



ZCN M5/M2 Series

User Guide

Revision 1.0

Jan 1, 2015

Copyright © 2015 ZDC WIRELESS

Copyright

© 2015 ZDC Wireless

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 ZDC Wireless.

Notice

ZDC Wireless 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. ZDC Wireless 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 ZDC Wireless.

Trademarks

ZDC Wireless logo is trademark of ZDC Wireless.

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

- Copyright.....
- 2 Notice.....
- 2 Trademarks.....
- 2 FCC Warning
- 3 FCC Caution..... 3
- FCC Radiation Exposure Statement
- 3 CE Mark Warning
- 3 R&TTE Compliance Statement
- 3
- Safety
- 3 EU Countries Intended for Use
- 3 EU Countries Not Intended for Use
- 3
- CONTENTS**
- 4 ABOUT THIS GUIDE.....**
- 6 Purpose..... 6
- Definitions, Acronyms and Abbreviations..... 6
- Abbreviation List..... 6
- FIRST CONNECTION**
- 9 ZCN-M5/M2 CONFIGURATION**
- 11 Applying and Saving Configuration Changes 11
- Status 11
- Information..... 11
- Statistics 13
- Wireless 14
- Settings 15
- Network Configuration 15
- Bridge 15
- Router IPv4..... 17
- Router IPv6..... 20
- IPv6 WAN (wired) settings: Dynamic Stateless..... 20
- IPv6 WAN (wired) settings: Dynamic Stateful 21
- IPv6 WAN (wired) settings: Static..... 21
- IPv6 WAN (wired) settings: PPPoE 21
- LAN (wireless) Settings 22
- Wireless 23
- Wireless Mode: Access Point (auto WDS) 24
- Wireless Mode: Access Point (iPoll 2)..... 28
- Wireless Mode: Station (WDS/iPoll 2)..... 31
- Wireless Mode: Station (ARPNAT)..... 34
- Wireless Security..... 37
- Wireless ACL..... 40
- Services Configuration 41
- Date & time..... 41
- Remote Management 42
- SNMP 42
- Ping watchdog 43
- WNMS 43
- System Configuration 44
- Device settings 44
- System functions 45
- User accounts..... 45
- LED settings 46
- Advanced settings 46

- Firmware Upgrade 51
- 46 Tools 51
 - 48 Site Survey 51
 - 48 Antenna Alignment 51
 - 48 Link Test 51
- 49 Support..... 51
 - 50 Troubleshooting 51
- 51 System Log..... 51
- INDEX 52**

About This Guide

Purpose

This document provides information and procedures on installation, setup, configuration, and management of the ZCN-M5/M2 unit.

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

Abbreviation	Description
IP	Internet Protocol
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.
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
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

First connection

The default product address is dynamic, given by DHCP server. If there is no DHCP server running on the network, the device will fallback to 192.168.2.66 IP address.



The default administrator login settings are:

Login: admin

Password: admin01

Follow the steps for first connection to the device:

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/admin01**.

The initial login screen looks as follow:

A screenshot of a web-based login interface. At the top, the word 'LOGIN' is displayed in orange. Below it are three input fields: 'Username' with a person icon, 'Password' with a key icon, and a language dropdown menu currently set to 'English'. A small downward arrow is visible on the right side of the language field. At the bottom right of the form is an orange 'Login' button.

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 than the permitted values for your country and regulatory domain.

OPERATING COUNTRY

User agreement

The correct country code must be selected before using the equipment to meet the regulatory requirements for authorized channels, channel width, output power, Dynamic Frequency Selection (DFS) and Automatic Transmit Control (ATC).

Installer or equipment owner takes all responsibility for proper product usage according to the regulatory rules.

Vendor or distributor/reseller is not responsible for illegal wireless equipment operation.

I agree

Operating country:

2.4 GHz Antenna gain, dBm:

5 GHz Antenna gain, dBm:

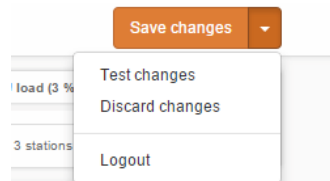
- Step 4.** After successful administrator login you will see the main page of the device Web management interface. The device now is ready for configuration.

ZCN-M5/M2 Configuration

This document contains the product's web management interface configuration description, allowing setups ranging from very simple to very complex.

Applying and 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 the device is working properly, and then Save changes. In case wrong settings were chosen (or even after faulty settings, administrator has 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 the action button is used, all changes will be applied.

Status

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

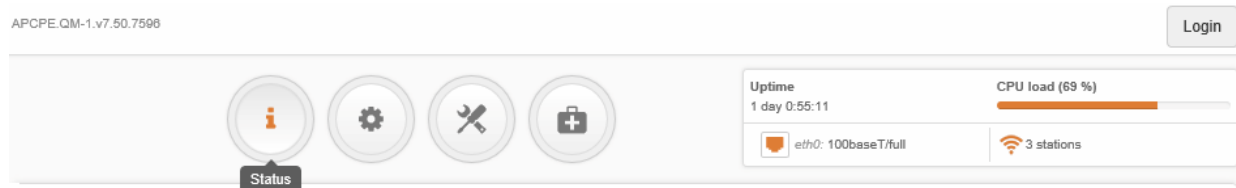


Figure 1 - Web Management Interface



Information

The Information page displays a summary of status information of your device. It shows important information for the ZCN-M5/M2 operating mode, radio, and network settings.

INFORMATION



Product name:		Operating country:	GB
Device serial No.:	081414200000142E	Friendly device name:	
Network mode:	Bridge	Device location:	Device location
Wireless mode:	Access point (iPoll 2)	Latitude/Longitude:	1 / 0

Radio

Channel:	157 (5785 MHz)	Protocol:	iPoll 2
Channel width (MHz):	20	Radio mode:	MIMO 2x2
Tx power (dBm):	20	Antenna gain (dB):	0
Noise level (dBm):	-95		

Wireless (Access point (iPoll 2))

Network SSID	Security	Broadcast SSID	VLAN	Stations
mtp	WPA/WPA2 Personal	Yes	--	0

Network

IP method:	Static	IPv6 method:	Disabled
IP address:	10.0.95.10		
Subnet mask:	255.255.255.0		
Default gateway:	10.0.95.1		

Figure 2 – Device Information Page



If ZCN-M5/M2 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, iPoll wireless modes:

- **Access point (Auto WDS) and (Access Point (iPoll 2))** – displays access point operating information: SSID, Security type, SSID Broadcast status, VLAN and number of connected clients.
- **Station (WDS/iPoll) 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 and traffic graphs of wired and wireless interfaces:

STATISTICS

Interface counters

Interface	MAC address	Tx data	Rx data	Tx packets	Rx packets	Tx errors	Rx errors
eth0 (eth0)	00:19:3B:03:16:79	192.70 MiB	243.87 MiB	767.50 k	455.65 k	0	0
lo	00:00:00:00:00:00	2.14 KiB	2.14 KiB	26	26	0	0
br0	00:19:3B:03:16:79	113.77 MiB	227.26 MiB	534.44 k	507.76 k	0	0
ath0 (mptp)	00:19:3B:03:16:78	1.87 GiB	740.86 MiB	13.19 M	11.98 M	0	0
wifi0	00:19:3B:03:16:78	1.87 GiB	1.27 GiB	27.01 M	27.66 M	1.12 k	0

Figure 3 – Network Statistics: Interface counters

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.

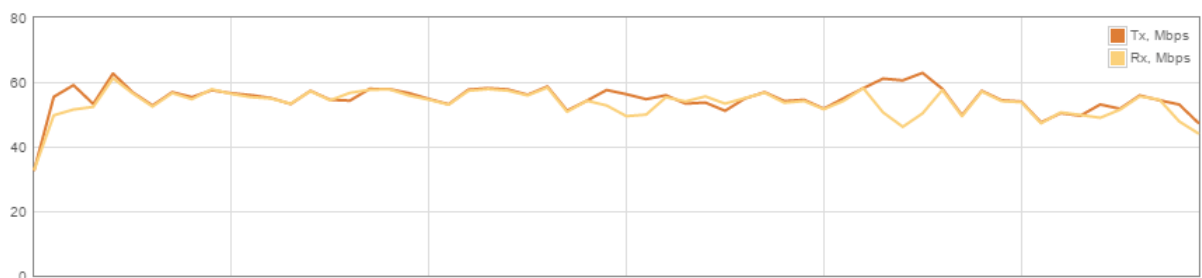
Rx packets – displays the number of received packets.

Tx errors – displays the number of the TX errors.

Rx errors – displays the number of the RX errors.

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

Wired (eth0) traffic (last 5 min.)



Wireless (ath0) traffic (last 5 min.)

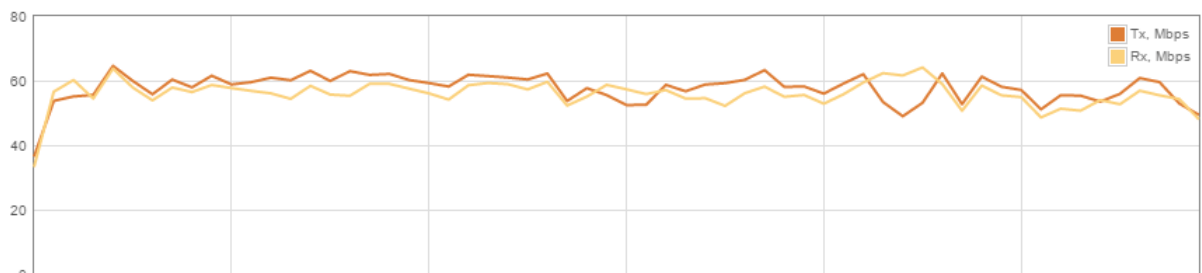


Figure 4 – Network Statistics: Graphs



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



Wireless



Status Wireless section is not available if device is operating as Station (WDS/iPoll) 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):

WIRELESS 

Enter keyword to filter results Info Counters

SSID: *atheros-mptp*

Total stations/limit: 2 / 128

<input type="checkbox"/>	Station	IP address	Signal, dBm	Tx/Rx rate, Mbps	Tx/Rx CCQ, %	Protocol	Link uptime
<input type="checkbox"/>	00:25:82:01:87:BC CPE12	0.0.0.0	-70 / -72	243 / 270	-- / --	W-Jet	0 min. 12 sec.
<input type="checkbox"/>	00:19:3B:84:9E:BD	0.0.0.0	-71 / -71	162 / 6	-- / --	W-Jet	0 min. 9 sec.

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.

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

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.

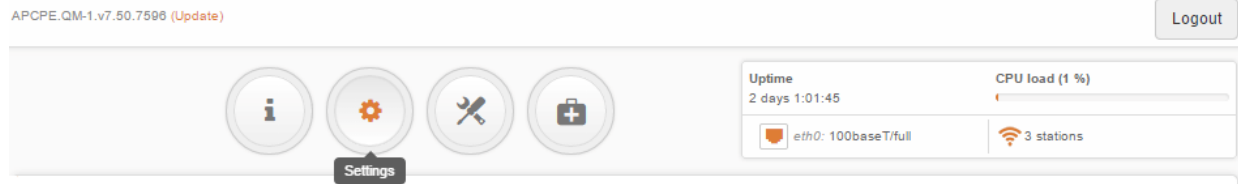
Protocol – displays the protocol at which the access point communicates with the particular station.

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.

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:

NETWORK CONFIGURATION



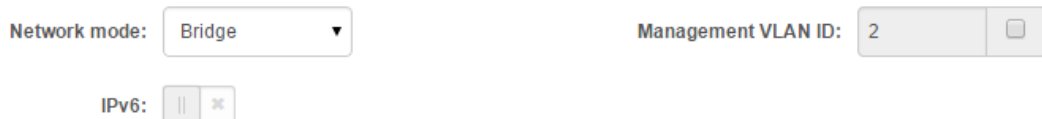
Figure 6 – Network Mode Options

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.

Bridge

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

NETWORK CONFIGURATION



IPv4 configuration

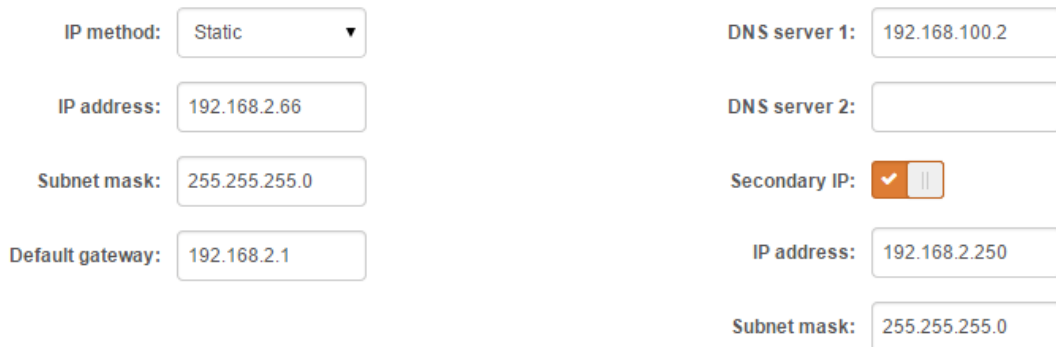


Figure 7 – Bridge Mode Settings

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 unit management.

IPv6 Configuration

Click the **IPv6** slide to enable IPv6 configuration:

NETWORK CONFIGURATION

Network mode:	<input type="text" value="Bridge"/>	Management VLAN ID:	<input type="text" value="2"/>
IPv6:	<input checked="" type="checkbox"/>		

IPv4 configuration

IP method:	<input type="text" value="Static"/>	DNS server 1:	<input type="text" value="192.168.100.2"/>
IP address:	<input type="text" value="192.168.2.66"/>	DNS server 2:	<input type="text"/>
Subnet mask:	<input type="text" value="255.255.255.0"/>	Secondary IP:	<input checked="" type="checkbox"/>
Default gateway:	<input type="text" value="192.168.2.1"/>	IP address:	<input type="text" value="192.168.2.250"/>
		Subnet mask:	<input type="text" value="255.255.255.0"/>

IPv6 configuration

IPv6 method:	<input type="text" value="Static"/>	IPv6 DNS server 1:	<input type="text"/>
IPv6 address:	<input type="text" value="fc00::c0:a8:2:42"/>	IPv6 DNS server 2:	<input type="text"/>
IPv6 prefix length:	<input type="text" value="64"/>		
IPv6 default gateway:	<input type="text" value="fc00::c0:a8:2:1"/>		

Figure 8 – 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. When device is configured to operate as Router, the following sections should be specified: WAN network settings, LAN network settings and LAN DHCP settings.

NETWORK CONFIGURATION

Network mode: Router IPv4 Enable NAT:

WAN (wired)

IP method: Dynamic DNS servers: Use following

DHCP IP fallback

IP address: 192.168.3.66 DNS server 1: 8.8.8.8

Subnet mask: 255.255.255.0 DNS server 2:

Default gateway: 192.168.3.1 Secondary IP:

LAN (wireless)

IP address: 192.168.2.66 Enable DHCP server:

Subnet mask: 255.255.255.0 IP address from: 192.168.2.101

IP address to: 192.168.2.200

Lease time (s): 86400

Figure 9 – 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:

WAN (wired)

IP method: Static DNS server 1: 8.8.8.8

IP address: 192.168.3.66 DNS server 2:

Subnet mask: 255.255.255.0 Secondary IP:

Default gateway: 192.168.3.1 IP address: 192.168.2.250

Subnet mask: 255.255.255.0

Figure 10 – 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 ZCN-M5/M2 unit management.

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

WAN (wired)

The screenshot shows the 'WAN (wired)' configuration page for a Dynamic IP method. The 'IP method' is set to 'Dynamic'. The 'DNS servers' are set to 'Obtain automatically'. The 'DHCP IP fallback' section is active, showing 'IP address: 192.168.3.66', 'Subnet mask: 255.255.255.0', and 'Default gateway: 192.168.3.1'. The 'Secondary IP' section is also active, showing 'Secondary IP' checked, 'IP address: 192.168.2.250', and 'Subnet mask: 255.255.255.0'.

Figure 11 – 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 ZCN-M5/M2 unit will not get the IP address from the DHCP, the specified fallback IP settings will be used.

Enable secondary IP – specify the alternative IP address and the netmask for ZCN-M5/M2 unit 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:

WAN (wired)

The screenshot shows the 'WAN (wired)' configuration page for a PPPoE client. The 'IP method' is set to 'PPPoE'. The 'DNS servers' are set to 'Obtain automatically'. The 'Username' is 'user', the 'Password' is masked with '****', and the 'MTU (bytes)' is '1492'. The 'Secondary IP' section is disabled, indicated by a greyed-out checkbox.

Figure 12 – 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.

Enable secondary IP – specify the alternative IP address and the netmask for ZCN-M5/M2 unit management.

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.

LAN (wireless)



The screenshot shows the LAN settings configuration interface. It includes the following fields and controls:

- IP address:** 192.168.2.66
- Subnet mask:** 255.255.255.0
- Enable DHCP server:** A toggle switch that is currently turned on (checked).
- IP address from:** 192.168.2.101
- IP address to:** 192.168.2.200
- Lease time (s):** 86400

Figure 13 – 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.

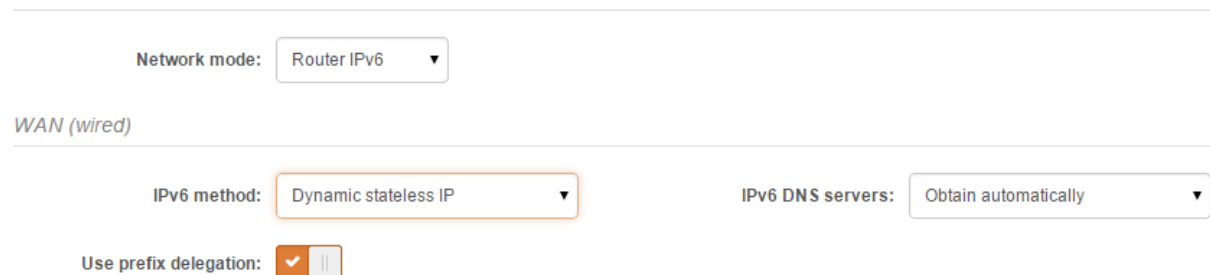
Router IPv6

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.

NETWORK CONFIGURATION



The screenshot shows the IPv6 WAN settings configuration interface. It includes the following fields and controls:

- Network mode:** Router IPv6 (selected from a dropdown menu)
- WAN (wired)** section:
- IPv6 method:** Dynamic stateless IP (selected from a dropdown menu)
- IPv6 DNS servers:** Obtain automatically (selected from a dropdown menu)
- Use prefix delegation:** A toggle switch that is currently turned on (checked).

Figure 14 – 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.

WAN (wired)

The screenshot shows the configuration interface for IPv6 WAN (wired) settings in Dynamic Stateful mode. It includes a dropdown menu for 'IPv6 method' set to 'Dynamic stateful IP', a dropdown for 'IPv6 DNS servers' set to 'Obtain automatically', and a checked checkbox for 'Use prefix delegation'.

Figure 15 – 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, settings must be specified manually:

NETWORK CONFIGURATION

The screenshot shows the configuration interface for IPv6 WAN (wired) settings in Static mode. It includes a dropdown for 'Network mode' set to 'Router IPv6', and several input fields: 'IPv6 method' set to 'Static', 'IPv6 address' set to 'fc00::c0:a8:2:42', 'IPv6 prefix length' set to '64', 'IPv6 default gateway' set to 'fc00::c0:a8:2:1', 'IPv6 DNS server 1' set to 'fc00::c0:a8:2:1', and an empty field for 'IPv6 DNS server 2'.

Figure 16 – 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.

NETWORK CONFIGURATION

Network mode: Router IPv6 ▼

WAN (wired)

IPv6 method: PPPoE ▼

IPv6 DNS servers: Obtain automatically ▼

Username: user

Password: ****

MTU (bytes): 1492

Figure 17 – 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.

LAN (wireless)

IPv6 address: fc00:1::c0:a8:2:42

IPv6 prefix length: 64

DHCPv6 server mode: Dynamic stateful IP ▼

IPv6 address from: 2001::1000

IPv6 address to: 2001::ffff

Lease time (s): 86400

Figure 18 – 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 ZCN-M5/M2 device can operate in four wireless modes: Access Point (Auto WDS), Access Point (iPoll 2), Station (auto iPoll 2) and Station (ARPNAT).

WIRELESS CONFIGURATION

The screenshot shows the 'Radio settings' section of the configuration page. It includes a toggle for 'Enable radio' which is turned on, and a dropdown for 'Operating mode' currently set to 'Access point (iPoll 2)'. A dropdown menu is open showing options: 'Access point (auto WDS)', 'Access point (iPoll 2)', 'Station (WDS/iPoll 2)', and 'Station (ARPNAT)'. Other settings include 'Tx power (dBm)' set to 20 and 'Channel' set to 52 (5260 MHz) / 40 MHz. Below this is a section for 'Advanced radio settings' which is currently collapsed, and a table for 'Wireless settings (AP)'.

Network SSID	Security	Management	Broadcast SSID	VLAN
mp1p	WPA/WPA2 Personal	Enabled	Yes	--

Figure 19 – Device Wireless Operating Mode



If ZCN 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)** – sets device 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 (iPoll 2)** – enables ZCN-M5/M2 radio function as access point for point-to-multipoint solution. The Access Point communicates with Station in iPoll 2 protocol, other clients requests will be not accepted.
- **Station (WDS/iPoll 2)** – with this wireless mode the device will act as Station and will automatically turn on iPoll 2 mode if detects that selected AP is operating in iPoll 2 protocol.
- **Station (ARPNAT)** – with this wireless mode the device is configured act as client and to connect to other radio functioning as an access point.

Wireless Mode: Access Point (Auto WDS)

WIRELESS CONFIGURATION

Enable radio:

Operating mode: Access point (auto WDS)

Operating country: GB

Radio settings

IEEE mode: 802.11n

Tx power (dBm):

Channel: 52 (5260 MHz) / 40 MHz

Advanced radio settings

Max 802.11n MCS index: Auto

AMSDU:

Short GI:

Fragmentation:

RTS/CTS:

ACK timeout (µs):
23.40 km / 14.54 miles

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN	
mptp	WPA/WPA2 Personal	Enabled	Yes	--	

Figure 20 – Access Point Wireless Settings

Enable radio – use slide to enable or disable radio.

Operating country – displays unit’s 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].

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.

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

CHANNEL

Channel width (MHz):

Non-standard channels:

<input type="checkbox"/>	Channel	TX limit, dBm	EIRP limit, dBm	DFS/ATPC required
<input type="checkbox"/>	36 (5180 MHz)	23	23	No
<input type="checkbox"/>	44 (5220 MHz)	23	23	No
<input checked="" type="checkbox"/>	52 (5260 MHz)	23	23	Yes
<input type="checkbox"/>	60 (5300 MHz)	23	23	Yes
<input type="checkbox"/>	100 (5500 MHz)	28	30	Yes
<input type="checkbox"/>	108 (5540 MHz)	28	30	Yes
<input type="checkbox"/>	116 (5580 MHz)	28	30	Yes
<input type="checkbox"/>	124 (5620 MHz)	28	30	Yes
<input type="checkbox"/>	132 (5660 MHz)	28	30	Yes
<input type="checkbox"/>	149 (5745 MHz)	28	36	No

Figure 21 – Channel List Table

Channel width – select the width of the operating radio channel. The device 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. .

Channel table – select the channel(s) at which the Access Point will operate. If more than one channel is selected, then auto channel 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.

Advanced Radio Settings

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

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 ZCN 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 ZCN will step down to the highest rate that allows data transmission. Available only on 802.11a or 802.11a/n IEEE modes.

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.

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.

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.


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

Wireless Settings (AP)

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN
mplp	WPA/WPA2 Personal	Enabled	Yes	--

Figure 22 - Wireless Settings

The wireless table allows configure main AP parameters, such as SSID, Security, WACL, etc. Click on the edit icon  and the wireless settings window will be displayed:

WIRELESS AP SETTINGS

SSID:

Broadcast SSID:

Security settings

Security:

WACL

Advanced settings

Figure 23 – Wireless AP Settings

SSID – specify the SSID of the wireless network device.

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



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

Advanced AP Settings

☰ *Advanced settings*

Client isolation:

Map to data VLAN ID:

Max connected clients: 128

Min client signal (dBm): -100

Management over wireless:

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

Map to data 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.

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.

Wireless Mode: Access Point (iPoll 2)

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

WIRELESS CONFIGURATION

Enable radio:

Operating country:

Operating mode:

Radio settings

Tx power (dBm): 20

Channel:

☰ *Advanced radio settings*

Max data rate, Mbps:

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN
mptp	WPA/WPA2 Personal	Enabled	Yes	--

Figure 24 – iPoll Access Point's Wireless Settings

Enable radio – use slide to enable or disable radio.

Operating country - displays ZCN unit's 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.

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

CHANNEL

Channel width (MHz): 40 Upper ▾

Non-standard channels: || ✖

<input type="checkbox"/>	Channel	TX limit, dBm	EIRP limit, dBm	DFS/ATPC required
<input type="checkbox"/>	36 (5180 MHz)	23	23	No
<input type="checkbox"/>	44 (5220 MHz)	23	23	No
<input checked="" type="checkbox"/>	52 (5260 MHz)	23	23	Yes
<input type="checkbox"/>	60 (5300 MHz)	23	23	Yes
<input type="checkbox"/>	100 (5500 MHz)	28	30	Yes
<input type="checkbox"/>	108 (5540 MHz)	28	30	Yes
<input type="checkbox"/>	116 (5580 MHz)	28	30	Yes
<input type="checkbox"/>	124 (5620 MHz)	28	30	Yes
<input type="checkbox"/>	132 (5660 MHz)	28	30	Yes
<input type="checkbox"/>	149 (5745 MHz)	28	36	No

Select Cancel

Figure 25 – Channel List Table

Channel width – select the width of the operating radio channel. The device 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.

Channel table – select the channel(s) at which the Access Point iPoll 2 will operate. If more than one channel is selected, then auto channel 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.

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 data rate that enables errorless data transmission.

Wireless Settings (AP)

Wireless settings (AP)

Network SSID	Security	Management	Broadcast SSID	VLAN
mptp	WPA/WPA2 Personal	Enabled	Yes	--

Figure 26 - Wireless Settings

The wireless table allows configure main AP iPoll2 parameters, such as SSID, Security, WACL, etc. Click on the edit icon  and the wireless settings window will be displayed:

WIRELESS AP SETTINGS

SSID:

Broadcast SSID:

Security:

WACL

Advanced settings

Figure 27 – Wireless AP Settings

SSID – specify the SSID of the wireless network device.

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



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

Advanced AP Settings

Client isolation:

Map to data VLAN ID:

Max connected clients:

Min client signal (dBm):

Management over wireless:

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

Map to data 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.

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 to disable wireless access and instead require a physical network connection using an Ethernet cable for administrative access.

Wireless Mode: Station (WDS/iPoll 2)

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

Use Wireless Configuration to setup radio interface of the device.

Enable radio:

Operating country: GB

Operating mode: Station (WDS/iPoll 2) ▼

Radio settings

Tx power (dBm):

Channel width (MHz): 20/40 ▼

Non-standard channels:

Advanced radio settings

Max 802.11n MCS index: Auto ▼

Max legacy data rate (Mbps): Auto ▼

AMSDU:

Short GI:

Fragmentation:

RTS/CTS:

ACK timeout (µs):
23.40 km / 14.54 miles

Wireless settings (station)

Network SSID	Security	Management	VLAN
mplt	WPA/WPA2 Personal	Enabled	--

Figure 28 – Station Wireless Settings

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

Operating country - displays unit's 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 ZCN-M5/M2 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.

Channel width - select the width of the operating radio channel. The device 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.

Advanced Radio Settings

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

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 data rate that enables errorless data transmission.

Max legacy data rate – choose the maximum data rate in Mbps at which device should transmit packets. It 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.

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.


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

Wireless Settings (Station auto iPoll 2)

Wireless settings (station)

Network SSID	Security	Management	VLAN
atheros-mptp	WPA/WPA2 Personal	Enabled	--

Figure 29 - Wireless Settings

The wireless table allows configure main station parameters, such as SSID of the AP unit, Security, etc. Click on the edit icon  and the wireless settings window will be displayed:

WIRELESS STATION SETTINGS

SSID:

Lock AP by MAC address:

Security settings

Security:

Advanced settings


Wireless VLAN ID:

Figure 30 – Wireless AP Settings

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

SSID:

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:

SEARCH SSID 

MEZON_00159_513 00:15:6D:F8:83:15 -87 dBm WPA/WPA2 Enterprise 802.11a CH52 (5260 MHz)
erdvesM246 DC:9F:DB:EE:51:5A -76 dBm WPA Personal 802.11a/n CH36 (5180 MHz)
MEZON_10116_512 0A:15:6D:D4:35:8E -82 dBm WPA/WPA2 Enterprise 802.11a CH36 (5180 MHz)
erdvesM346 24:A4:3C:EE:11:07 -83 dBm WPA Personal 802.11a/n CH36 (5180 MHz)
erdvesM294 DC:9F:DB:8A:E8:AC -83 dBm WPA Personal 802.11a/n CH36 (5180 MHz)

Last updated: 1/29/2015, 9:36:43 AM

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*.

Advanced AP Settings

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.

Wireless Mode: Station (ARPNAT)



The wireless mode Station (ARPNAT) is available only if the 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:

Enable radio:

Operating mode: Station (ARPNAT)

Operating country: GB

Radio settings

Tx power (dBm):

Channel width (MHz): 20/40

Non-standard channels:

Advanced radio settings

Max 802.11n MCS index: Auto

Max legacy data rate (Mbps): Auto

AMSDU:

Short GI:

Fragmentation:

RTS/CTS:

ACK timeout (µs):
23.40 km / 14.54 miles

Wireless settings (station)

Network SSID	Security	Management	VLAN
mplt	WPA/WPA2 Personal	Enabled	--

Figure 31 – Station Wireless Settings

Enable radio – use slide to enable or disable radio.

Operating country - displays unit's 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 ZCN-M5/M2 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.

Channel width - select the width of the operating radio channel. The device 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.

Advanced Radio Settings

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

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 legacy data rate – choose the maximum data rate in Mbps at which device should transmit packets. It 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 data rate that enables errorless data transmission.

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.


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

Wireless Settings (Station auto iPoll 2)

Wireless settings (station)

Network SSID	Security	Management	VLAN
atheros-mptp	WPA/WPA2 Personal	Enabled	--

Figure 32 - Wireless Settings

The wireless table allows configure main station parameters, such as SSID of the AP unit, Security, etc. Click on the edit icon  and the wireless settings window will be displayed:

WIRELESS STATION SETTINGS

SSID:

Lock AP by MAC address:

Security settings

Security:

Advanced settings


Wireless VLAN ID:

Figure 33 – Wireless AP Settings

SSID – specify the SSID of the wireless network device manually, or scan for iPoll 2 Access Points automatically:

SSID:

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:

SEARCH SSID 

Enter keyword to filter results

MEZON_00159_513 00:15:6D:F8:83:15 -87 dBm WPA/WPA2 Enterprise 802.11a CH52 (5260 MHz)
erdvesM246 DC:9F:DB:EE:51:5A -76 dBm WPA Personal 802.11a/n CH36 (5180 MHz)
MEZON_10116_512 0A:15:6D:D4:35:8E -82 dBm WPA/WPA2 Enterprise 802.11a CH36 (5180 MHz)
erdvesM346 24:A4:3C:EE:11:07 -83 dBm WPA Personal 802.11a/n CH36 (5180 MHz)
erdvesM294 DC:9F:DB:8A:E8:AC -83 dBm WPA Personal 802.11a/n CH36 (5180 MHz)

Last updated: 1/29/2015, 9:36:43 AM

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*.

Advanced AP Settings

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.

Wireless Security

If device is set as an Access Point (auto WDS) or Access Point (iPoll 2) the wireless security settings will be used by the wireless stations for association. Thus wireless station security settings must conform the settings configured on the AP that station is associated with.

The ZCN supports various authentication/encryption methods:

- **Open** – no encryption.
- **WEP** – encrypts the data portion of each packet exchanged on a wireless network using a 64-bit or 128-bit WEP encryption key.
- **Personal WPA/WPA2** – authorizes and identifies clients based on a secret key that changes automatically at regular intervals.
- **Enterprise WPA/WPA2** – RADIUS server based authentication (requires configured RADIUS server).

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

Security method	Access Point (Auto WDS)	Access Point (iPoll 2)	Station (WDS/iPoll 2)	Station (ARPNAT)
Open	x	x	x	x
WEP 64bit/128bit			x	x
Personal WPA/WPA2	x	x	x	x
Enterprise WPA/WPA2	x	x	x	x

Open

By default there is no encryption enabled on the device:

Security settings

Security: Open

Figure 34 – Wireless Security: Open with RADIUS MAC Authentication Enabled

WEP Encryption

WEP encryption can be either 64bit or 128bit. Select the required one and enter the rest parameters:

Security settings

Security: WEP 128bit

Key index: 1

Key: *****

Figure 35 – Wireless Security: WEP Security

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

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

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

WPA/WPA2 Personal

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

Security settings

Security: WPA/WPA2 Personal

Passphrase: *****

Figure 36 – Wireless Security: Personal WPA/WPA2 Security

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

WPA/WPA2 Enterprise for Access Points

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.

Security settings

Security: WPA/WPA2 Enterprise ▼

Auth. server IP/Port: 192.168.2.2 1812

Auth. server key: *****

Accounting server:

Acc. server IP/Port: 192.168.2.2 1813

Acc. server key: *****

Figure 37 –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.

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

Acc. server key – enter the key for the authentication on specified accounting RADIUS server.

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.

Security settings

Security: WPA/WPA2 Enterprise ▼

EAP method: EAP-TTLS ▼

Identity: username

Password: *****

Figure 38 –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.

Wireless ACL



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

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

WACL

MAC filter policy: Deny MAC in the list

Enter keyword to filter table data Add

MAC address	Description	
AC:81:12:57:8F:5F	description	✓ ✕

WACL

MAC filter policy: Deny MAC in the list

Enter keyword to filter table data Add

MAC address	Description	
00:81:12:55:8F:5F	description	✓ ✕
AC:B9:11:02:7C:55	description	✎ ✕

Figure 39 – 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.



Services Configuration

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

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

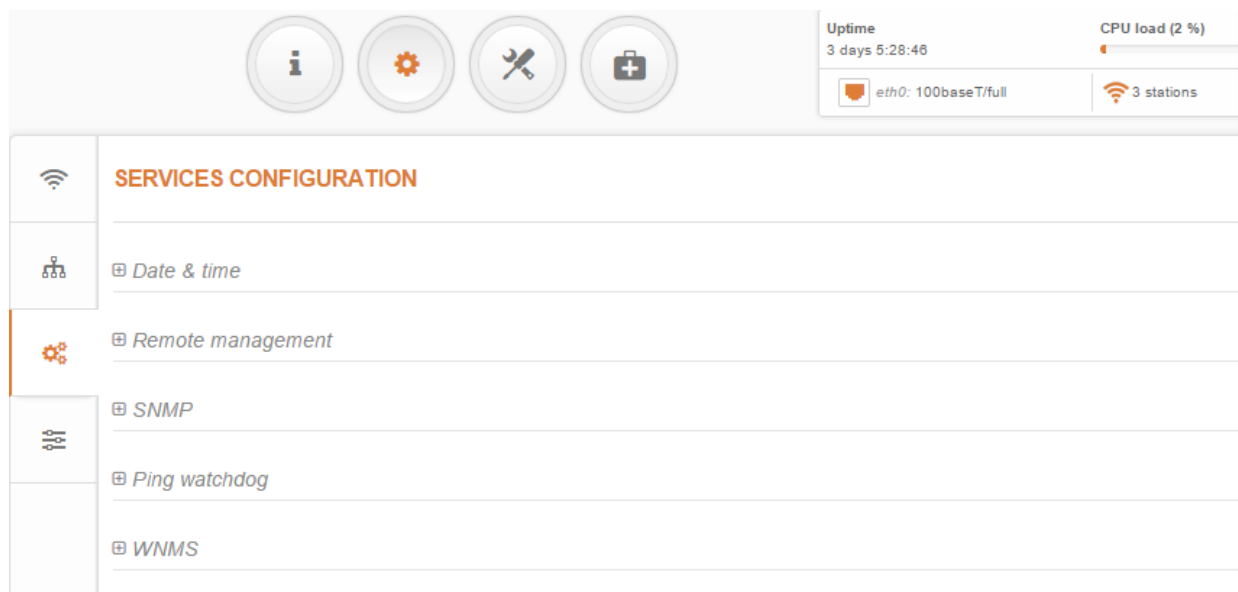


Figure 40 - Services Menu

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.

▢ Date & time

Enable NTP:
Timezone:

NTP server 1:
Date: 30/01/2015

NTP server 2:
Time: 06:03

Test NTP servers:

Figure 41 – Date&time: NTP Configuration

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

Time zone – select the time zone. 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:

☰ *Date & time*

Enable NTP:

Timezone: UTC

Date (DD/MM/YYYY): 01/05/2014

Time (HH:MM): 00:00

Figure 42 – Date&time: Manual Configuration

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

Time zone – select the time zone. 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 or Telnet:

☰ *Remote management*

Enable SSH:

SSH port: 22

Enable telnet:

Telnet port: 23

Figure 43 – 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.

SNMP

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

SNMP

Enable SNMP:

SNMP v1

R/O community:

Figure 44 – 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 a ZCN-M5/M2 manager to read values, but denies any attempt to change values.

Ping watchdog

Enable Ping Watchdog for continuous monitoring of the ZCN-M5/M2 unit network connection with the specified trusted host. If enabled, the ZCN-M5/M2 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 device.

Ping watchdog

Enable ping watchdog:

Host/IP address:

Test host/IP address:

Ping interval (min):

Ping fail count to reboot:

Figure 45 – 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 responds 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 ZCN 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 an WNMS client service running on every device.

WNMS

Enable WNMS agent:

Server/Collector URL:

Test connection:

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

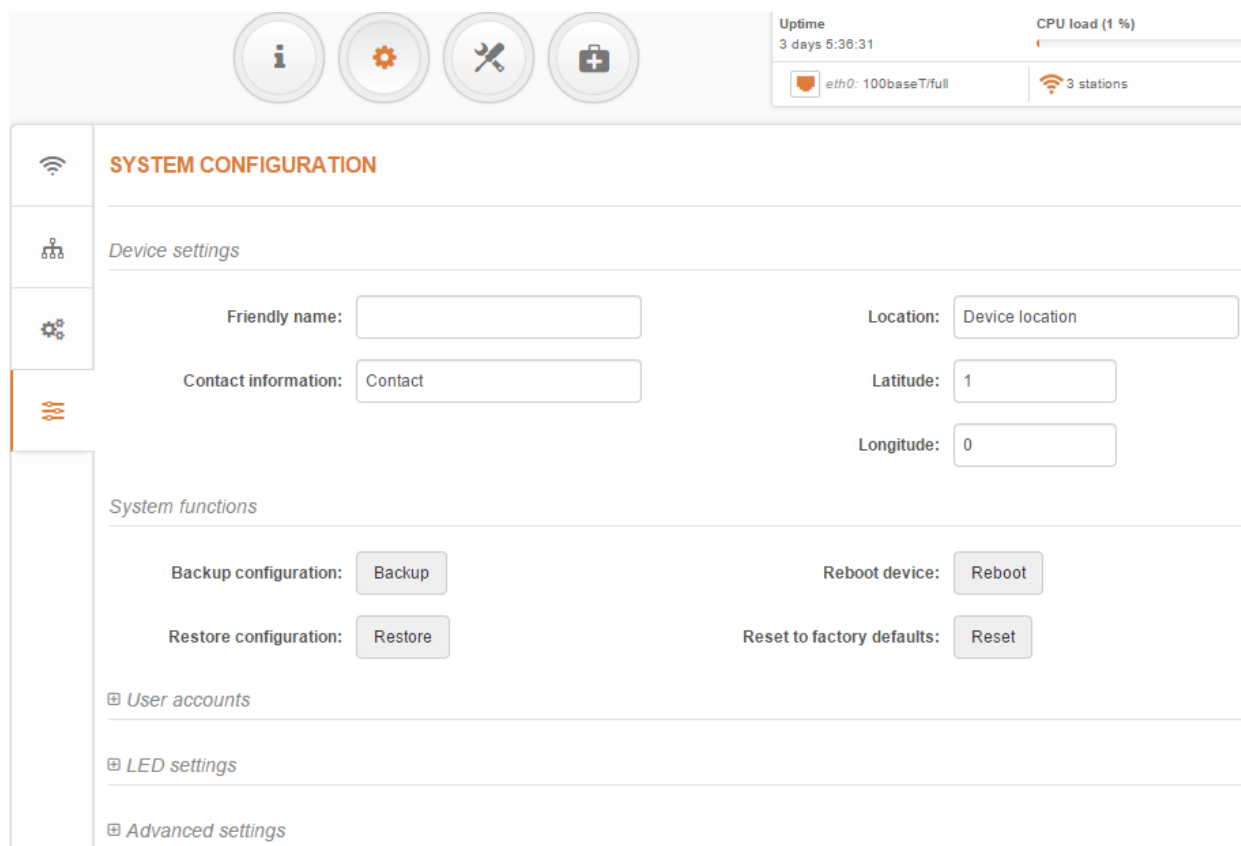


Figure 46 - System Menu

Device settings

Device settings

Friendly device name:	<input type="text"/>	Device location:	<input type="text" value="Device location"/>
Contact information:	<input type="text" value="Contact"/>	Latitude:	<input type="text" value="0"/>
		Longitude:	<input type="text" value="0"/>

Figure 47- 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.

Device location – describe the 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

System functions



Figure 48 - 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.

User accounts

User: admin

Figure 49 – User Accounts



Default administrator logon settings are:

Username: **admin**

Password: **admin01**

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

ACCOUNT SETTINGS

Username	<input type="text" value="admin"/>
Old password	<input type="password" value="*****"/>
New password	<input type="password" value="*****"/>
Verify password	<input type="password" value="*****"/>

Figure 50 – User Account Settings

Username – change the administrator’s username.

Old password – enter the old administrator password.

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

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



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

LED settings

The device has possibility to control LEDs:

☰ [LED settings](#)

LED status:

Figure 51 – Device LED Control

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

Advanced settings

☰ [Advanced settings](#)

Device discovery:

Public status page:

Figure 52 – Device discovery

Device discovery – select to enable discovery function. Enable this feature to allow the ZCN-M5/M2 unit discovery within reach of a single multicast packet

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

Firmware Upgrade

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

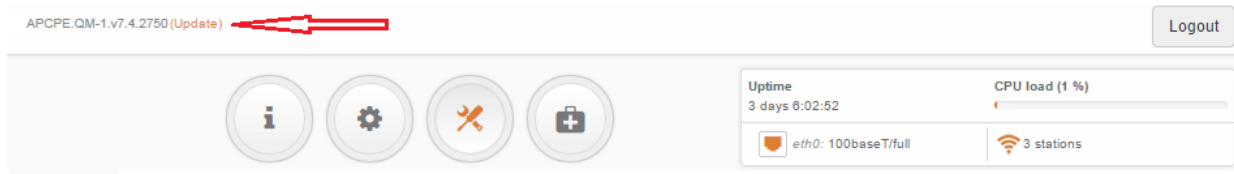


Figure 53 – Firmware Version



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:

FIRMWARE UPDATE

Select a File to Upload

APCPEQM-1.v7.4.2750.img

Figure 54 – 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 **Upload** button:

FIRMWARE UPDATE

Current firmware: APCPE.QM-1.v7.3.2426
 Uploaded firmware: APCPE.QM-1.v7.4.2750

Figure 55 –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


APCPE.QM-1.v7.50.7596 (Update) Logout

Uptime
3 days 6:23:26

 eth0: 100baseT/full

CPU load (2 %)

 3 stations



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**:

SITE SURVEY

Note: starting site survey scan may temporary disable wireless link(s).

Start scan

Enter keyword to filter results

MAC address	SSID	Security	Signal, dBm	Noise, dBm	Protocol	Channel
00:19:3B:87:65:46	Noname	WPA2 Personal	-90	-95	--	28 (5140 MHz)
00:15:6D:4C:37:1F	Energija5	WPA/WPA2 Enterprise	-81	-95	802.11a/n	60 (5300 MHz)
DC:9F:DB:6E:8A:F3	U-SK2	WPA2 Personal	-89	-95	802.11a/n	32 (5160 MHz)
24:A4:3C:7E:D2:F1	fstnsm5ver 1	Open	-79	-95	802.11a/n	6 (5030 MHz)
DC:9F:DB:8C:19:B1	FLANK3	Open	-90	-95	802.11a/n	8 (5040 MHz)
00:27:22:2A:AD:96	fstrm5base	Open	-91	-95	802.11a/n	12 (5060 MHz)

Last updated: 1/30/2015, 3:44:22 PM

Figure 56 – Site Survey Results



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.

ANTENNA ALIGNMENT

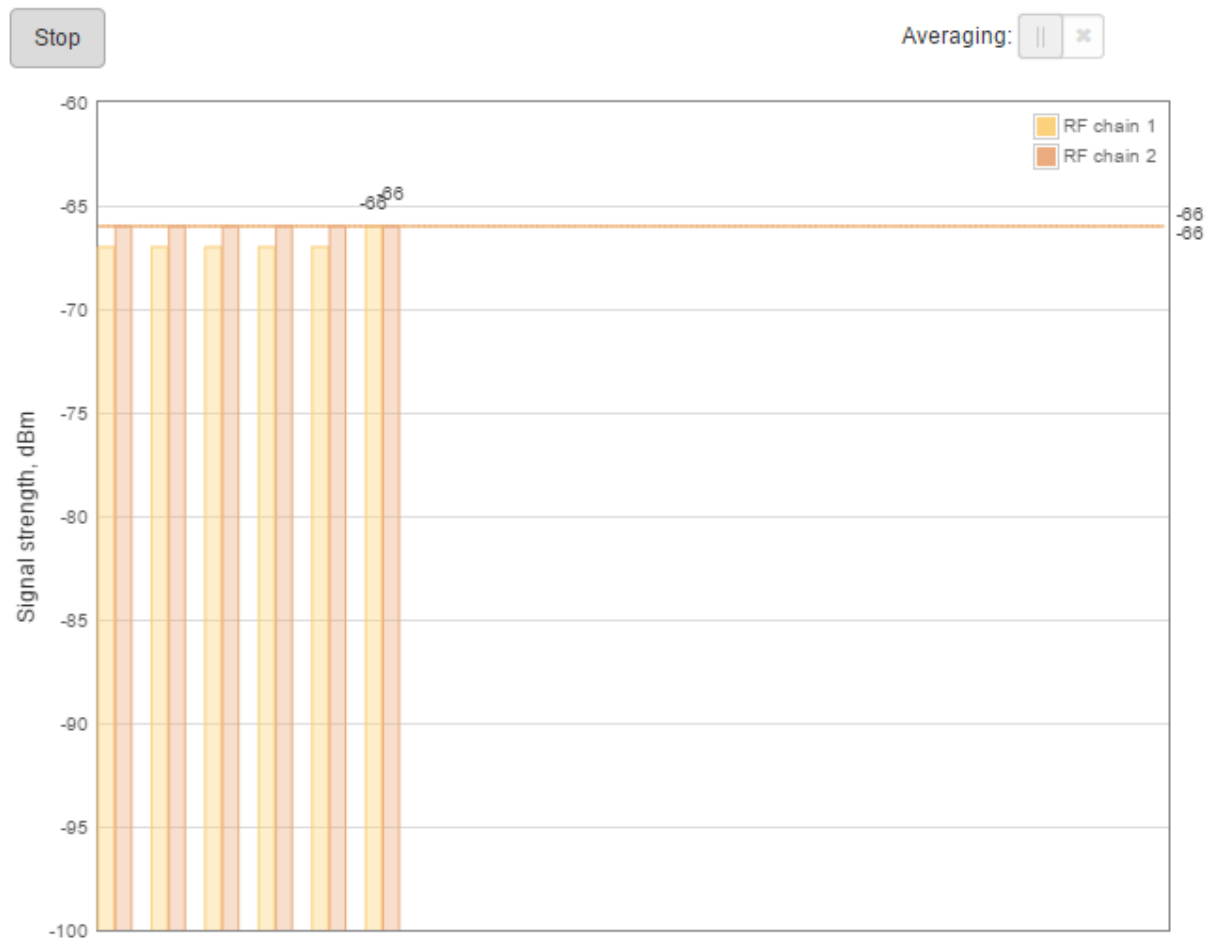


Figure 57 – Antenna Alignment

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 **iPoll 2** link. This tool tests the throughput at selected packet sizes and iterations.

LINK TEST

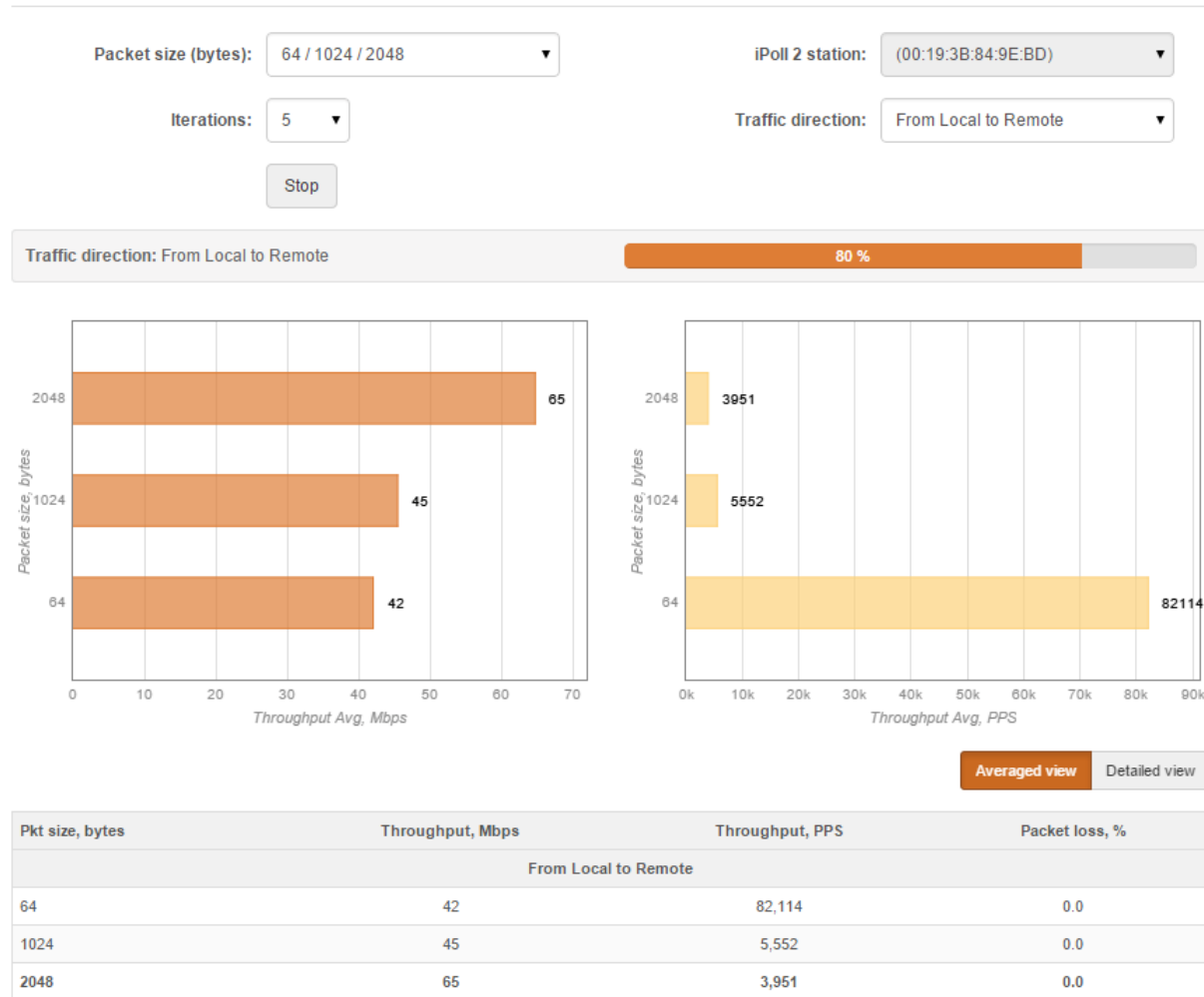


Figure 58 – Linktest Results

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

Iterations - select number of test iterations.

iPoll 2 Access Point – displays the Access Point information (iPoll 2 station side).

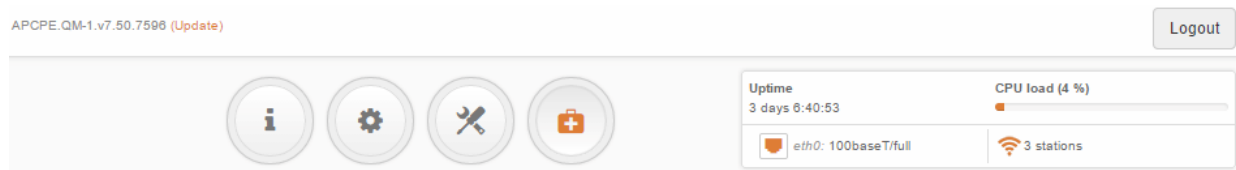
iPoll 2 station – select the Station the Link Test will be performed with (iPoll 2 Access Point side).

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

Start – click to start the throughput test.

Stop – click to stop the throughput test.

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.

TROUBLESHOOTING



Figure 59 – 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.

SYSTEM LOG

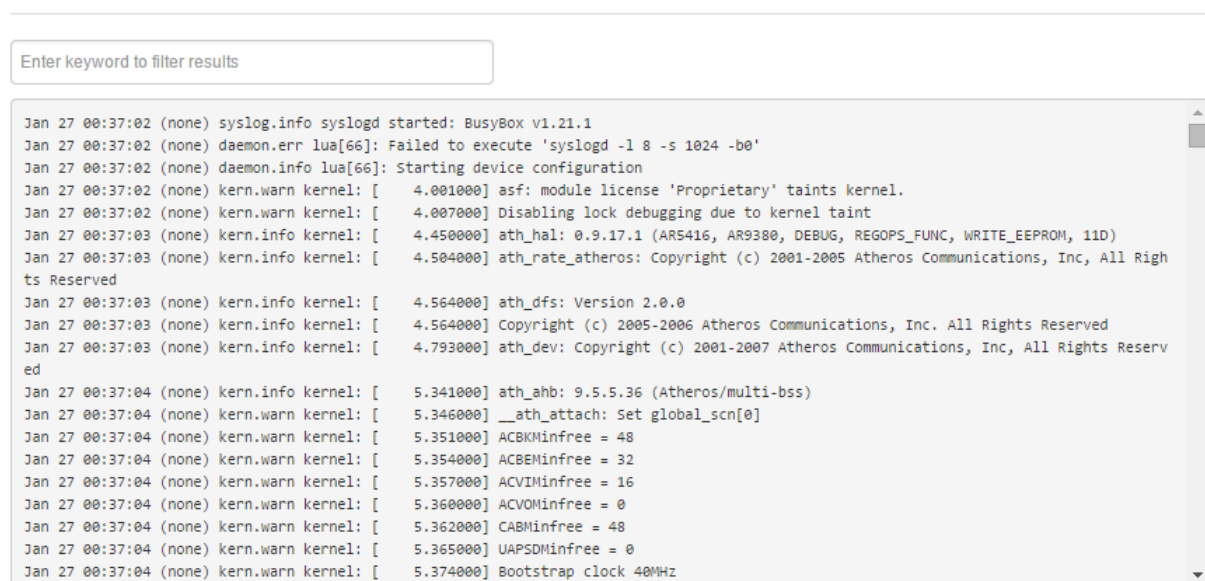



Figure 60 – Device System Log

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

Index

8

802.11, 25, 29, 32, 34, 35
802.11a, 24, 26
802.11a/n, 24, 25
802.11n, 24, 25, 32, 35

A

abbreviations, 6
Access Point (auto WDS), 24
ACK, 6, 26, 35
ACL, 6, 40
AES, 6
aggregation, 26, 32, 35
AMSDU, 6, 26, 32, 35
antenna alignment, 49
ARPNAT, 14, 23, 34
ATPC, 6, 25, 29
autochannel, 24, 28

B

black list, 40

C

CCQ, 6
client isolation, 27, 30
configuration backup, 46
configuration file, 46
country, 31, 34
CPU load, 11

D

default login, 46
device discovery, 47
DFS, 25, 29
DHCP, 6, 15
 client, 19
DHCP server, 17, 19, 20
DHCPv6, 20, 22
DNS, 19, 20
dynamic IP, 18
dynamic stateful, 17, 21
dynamic stateless, 17, 20

E

EAP, 6
ethernet, 11, 27, 31

F

firmware upgrade, 48
fragmentation threshold, 26, 32, 35

G

gateway, 19, 21
GMT, 6, 42
graphs, 13

I

IEEE, 6, 24
IGMP, 6
IP, 7
IP method, 16
IP settings
 dynamic IP, 18
 static IP, 18
iPoll 2, 12, 23, 28, 31, 37, 50
IPv4, 15
IPv4 settings
 dynamic IP, 16
 static IP, 16
IPv6, 15, 16, 20
IPv6 settings
 dynamic IP, 16
 static IP, 16
ISP, 7, 19

L

LAN, 7, 15, 17, 20
latitude, 45
lease time, 20, 22
LED, 7, 47
longitude, 45

M

MAC, 7
MCS, 7, 35
MCS index, 25
MIMO, 7
MSCHAPv2, 7
MTU, 19, 22

N

NAT, 7, 18
NTP, 7, 42

P

PC, 7
PDA, 7
PEAP, 7
PPPoE, 18, 19, 21
PSK, 7

Q

QoS, 7

R

radio, 12, 32
RADIUS, 7, 39, 40
reboot device, 46
router IPv4, 17
router IPv6, 20
RSSI, 7
RTS threshold, 26
RX errors, 13

S

scan SSID, 49
SISO, 7
site survey, 49
SMTP, 7
SNMP, 7, 44
SSH, 7, 43
SSID, 7, 26, 27, 30, 33, 36
static IP, 18
station, 12
syslog, 52

T

tagging, 27, 30, 33, 37
TCP, 7

threshold, 27, 31, 32, 35
timezone, 42, 43
TKIP, 7
troubleshooting, 52
TTLS, 7
TX errors, 13

U

UAM, 7
UDP, 7
uptime, 11, 14
UTC, 43

V

VLAN, 7, 16
VLAN tagging, 16
VoIP, 7

W

WACL, 7, 26, 27
WAN, 15, 17, 18
WDS, 7, 23, 31
WEP, 7, 37, 38
white list, 40
WISPr, 7
WLAN, 8
WNMS, 44
WPA, 8, 37, 38
WPA2, 8, 37, 38