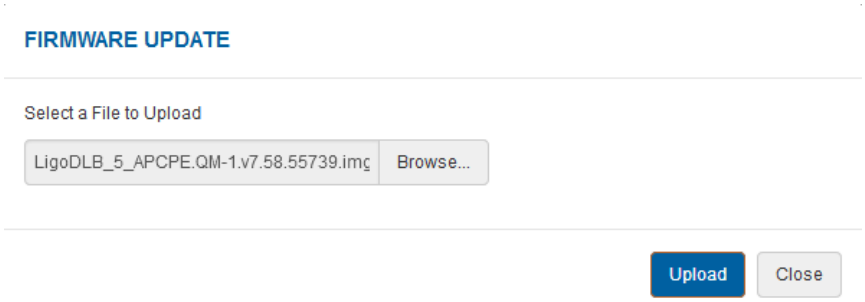


Figure 76 – Firmware Upload

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 77 –Firmware Upgrade

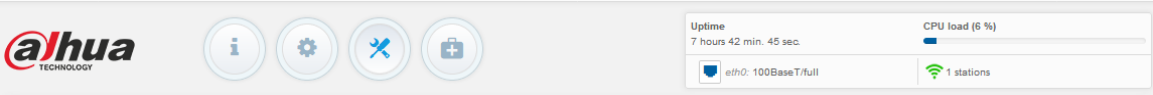
Current version – displays version of the current firmware.

Uploaded version – displays version of the uploaded firmware.

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.

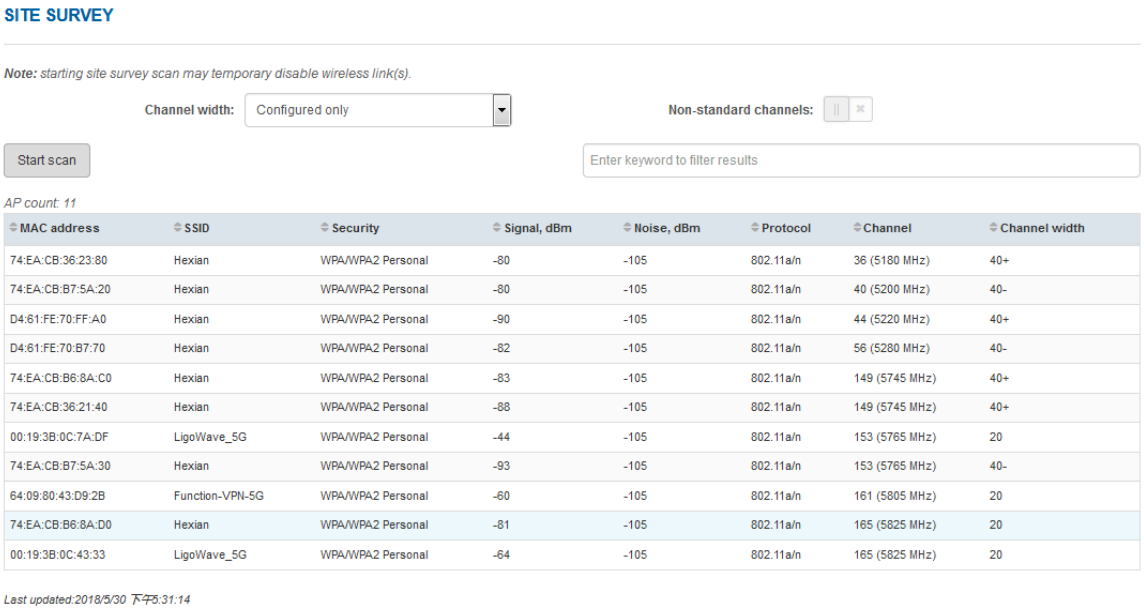
Tools



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 wireless devices, check their operating channels, encryption and see signal/noise levels.

To perform the Site Survey test currently, click the **Start scan**:



MAC address	SSID	Security	Signal, dBm	Noise, dBm	Protocol	Channel	Channel width
74:EA:CB:36:23:80	Hexian	WPA/WPA2 Personal	-80	-105	802.11a/n	36 (5180 MHz)	40+
74:EA:CB:B7:5A:20	Hexian	WPA/WPA2 Personal	-80	-105	802.11a/n	40 (5200 MHz)	40-
D4:61:FE:70:FF:A0	Hexian	WPA/WPA2 Personal	-90	-105	802.11a/n	44 (5220 MHz)	40+
D4:61:FE:70:B7:70	Hexian	WPA/WPA2 Personal	-82	-105	802.11a/n	56 (5280 MHz)	40-
74:EA:CB:B6:8A:C0	Hexian	WPA/WPA2 Personal	-83	-105	802.11a/n	149 (5745 MHz)	40+
74:EA:CB:36:21:40	Hexian	WPA/WPA2 Personal	-88	-105	802.11a/n	149 (5745 MHz)	40+
00:19:3B:0C:7A:DF	LigoWave_5G	WPA/WPA2 Personal	-44	-105	802.11a/n	153 (5765 MHz)	20
74:EA:CB:B7:5A:30	Hexian	WPA/WPA2 Personal	-93	-105	802.11a/n	153 (5765 MHz)	40-
64:09:80:43:D9:2B	Function-VPN-5G	WPA/WPA2 Personal	-60	-105	802.11a/n	161 (5805 MHz)	20
74:EA:CB:B6:8A:D0	Hexian	WPA/WPA2 Personal	-81	-105	802.11a/n	165 (5825 MHz)	20
00:19:3B:0C:43:33	LigoWave_5G	WPA/WPA2 Personal	-64	-105	802.11a/n	165 (5825 MHz)	20

Figure 78 – Site Survey Results

Channel width – choose the channel width at which the scan will be performed:

- **Configured only** – with this option the scan will be performed on configured channel width (refer to the *Status* | *Information* page where the operating channel width is indicated)
- **All possible** – with this option, the scan will be performed on all available channel widths.

Start/Stop scan – click to start or to stop the scan.

Additionally, two charts display connected **Device count** and **Signal leve**l on particular frequencies. The grey colored column represents the unit's operating frequency:

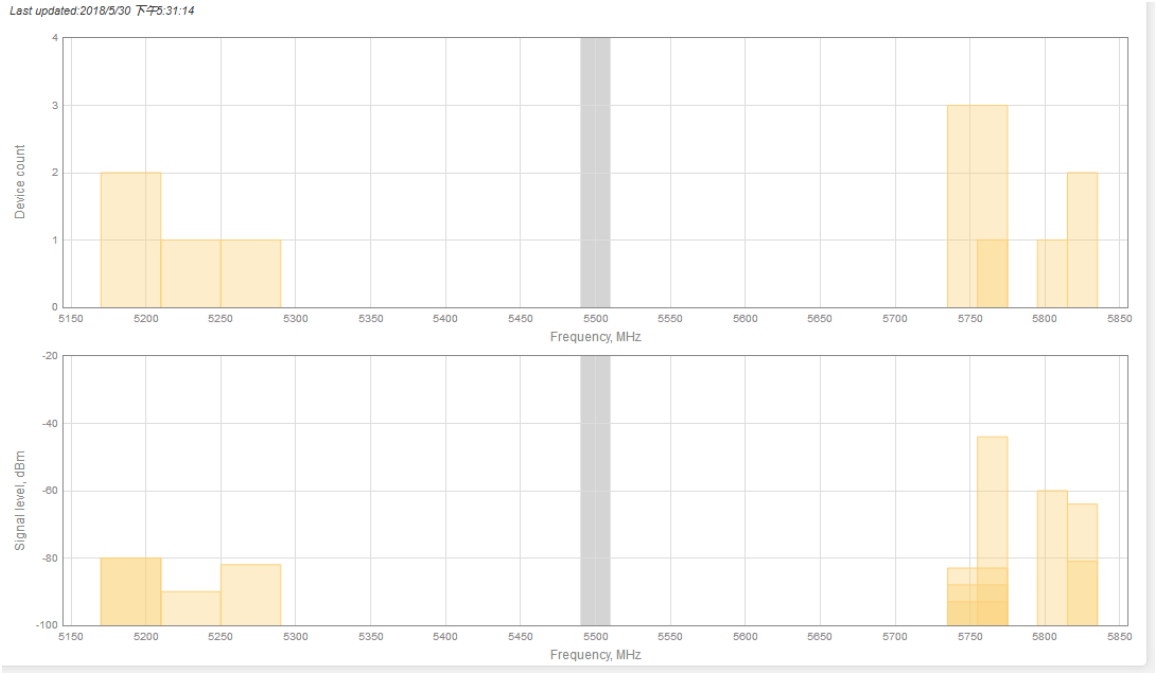


Figure 79 - Site Survey Charts: Device count and Signal level.

Antenna alignment

The Antenna Alignment tool measures signal quality between the Station and AP. For best results during the antenna alignment test, 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 as you adjust the antenna.

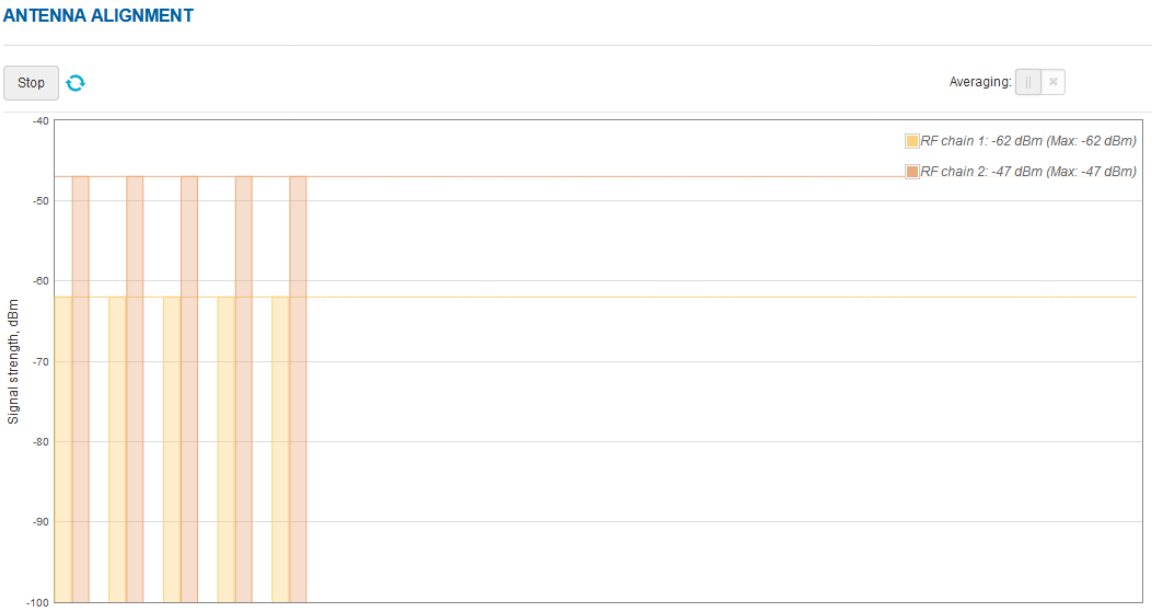


Figure 80 – Antenna Alignment

Start – press this button to start antenna alignment.

Stop – press this button to stop antenna alignment.

Averaging – if this option enabled, the graph will display the average Signal Strength of both antennas.

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 **TDMA 2 / TDMA 3** link. This tool tests the throughput at selected packet sizes and iterations.

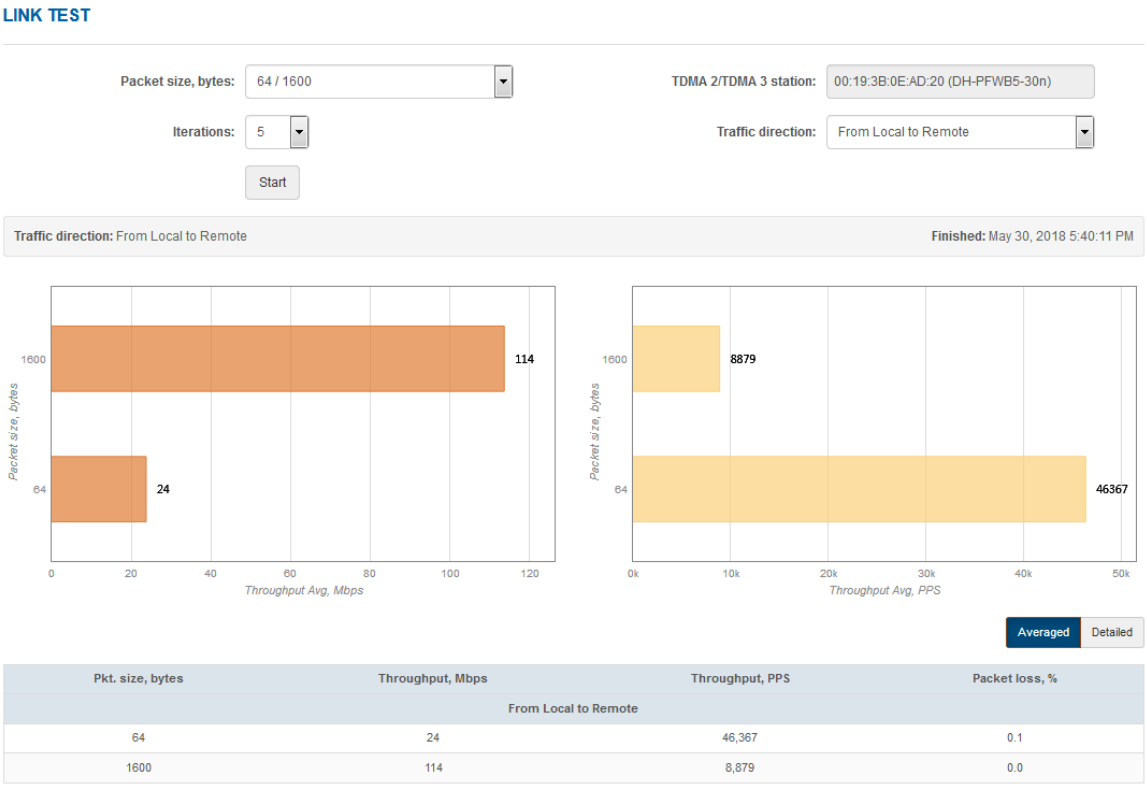


Figure 81 – Linktest Results

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

Iterations - select number of test iterations.

TDMA 2 / TDMA 3 Access Point – displays the Access Point information (if the Link Test is performed from the TDMA 2 / TDMA 3 station side).

TDMA 2 / TDMA 3 Station – select the Station by MAC address the Link Test will be performed with (if the Link Test is performed from the TDMA 2 / TDMA 3 Access Point side).

Traffic direction – select the traffic direction for the performing test.

Start – click to start the throughput test.

Stop – click to stop the throughput test.

Spectrum Analyzer

The **Spectrum analyzer** test displays detailed information about signal level of each 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.

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

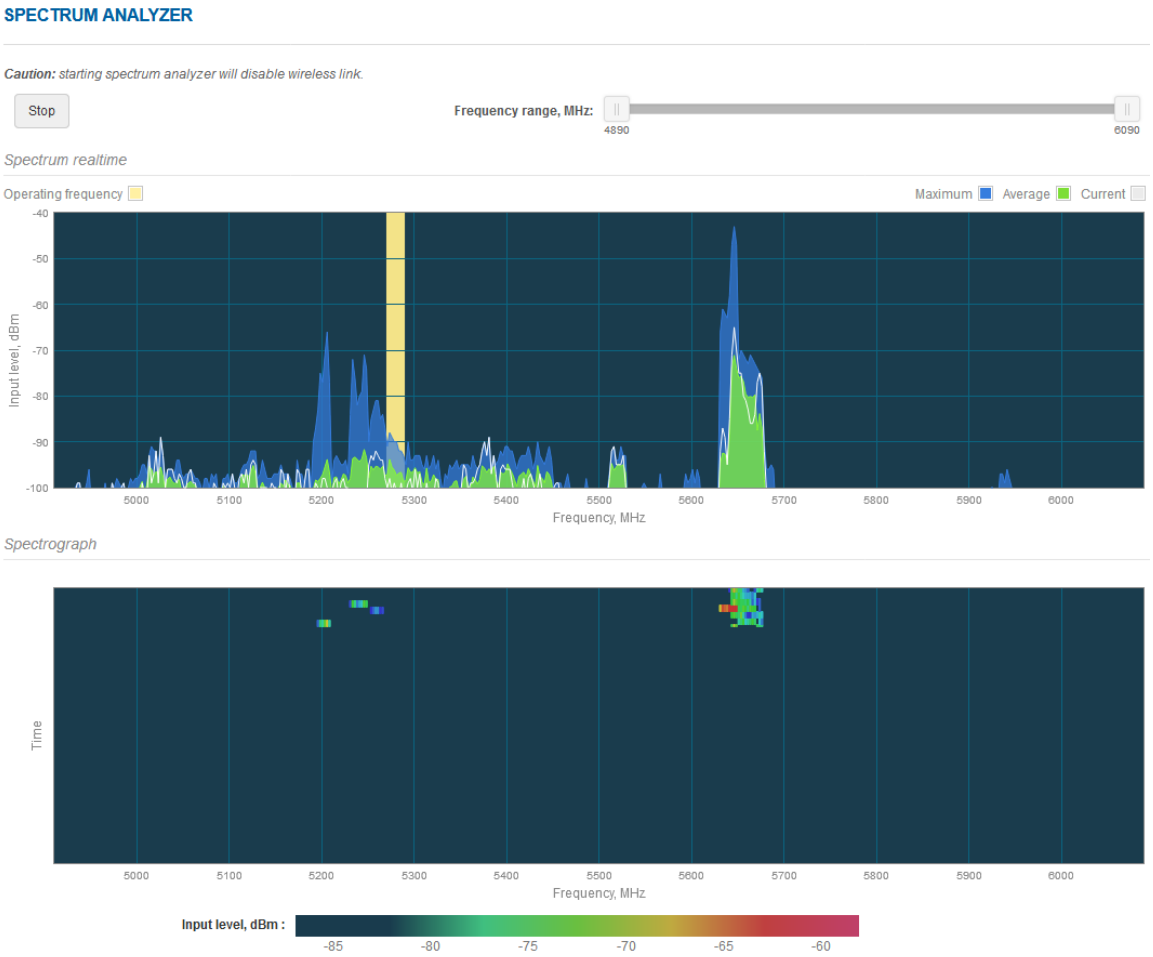


Figure 82 – Spectrum Analyzer Results

Ping & Trace

Use **Ping** tool to discover how long it takes for packets to reach the specified trusted host. The ping results are displayed in the table and graphically:

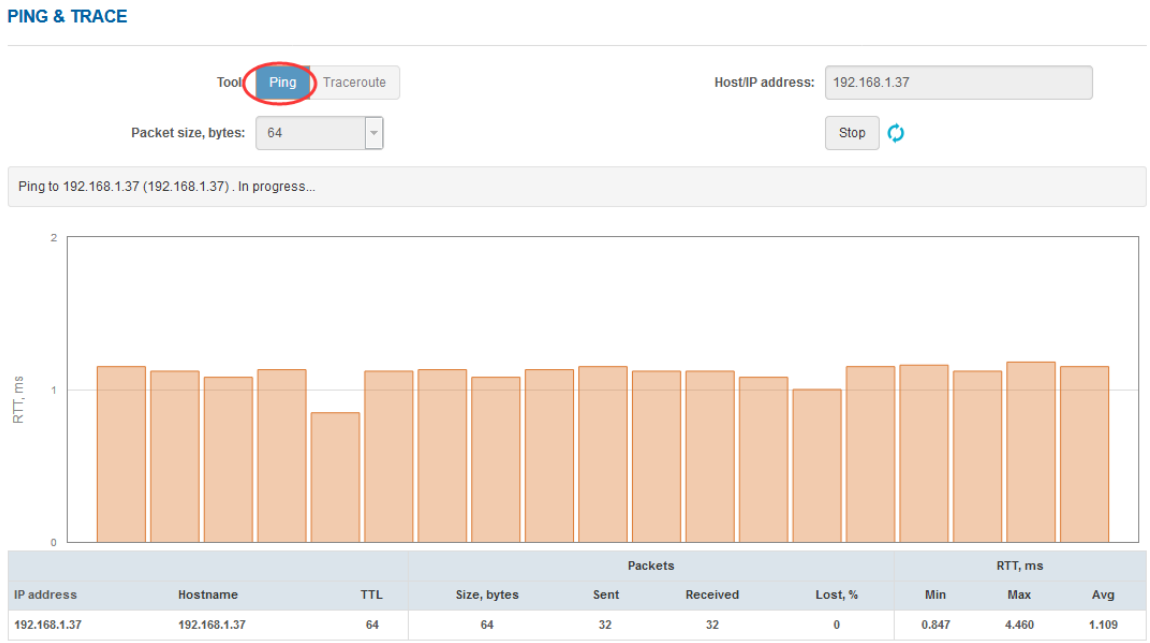


Figure 83 - Ping tool

Host/IP address – specify the host where the Ping requests will be sent to.

Packet size (bytes) – specify the size in bytes of the packet.

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

Use **Traceroute** tool to track the route of packets to the destination host from Dahua unit. This is useful when trying to find out why destination is unreachable, as you will be able to see where the connection fails.

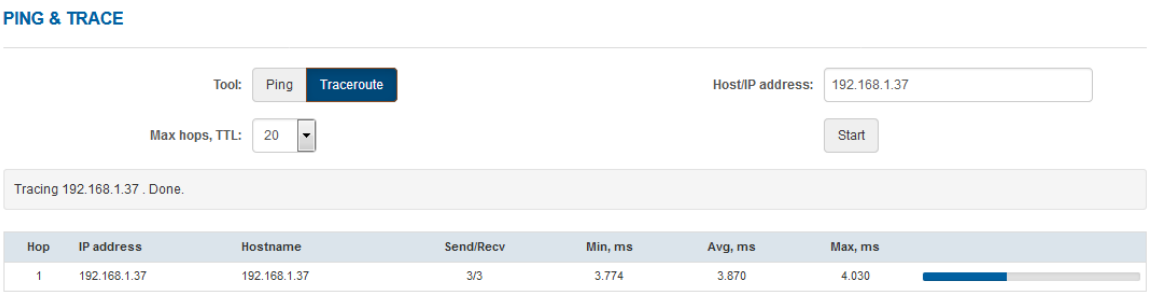


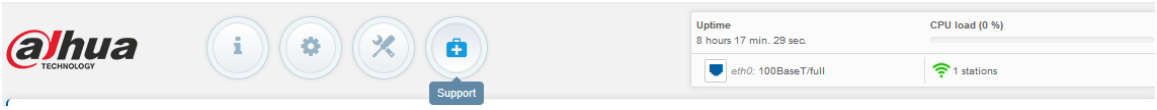
Figure 84 - Trace tool

Host/IP address – specify hostname or IP address of the target host.

Max hops (TTL) – specify the maximum number of hops to search for target.

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

Support



Troubleshooting

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.

Figure 85 – Troubleshooting File Download

Download– click to download the troubleshooting file. This may take a few minutes to gather information and to complete download.

System log

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.

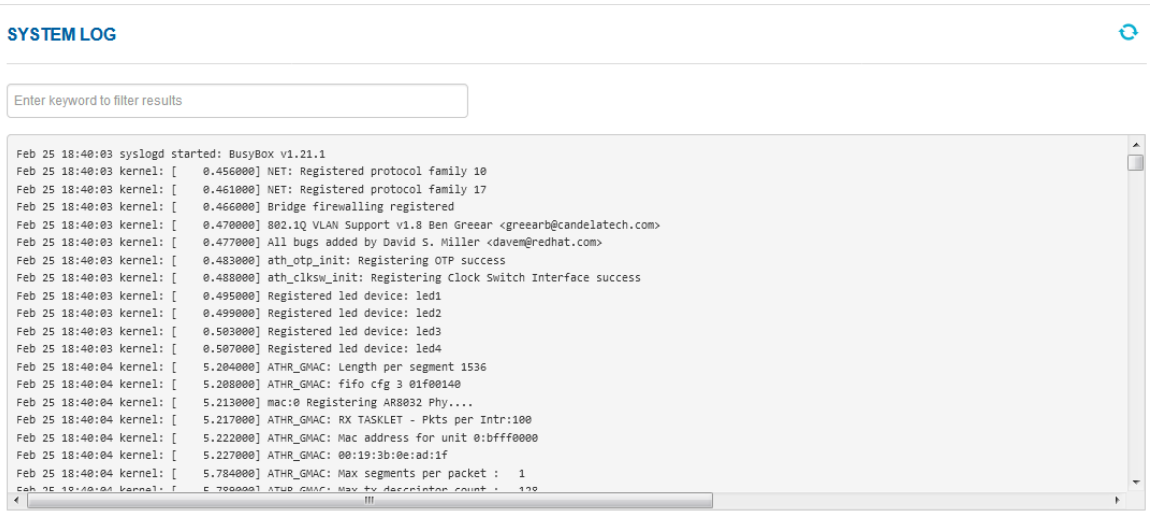


Figure 86 – Device System Log

Click the refresh icon, on the upper right corner, to view current system messages.

Поставщик систем безопасности TELECAMERA.RU

Index

Поставщик систем безопасности TELECAMERA.RU

P

Q

R

S

T

U

V

W