Televes®

wave DATA

Refs. 769001, 769002

Art. Nr. WAVEDATAP, WAVEDATAS

WaveData AP MyNETWiFi

User Guide

Televes

Table of Contents

Important Safety Instructions

Before handling or connecting the equipment, please read this manual!

Safe installation

- Read these instructions before handling or connecting the equipment. Keep these instructions. Heed all warnings. Follow all instructions.
- Clean only with dry cloth.
- Do not use this apparatus near water. Apparatus shall not be exposed to dripping or splashing and no objects filled with liquids, such as glasses, shall be placed on the apparatus.
- Do not block any ventilation openings. Install in accordance with the manufacturer's instructions. Please allow air circulation around the equipment.
- Do not place the equipment in a highly humid environment.
- Do not install near any heat sources such as radiators, heat registers, stoves, or other apparatus (including amplifiers) that produce heat. Do not place naked flames, such as lighted candles on or near the product.
- Do not place the equipment in a place where it can suffer vibrations or shocks.
- Only use attachments/accessories specified by the manufacturer.

Safe operation of equipment connected to the mains supply

- Ambient temperature should not be higher than 45ºC.
- Power requirements for this product are: 220-230V~ 50/60Hz.
- It is strongly recommended not to connect the equipment to the mains supply until all connections have been done.
- The socket outlet shall be installed near the equipment and shall be easily accessible.
- To disconnect the equipment from the mains supply pull the plug never the cable.
- Protect the power cord from being walked on or pinched particularly at plugs, convenience receptacles, and the point where they exit from the apparatus.
- Unplug this apparatus during lightning storms or when unused for long periods of time.
- Refer all servicing to qualified service personnel. Servicing is required when the apparatus has been damaged in any way, such as power-supply cord or plug is damaged, liquid has been spilled or objects have fallen into the apparatus, the apparatus has been exposed to rain or moisture, does not operate normally, or has been dropped.

Warning

- Reduce the risk of fire or electric shock, do not expose this apparatus to rain or moisture.

This symbol indicates that equipment meets the safety requirements for Class II equipment.

This symbol indicates that equipment meets the CE marking requirements.

This symbol indicates that the equipment meets the safety requirements for Class II equipment.

This symbol indicates that this product can not be treated as conventional household waste. Make sure product is disposed of correctly.

Introduction

Ref. 769001 **WaveData** AP is a next generation of Wireless Access Points with latest 2.4GHZ IEEE 802.11/b/g/n and 5GHz IEEE 802.11/n/ac Wave2 technologies.

WaveData highlights

IEEE 802.11ac is the next evolution of the Wi-Fi standard. It can reach maximum throughputs well above a Gigabit per second. The 802.11ac specification mandates operation in the 5 GHz band, where there is relatively less interference and more channels are available compared to the 2.4 GHz band. 802.11ac achieves higher performance than 802.11n by using more spatial streams, wider bandwidth, higher order modulation, and improved bandwidth management techniques.

WaveData IEEE 802.11ac 5GHz Ratio introduces 80 MHz channel bandwidth in addition to the 20 MHz and 40 MHz specified in 802.11n. 80 MHz channels is formed by combining two adjacent, non-overlapping 40 MHz channels.

Multi-user MIMO (MU-MIMO): is an advanced feature defined in the 802.11ac standard that allows simultaneous multiple transmissions from the access point (AP) to up to four client stations (STAs). MU-MIMO mode increases client performance even with fewer antennas.

Wireless features

- 2.4GHz IEEE 802.11/b/g/n 2 Streams MIMO (2x2).
- 5GHz IEEE 802.11/n/ac Wave2 with 2 Streams MIMO (2x2)
- Up to 16 SSIDs and 124 stations per SSID.
- OFDM BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM modulations and 20/40/80MHz bandwidth channels to reach up to 1.73 Gbps. 2x2 On-Board 5 GHz radio, up to 867 Mbps and 2x2 On-Board 2.4 GHz radio, up to 300 Mbps.
- 4x Dual Band Antenna with +4dBi of antenna gain. 2.4 GHz TX Power: 23.5dBm@MCS0 HT20 and 16.5dBm@MCS9 HT40. 5 GHz TX Power: 22dBm@ MCS0 HT20 and 14.5dBm@MCS9 HT40.
- **Wi-Fi Security Modes** Open, WEP, WPA-PSK and WPA-EAP (aka WPA Enterprise) and support of WPA-TKIP and WPA-AES ciphers to secure Wi-Fi connections.
- AP Client isolation: To isolate SSID AP clients and avoid STA to STA communication.
- **Multi-user MIMO (MU-MIMO)**: is an advanced feature defined in the 802.11ac standard that allows simultaneous multiple transmissions from the access point (AP) to up to four client stations (STAs).
- **Load Band Steering**: support simultaneous dual band (2.4 GHz and 5 GHz) with ability to actively guide customers to the best available bandwidth.
- **QoS**: WMM and 802.11e for Voice, video and other time-sensitive protocols over Wi-Fi.
- **Wi-Fi Roaming**: fast authentication of mobile clients to the best available AP using the IEEE 802.11k standards for Radio Resource Management (RRM) and IEEE 802.11r Fast BSS transition (FT-BSS).

Network Features

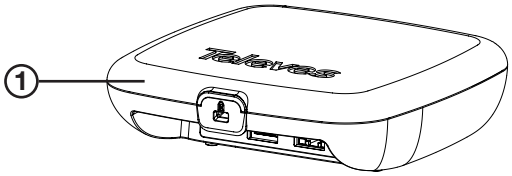
- Device can operates on Bridging or Routing Modes.
- Full IEEE 802.1Q VLAN support over all interfaces: Ethernet and Wi-Fi.
- Support network protocols: DCHP, PPPoE, L2TP, to allow a easy integration with provider network.
- Support for Multicast traffic and IGMP or MLD Snooping.
- Built in with Firewall to protect and secure device.
- **Open-VPN** to create secure connections with external networks.
- **IEEE 802.1X** port-based authentication with external Radius Server. Allows authentication of connected devices, establishing a point-to-point connection or preventing access by that port if authentication fails.
- Possibility of powering the device through a PoE IEEE802.3af switch or an external 12Vdc power supply.

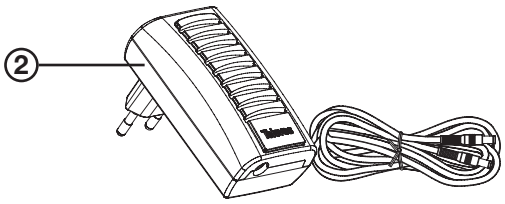
EN

System Requirements

- The system is an already Plug And Play device and no requires no software or driver.
- To configure device requires PC with an Ethernet or Wi-Fi interface via web interface. Latest versions of Firefox or Google Chrome are strongly recommended.

WaveData Package content





1	WaveData
2	12 Vdc power supply (769002 only)

Security Considerations

Please note that SSH and Web access to the WaveData are accessible on both LAN and WAN interfaces.

- SSH/Web Access Account root/76Wave90Data01 is public, as this manual. Changing this password should be done prior to any further configuration.
- The firewall has been enabled on WAN, named WAN Zone: only DHCP requests, UPNP, SSH and Web are opened to external access.
- The firewall has been enabled on LAN, named LAN Zone: All access requests from LAN are allowed. NAT is enabled to allow forwarding packets to WAN network.

On some installations consider change firewall rules to restrict access to device from LAN (on hotels or public domain networks where user connection to device is undesired) or WAN (if device obtain a public IP address and WAN is exposed to external hacks).

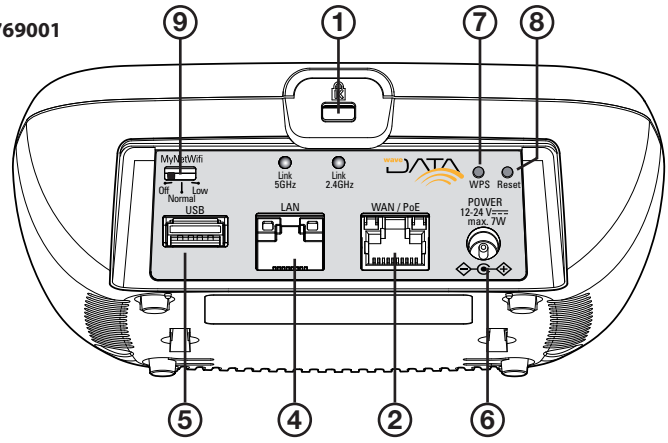
Operating Considerations

Consider the following operating notes about WaveData:

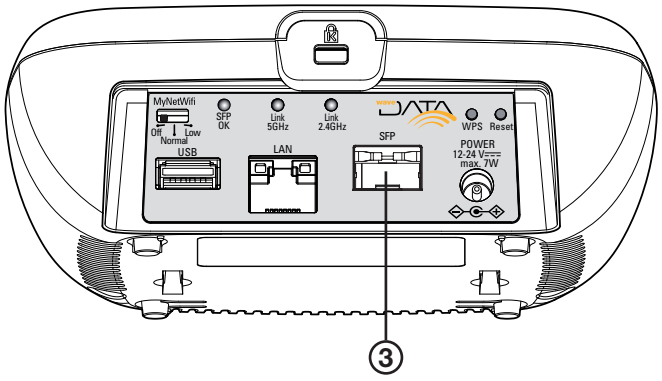
- Do not cover device, place device on right place to avoid thermal issues; thermal dissipation slots on external plastic chassis should be ventilated and air flow through device.
- Place device on a clear location in order to guarantee Wi-Fi coverage. Device must be placed on location where Wi-Fi coverage as longer as possible. Mount device on building wall as possible.

WaveData Device

769001



769002



Port Connections

① Kensington Security Slot

There is a slot for a Kensington lock on Wavedata back side to prevent to be stolen.

② 1xEthernet RJ-45 WAN (PoE) - (only ref. 769002)

Supports passive PoE 24V and IEEE 802.3af/at PoE connector up to 24Watts (max). Also provide Ethernet 100BASE-TX/1000BASE-T connector with auto-negotiation and Auto-MDIX.

③ 1xSFP 1000BASE-X

SFP 1000BASE-X connector (small form-factor pluggable transceptor). For optic fibre connection.

④ 1xEthernet RJ-45 LAN

Ethernet 1000BASE-T with Auto-MDIX. Provides Wired access to local network.

⑤ USB Connector

USB 3.0 Connector to plug device storage capacity or Mobile USB Modems (GPRS, 3G, etc...) to access mobile networks.

⑥ Jack Power 12-24Vdc

Jack Power is an PoE alternative connector to supply device power with 12-24 Vdc. Max current is 12V/2A.

Device Buttons

⑦ WPS Button

This button have a double function

- **WPS session**: press button to initiate a WPS session to authorize devices. Push WPS on Wi-Fi STATION, too in order to complete a WPS session. WPS session is active for a maximum of 120 seconds before become inactive.
- **Factory defaults**: press button for at least 3 seconds to restore factory default settings. This erase all device configuration and set device to factory state.

⑧ Reset Button

Press button to hard reset device. As alternative, perform a soft reset and perform a Reboot operation via Web or SSH command. Soft Reset is a preferred method to reset device in a proper way and preserve settings of device.

⑨ MyNETWi-Fi Switch

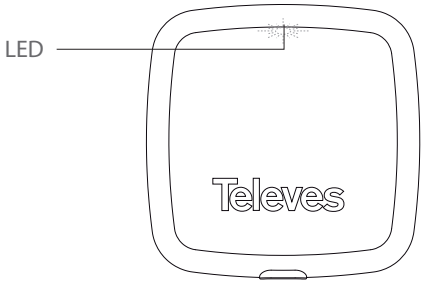
This tri-state switch allows power of Wi-Fi radios or reduce power on air.

MyNETWi-Fi Position	Switch Function
Off	Wi-Fi Off
Normal	Wi-Fi Power controlled by Software (max. 22dBm)
Low	MyNETWi-Fi Mode (max. 10dBm)

Device Leds

Frontal RGB Led

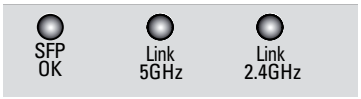
Device has a frontal RGB Led to indicate device status.



RBG Led Functions	
Device Activity	LED Pattern
System boot-up (kernel stage)	Blink Orange.
AP is Broadcasting SSIDs	Fixed Green.
myNETWi-Fi	Fixed Orange.
Wi-Fi Off/All Vaps Disabled	Fixed Blue.
System upgrade (firmware or configuration)	Blink Blue
Device Failure	Fixed or Blink Red.
System shut-down or power Off	All Leds Off

Device Indicator Leds

Device has several internal led indicators:



- **2.4GHz Link**: Blink indicates 2.4G Wi-Fi Radio is up and running. Fixed or Off 2.4G Radio is down.
- **5GHz Link**: Blink indicates 5G Wi-Fi Radio is up and running. Fixed or Off 5G Radio is down.
- **SFP OK** (only in ref. 769002): indicates what is known as "LOS LEDs (SFP)". That is, it indicates that the SFP is installed and that there is an optical link.

  LOS: *Loss Of Signal*. Signal loss led. Indicates if there is a problem with the fiber network.

  ACTIVE "LOS" LED (LED in RED), if the reception of the interface (RX) detects loss of signal (LOS). LED "LOS" will be OFF if it detects the presence of a signal (LINK).

EN

Installing WaveData

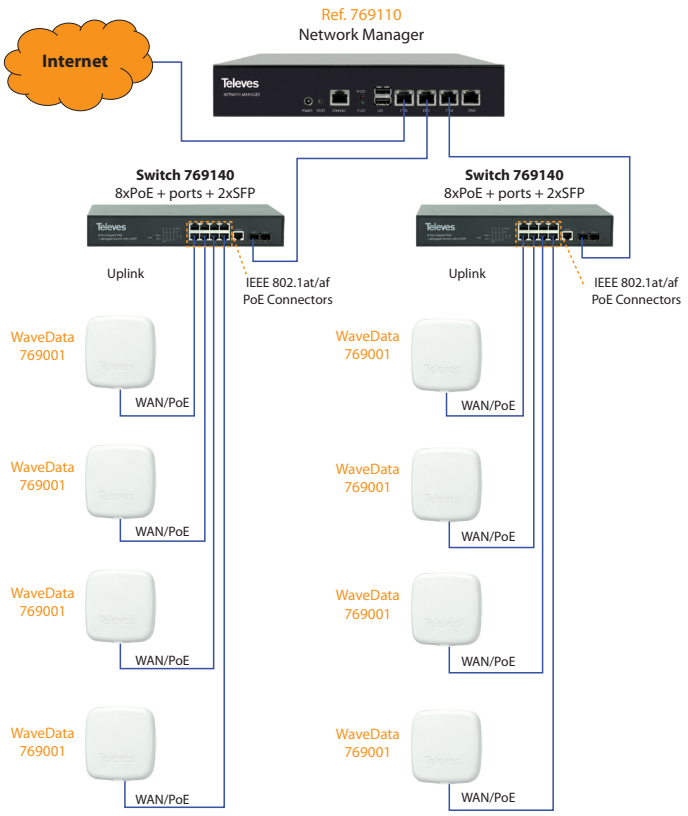
Installation example Ref.769001

The following figure shows reference installation of Ref.769001 WaveData PoE.

In the installation we use two PoE 769140 switches with 8 IEEE 802.3af/at PoE ports to power and connect with Ref. 769001.

Ethernet connector provides power and data simultaneously.

Ref.769110 Network Manager is used as an Internet Router.

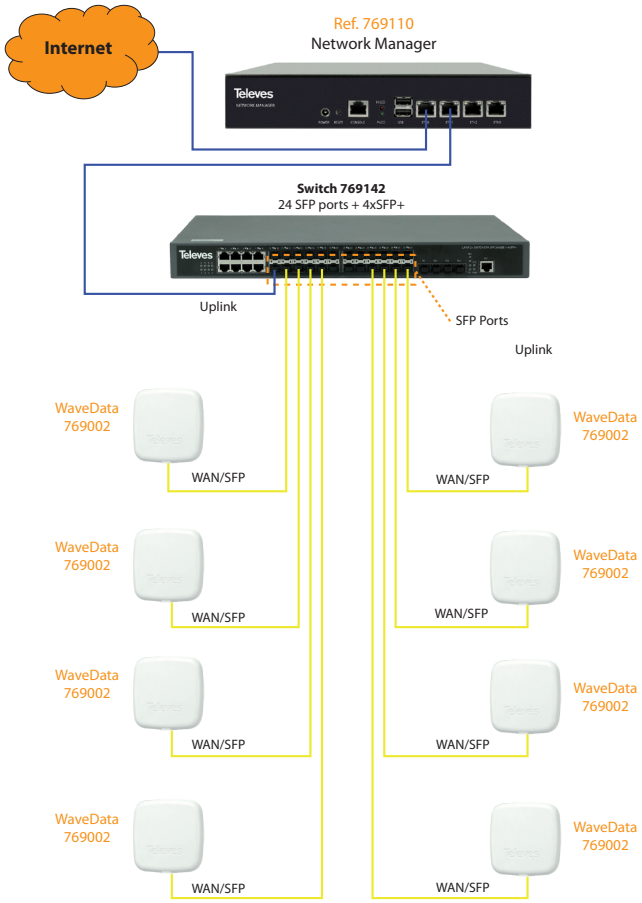


Installation example Ref.769002

In the installation shown, Switch 769142 with 24xSFP ports + 4xSFP+ is used to connect Ref. 769002 WaveData SFP.

Single-mode fiber optic links can be made with SFP's 769210 or 769212.

Televes Ref. 769110 Network Manager is used as Internet Router.



Connect to WaveData

To facilitate product installation, the device is configured in bridge mode and predefined with two interfaces.

- **LAN**: static IP 169.254.1.254. LAN interface includes all Ethernet ports and Wi-Fi interfaces.
- **LAN_DHCP**: LAN interface configured as a DHCP client.

In this way, we will have two IPs on the LAN interface:

- A fixed IP address 169.254.1.254: available for local connection to the device when there is no DHCP server in the installation.
- An IP address obtained by a DHCP client when the device is installed on a network where the Router assigns addresses to devices on the network with a DHCP server.

In order to access device user following credentials

- Default IP: LAN => 169.254.1.254, LAN_DHCP => DHCP client.
- username: **root**
- Password: **76Wave90Data01**

WaveData access via SSH

SSH Terminal can execute any command on the WaveData such as install new packages, remove/add/restart services or configuration. SSH service is running on port 22.

By default SSH operates on LAN and WAN interfaces and allowed on firewall configuration. Change firewall rules to block SSH traffic on desired interfaces.

Following example shows how to connect via SSH.

```
$ sshpass -p 76Wave90Data01 ssh root@192.168.1.1
BusyBox v1.25.1 (2018-06-25 18:51:51 CEST) built-in shell (ash)
     MM           NM                   MMMMMMM           M       M
    $MMMMM        MMMMM               MMMMMMMMMMM      MMM     MMM
   MMMMMMMM     MM MMMMM.             MMMMM:MMMMMM:    MMMM   MMMMM
MMMM= MMMMMM  MMM    MMMM       MMMMM   MMMM  MMMMMM   MMMM  MMMMM'
MMMM=  MMMMM MMMM     MM        MMMMM    MMMM    MMMM   MMMMNMMMMM
MMMM=    MMMM  MMMMM           MMMMM     MMMM    MMMM   MMMMMMMM
MMMM=    MMMM   MMMMMM        MMMMM      MMMM    MMMM   MMMMMMMM
MMMM=    MMMM     MMMMM,     NMMMMMMMM   MMMM    MMMM   MMMMMMMMM
MMMM=    MMMM       MMMMMM   MMMMMMMM    MMMM    MMMM   MMMM  MMMMMM
MMMM=    MMMM   MM    MMMM    MMMM      MMMM    MMMM   MMMM    MMMM
MMMM$ ,MMMMM  MMMMM  MMMM    MMM       MMMM    MMMM   MMMM    MMMM
  MMMMMMM:      MMMMMMM     M          MMMMMMMMMMM  MMMMMMM MMMMMMM
    MMMMMM       MMMMN     M           MMMMMMMMM      MMMM    MMMM
     MMMM          M                   MMMMMMM       M       M
       M
 ------------------------------------------------------------
   For those about to rock... (Chaos Calmer, r47828)
 ------------------------------------------------------------
root@OpenWrt:~#
```

WaveData access via Web

Device has a Web Service running on port 80. By default, Web service is accessible via LAN and WAN interfaces since web is allowed on all device firewall zones.

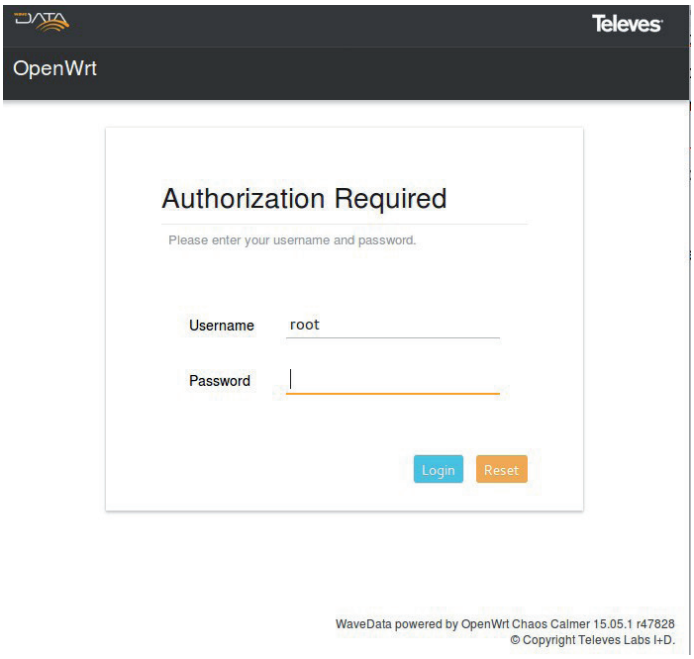
Web Main purpose is perform Network configuration and administration tasks.

Use the following account to login.

- username: **root**
- Password: **76Wave90Data01**

Web Login

Below is capture of Web Interface login. Input credentials.

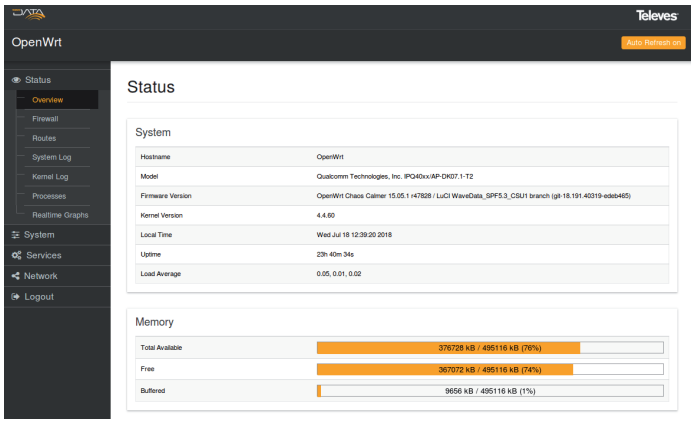


EN

Configure WaveData

Device Status

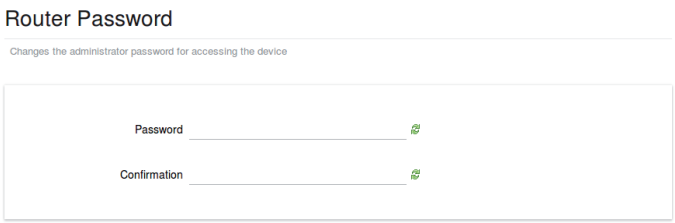
To view device state go to **Status>Overview**



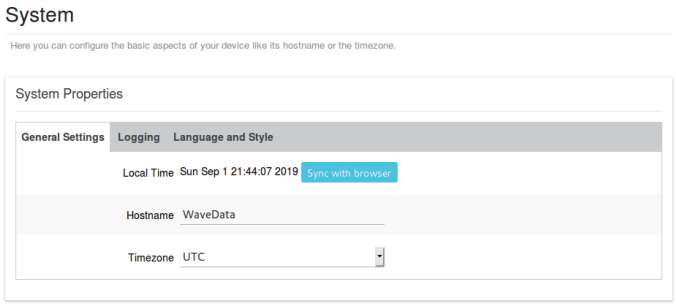
System Configuration

Change Password

Go to **System>Administration** to change password of admin account used on login.



System Hostname and TimeZone



- **Sync with browser**: Set current date of device to browser time.
- **Hostname**: Enter device hostname
- **Timezone**: Select device timezone. Default is UTC.

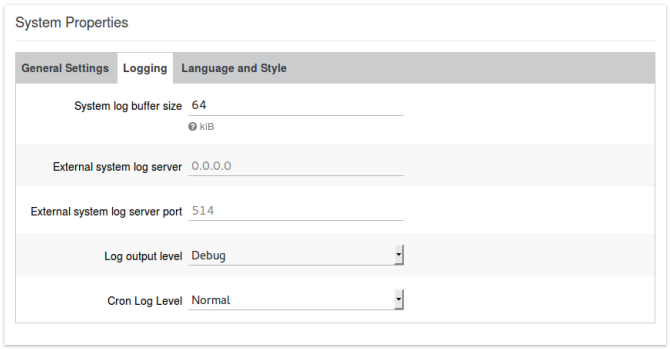
System Time

WaveData can sync time via NTP server.

- **Enable NTP Client**: Check to configure system time via NTP server candidates.
- **Provide NTP Server**: WaveData also provide NTP service with current system time.
- **NTP Server Candidates**: Input valid NTP servers to configure time.

System Logging

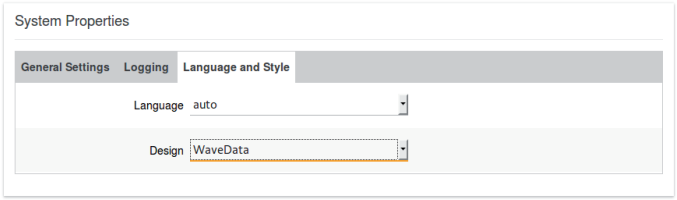
WaveData keeps an event log. By default the data is not stored in a file, it is stored in a circular buffer. As new entries are entered in the registry, the oldest ones are deleted. The following web configures the system registry.



- **System log buffer size**: Default buffer size of system log. By default 64kiB.
- **System Log server**: Enter valid IP Address of system log server. hostname is not supported. You can setup destination port. Default is 514.
- **Log output Level**: Change level of messages added to system log buffer.
- **Cron Log level**: Enter log level messages of cron server.

System Language and Style

Change Language and theme of Web front-end



- **Language**: Language of web GUI.
- **Design**: Change theme of web GUI.

Configure network interfaces

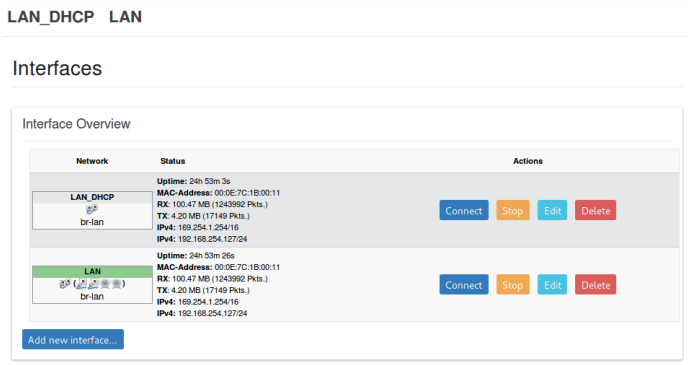
By default System predefined two interfaces:

- **LAN**: This is a bridge interface, called BR-LAN: as members it has all the physical interfaces of the system, that is, the 2.4G (ath0) and 5G (ath1) Wi-Fi VAP (Virtual access point) and the eth0 and ethernet interfaces eth1. It is statically assigned IP 169.254.1.254.
- **LAN_DHCP**: This interface adds a DHCP client to the LAN interface. The purpose of this interface is to allow the device to obtain an additional IP address via DHCP, at the expense of the IP address 169.254.1.254 assigned statically to LAN.

This default configuration allows the traffic received by the interfaces to be automatically propagated depending on where the destination host is located, minimizing the configuration needs and facilitating the propagation of traffic. If you need to enable Router mode on the device, see the section Configure Router Mode.

List interfaces

To list network interfaces go to **Network>Interfaces**



Interface options:

- **Delete Interface**: remove interface on device. Settings are cleared.
- **Connect/Stop Interface**: Power up or Shut-down interface. These buttons start/stop interfaces. When you stop an interface through which you connect to the device you lose connectivity with it.
- **Add New Interface**: Add a new interface on device.
- **Edit Interface**: Change interface settings.

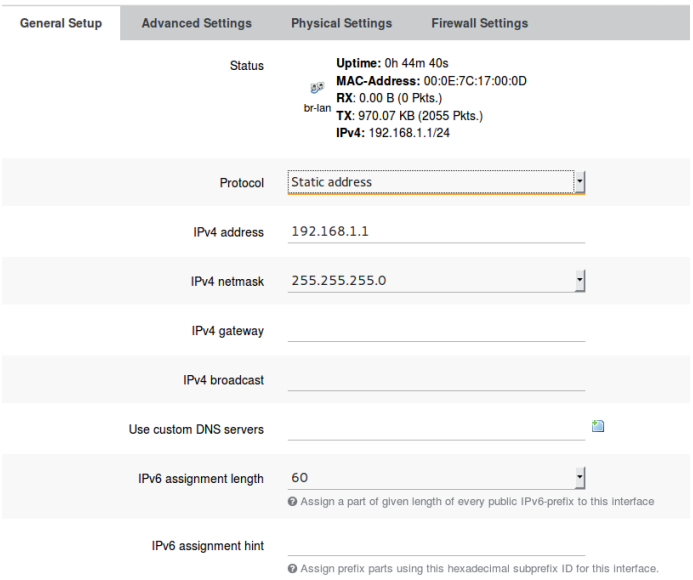
When changes are made to the configuration of several interfaces, it is advisable to save the changes in the configuration first, to subsequently apply them together in the system. This avoids unnecessary connection losses. e.g. when a physical interface such as eth0 is unassigned from the LAN interface to be assigned to another WAN.

To allow type of save and apply operations, global options are provided to manage changes in the configuration before apply:

- **Save&Apply**: Save and Apply all configuration changes made.
- **Save**: Save the changes made in the configuration, before apply to system. These changes can be undone with Reset button.
- **Reset**: Remove all previously saved changes.

Interface General Setup

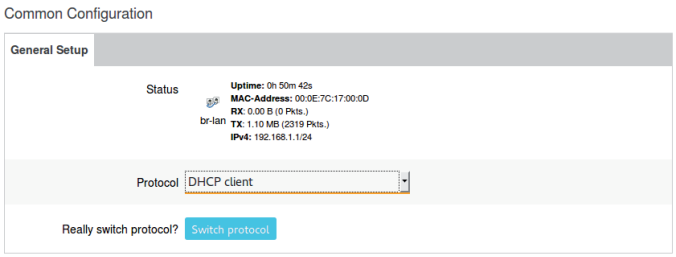
Go to *Edit Interface* > *General Setup* to configure interface settings and select interface protocol. Below screenshot shows configuration for static IP LAN interface.



- **Protocol**: Select interface protocol to setup. Valid values are DHCP, Static, PPPoE or L2TP. When change interface protocol is needed setup valid values for selected protocol.

  Add more software packages to expand supported protocols.

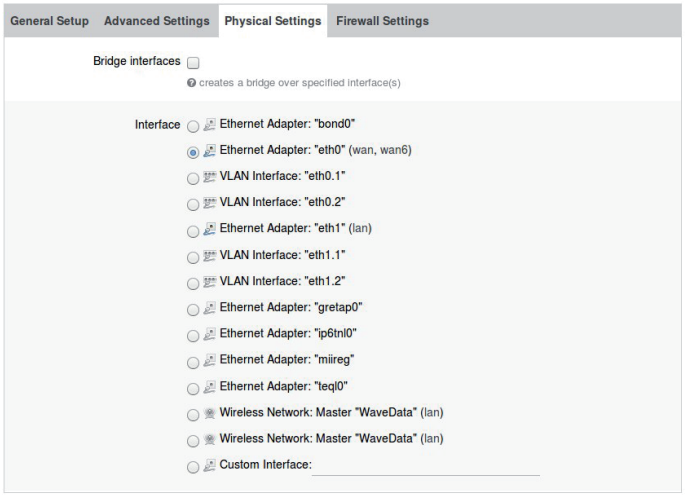
  Click on "Switch Protocol" Button to change interface protocol.



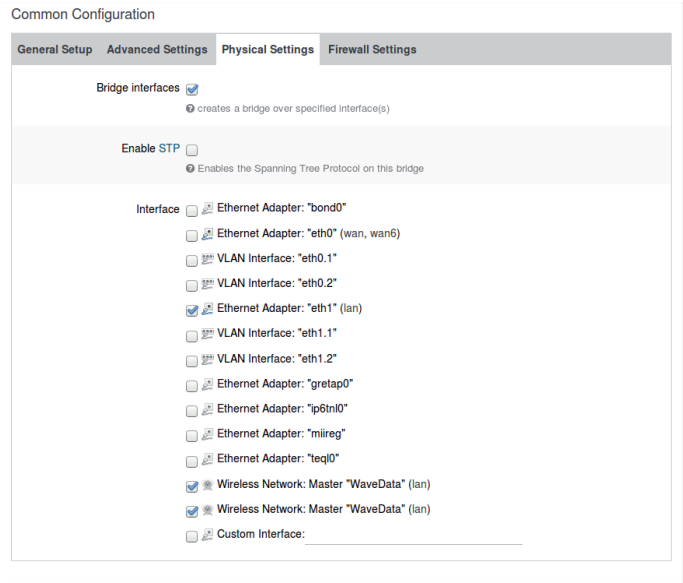
Interface: Physical Settings

Go to *Edit Interface* > *Physical Settings* to setup physical interfaces bounded to a network. There are two ways:

- **Single interface**: Interface is formed by only one physical interface. WAN is an example of single interface where WAN interfaces bind eth0 as single physical interface.



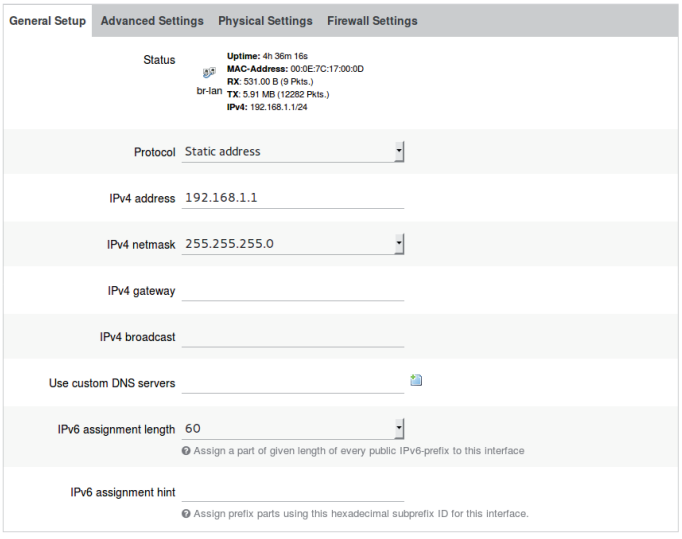
- **Bridged interface**: Interface is a bridge where physical interfaces are member. LAN is an example of bridge interface and creates a bridge, named BR-LAN, bind to two Wi-Fi radios (for 2.4GHz and 5GHz) and local eth1 LAN physical interface.



Interface: Select protocol

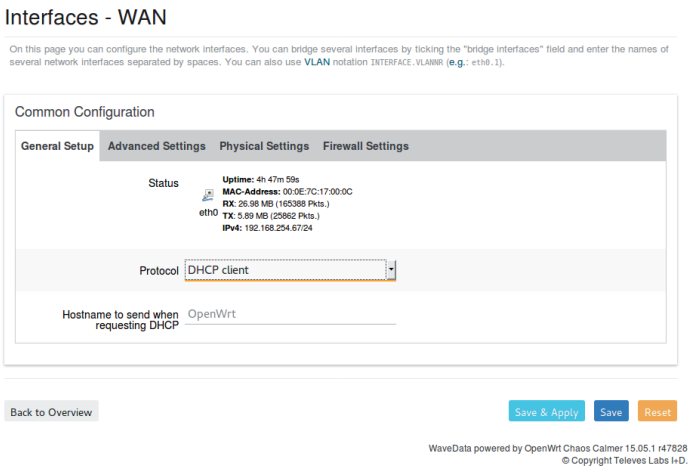
On *Edit Interface* > *General Setup* select interface protocol between: Static IP Address, DHCP client, PPPoE or L2TP. Every protocol has its own configuration page according to required parameters.

Static Address



- **IPv4 Address**: Fixed IP Address for interface.
- **IPv4 netmask**: Netmask of interface network.
- **IPv4 gateway**: Gateway for interface network.
- **IPv4 broadcast**: broadcast address for interface network.
- **DNS Servers**: DNS servers for interface network. Multiple options are available.

DHCP Client

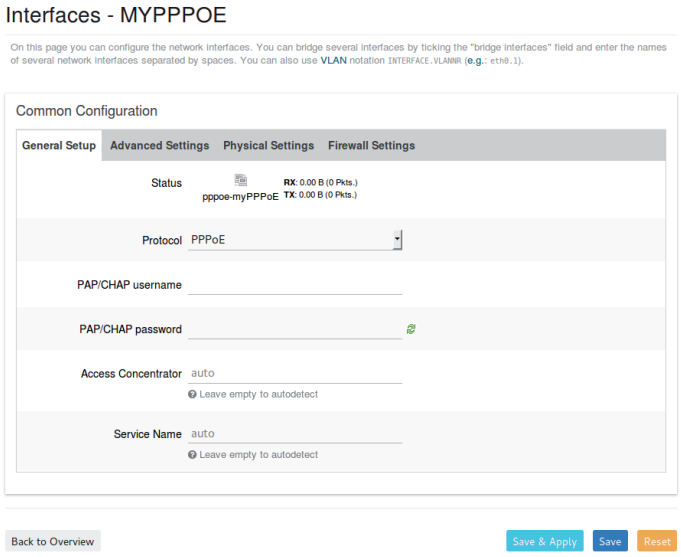


- **Hostname**: Use this field to set a custom hostname, other than default on system, when send DHCP requests.

PPPoE Client

Create a new PPPoE connection with a PPPoE server.

PPPoE (Point-to-Point Protocol over Ethernet) is a network protocol for PPP encapsulation over an Ethernet layer. It is a point-to-point Internet access protocol that allows WaveData to establish a connection with a server offering authentication, encryption, maintenance and compression. Check with your provider to see if they offer this service.



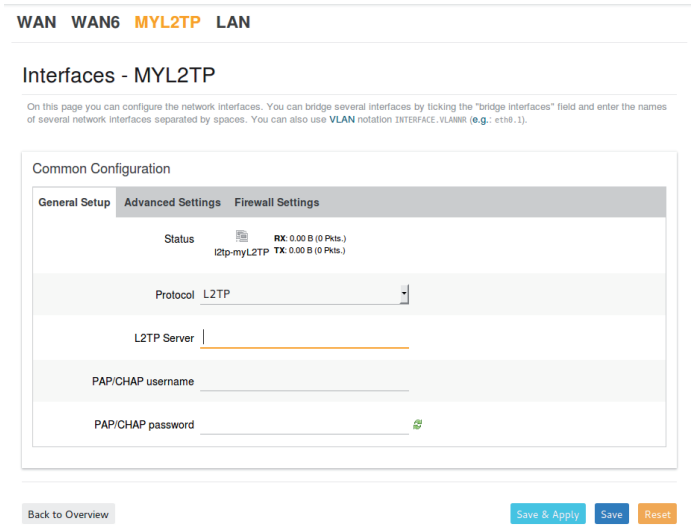
Please, use following PPP parameters to configuration tunnel:

- **PAP/CHAP username**: Username of PPP account.
- **PAP/CHAP password**: Password of PPP account.
- **Access Concentrator**: Specifies the Access Concentrator to connect to. If unset, pppd uses the first discovered one.
- **Service Name**: Must be the same than PPP Server configuration. If unset, pppd uses the first discovered one.

L2TP tunnel

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

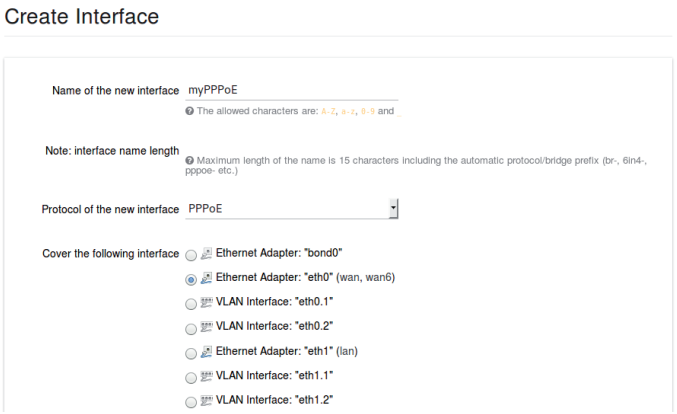
Published in 1999 as proposed standard RFC 2661, L2TP has its origins primarily in two older tunneling protocols for point-to-point communication: Cisco's Layer 2 Forwarding Protocol (L2F) and Microsoft's[2] Point-to-Point Tunneling Protocol (PPTP).



- **L2TP Server**: L2TP server to connect to. Acceptable datatypes are hostname or IP address.
- **PAP/CHAP username**: Username of PPP account.
- **PAP/CHAP password**: Username of PPP account.

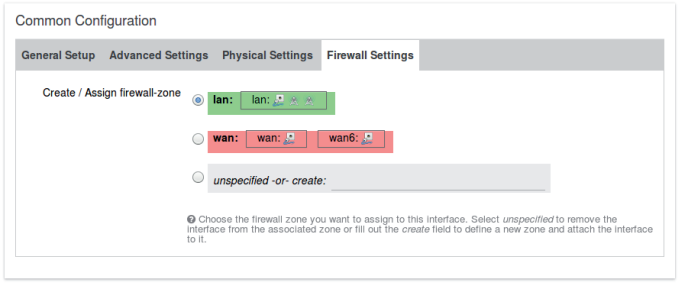
Add New Interface

Click on Add button to create a new interface. Yo can select protocol and physical interface to bound. Same physical interface can operate a lot of different protocols.



Interface: Firewall Settings

Go to *Edit Interface* **>** *Firewall Settings* to change firewall zone.

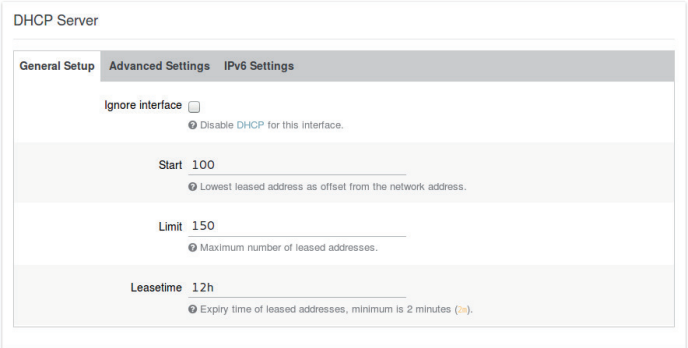


Interface can be configured to apply rules of a firewall zone. Firewall configuration is split on zones and every zone has own filter rules. Go to *Network* > *Firewall* to add or change rules of zones on Firewall.

Interface: DHCP Server

Go to *Edit Interface* > *DHCP server* to enable DHCP server on interface.

- **Ignore interface**: Check if you want DHCP server not provide IP Configuration on this interface.
- **Start**: First valid DHCP IP address as offset of network address.
- **Limit**: Max Number of DHCP Address.
- **Lease Time**: Expiry time of leased addresses. Put a number and a prefix (s for seconds, h for hours). Valid values are 120s or 24h.



Configure Router Mode

The device is preconfigured to operate as a bridge over all interfaces. To change the configuration mode, from Bridge mode to Router mode, it is necessary to create a new interface, called WAN:

- **WAN**: This interface will be assigned the eth0 physical interface and will use the external interface WAN/PoE (769001) or WAN/SFP (769002). By default it will be configured as a DHCP client.
- **WAN6**: This interface will be assigned the physical interface eth0 and will use the external interface WAN/PoE (769001) or WAN/SFP (769002). By default it will be configured as a DHCPv6 client.

In router mode the device will have local interface:

- **LAN**: this interface creates a bridge, called BR-LAN, and has as members all Wi-Fi VAP (Virtual access point) interfaces of 2,4G (ath0) and 5G (ath1) and the local ethernet interface (eth1). It will be configured with IP 192.168.1.1 and a DHCP server for local clients.
- **LAN_DHCP**: this interface will not be necessary and will be deleted.

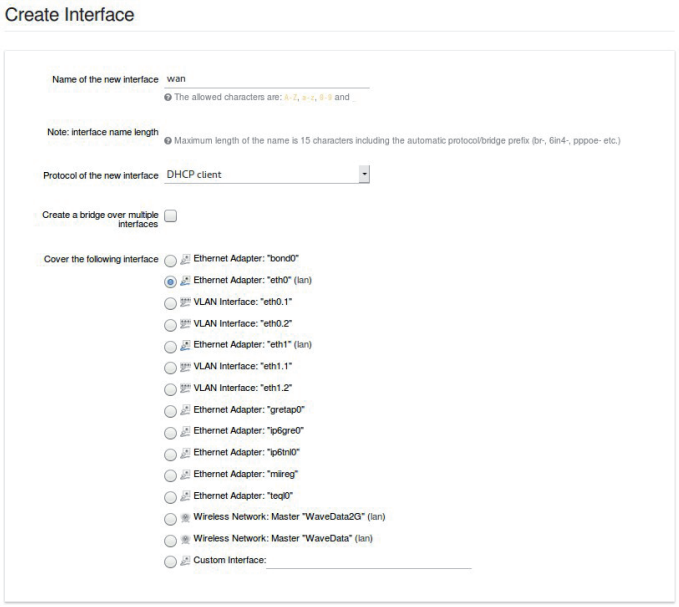
WAN interface enables device to operate in router mode. WAN is connected to the provider's network and will be configured via DHCP. LAN interface is a bridge with local ethernet interface (eth1) and Wi-Fi interfaces as members. LAN traffic will be routed to WAN using NAT (Network Address Translation).

Router Mode: Adding WAN interface

New WAN interface requirements:

- Create WAN interface with DHCP client protocol.
- Assign eth0 physical interface to WAN interface.
- Assign WAN zone of the firewall to WAN interface.
- Enable NAT masquerading in the WAN zone.

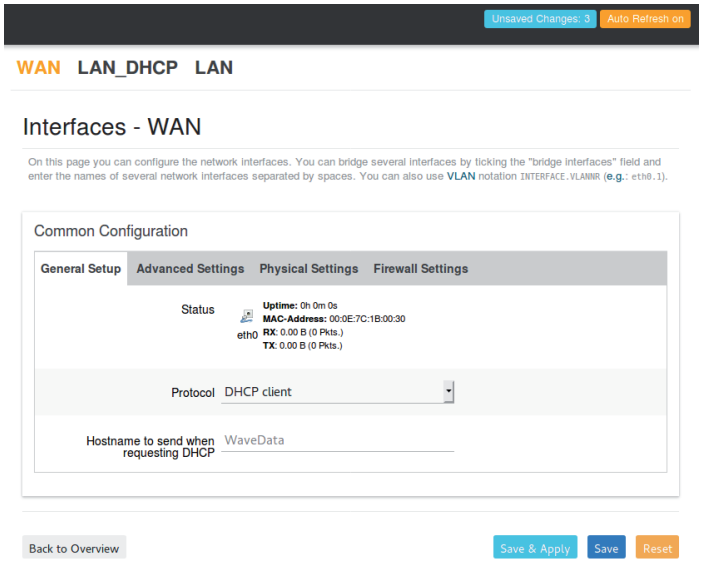
Go to *Interfaces> Add new Interface* to create a new interface, named wan.
Select DHCP client as the protocol of the interface and the physical interface eth0.
To finish the process click on *Submit*. This button will only make changes to configuration but will not apply them.



The changes made are indicated in the upper left: Unsaved Changes: 3

By changing the configuration but not applying it, it allows us to continue configuring the device until the configuration change is completed.

Otherwise, if we apply the modification of the configuration on the interface with which we connect to device, the change may lead to a connection lost.



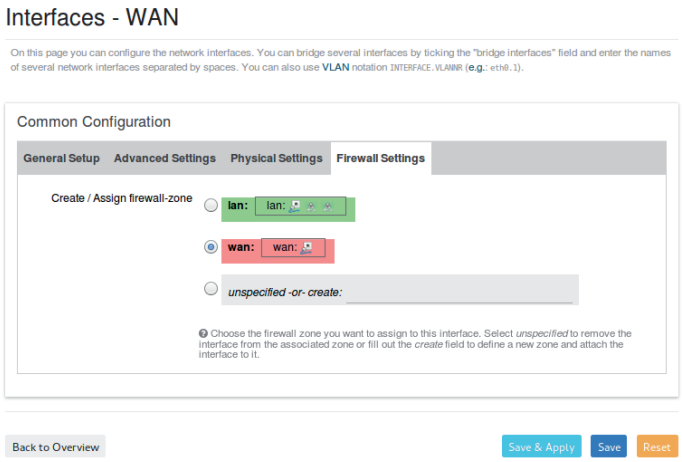
Router Mode: firewall WAN zone

If the WAN network on which the device operates is not secure, it is necessary to activate the firewall. By default Router comes with a predefined and configured firewall zone named WAN.

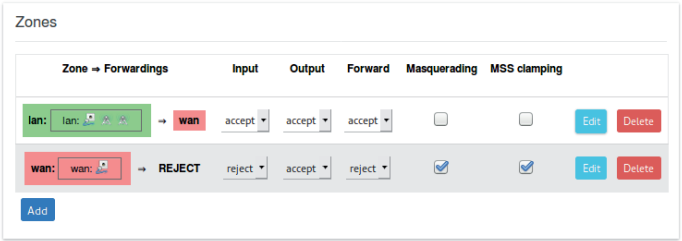
In Router mode, we also need to activate NAT masquerading for WAN outbound traffic.

To assign the WAN interface to this zone go to *Interfaces* > *WAN*> *Firewall Settings* and select *WAN zone* to be used by the interface.

Press *Save* to save the changes.



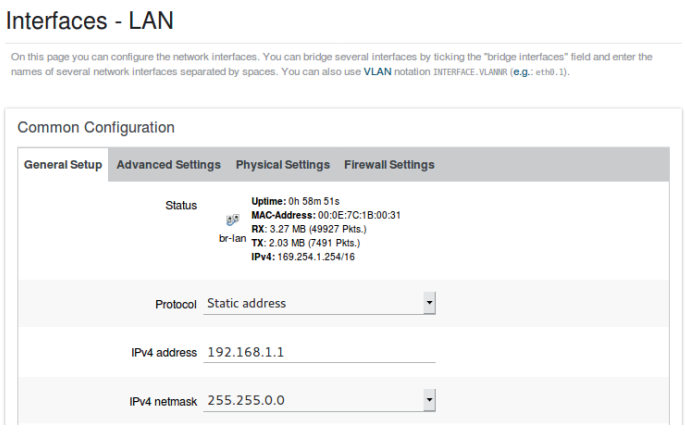
Go to *Firewall* > *Zones* and verify WAN zone has activated NAT masquerading.



Router Mode: LAN interface Configuration

Following steps show how to configure LAN interface in Router mode:

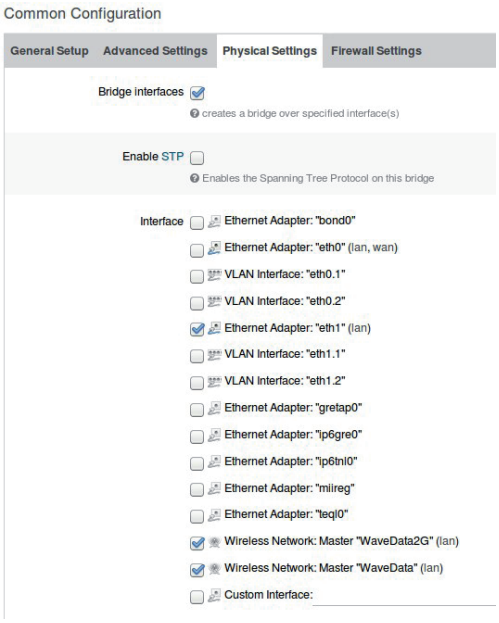
Go to *Interfaces* > *LAN* > *IPV4 Address* and configure IP Address 192.168.1.1.



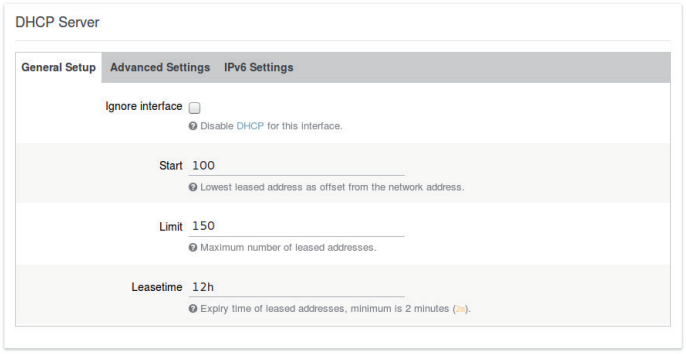
Unassign eth0 physical interface of LAN interface (it is assigned by default).

Go to *Interfaces* > *LAN* > *Physical Settings* and remove eth0 from the list.

EN

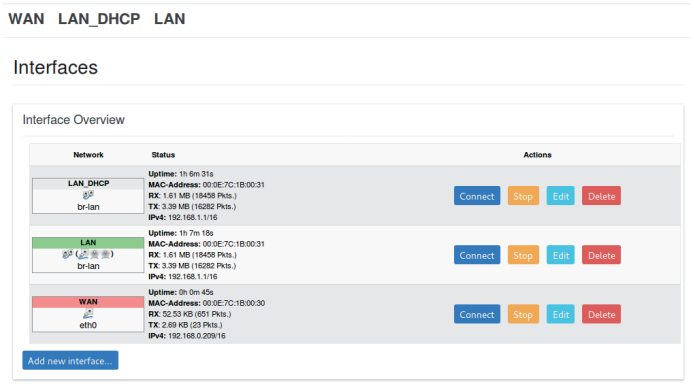


Go to *Interfaces* > *LAN* > *DHCP Server* and enable DHCP server on interface.

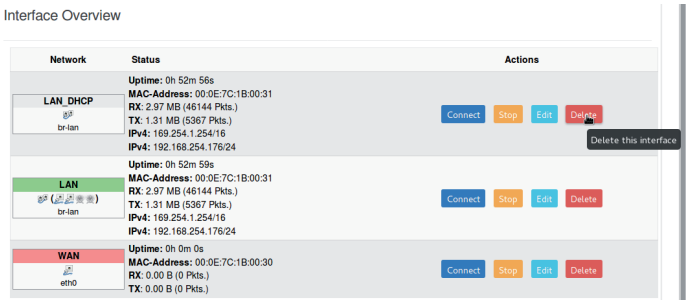


Finally, to apply changes made click on Save & Apply.

Capture shows list of interfaces, with new WAN interface on the list and with IP assigned by DHCP.

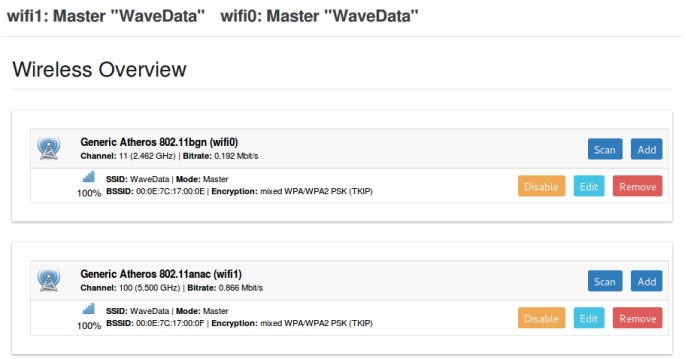


In router mode, LAN_DHCP interface is no longer necessary. Go to *Interfaces* and click on the *Delete* button to remove LAN_DHCP interface.



Configure Wi-Fi interfaces

Go to *System* > *Wi-Fi* to see Wi-Fi interfaces list.



Interface offers following buttons per interface

- **Scan**: Scan network for available AP.
- **Add**. Create a new VAP.

And following buttons per VAP (Virtual Access Point)

- **Disable/Enable** VAP.
- **Edit**: Configure VAP options.
- **Remove**: Remove VAP from Wi-Fi interface.

Associated Stations

Displays the list of connected clients with Wi-Fi interfaces.

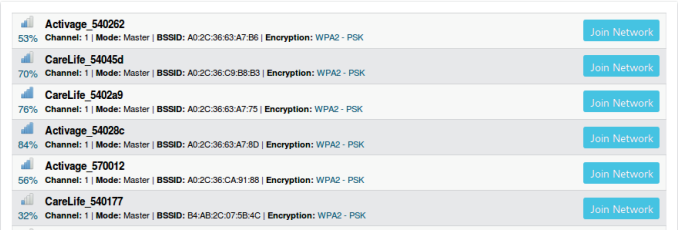
For each client, it shows the SSID with which it is connected, its MAC and the rates and signal levels of the Wi-Fi connection.

Scan for Wi-Fi networks

When scan for new Wi-Fi networks interface listen to get all AP beaconing on air.

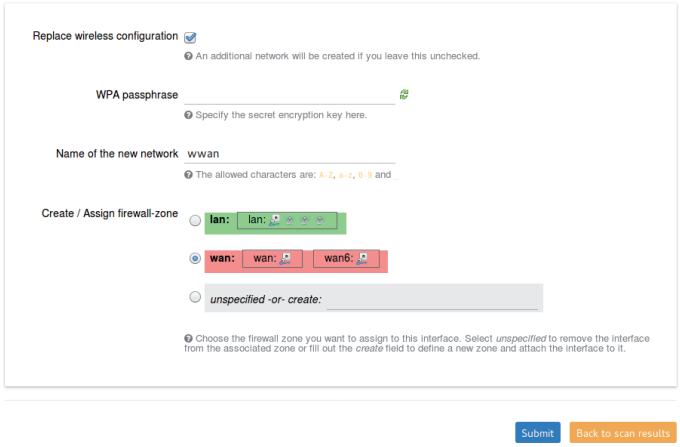
EN

Join Network: Wireless Scan



- **Join network**: Provides a GUI to connect to selected wireless network.

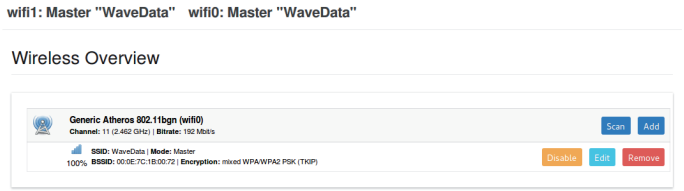
Join Network: Settings



When device creates a new VAP for join to a network, by default creates a new network named **WWAN**. WWAN network will be preconfigured as bridge interface, name BR-WWAN, with only one physical interface, the new STA VAP created to join to wireless network.

- **Replace wireless configuration**: When create new STA VAP, delete all VAPs on Wi-Fi interface and only create new STA VAP.
- **Create/Assign Firewall zone**: for wwan network created.

If you need create a new STA VAP without scan and join, use Add button to create new VAP with desired parameters: SSID, WPA key, etc...

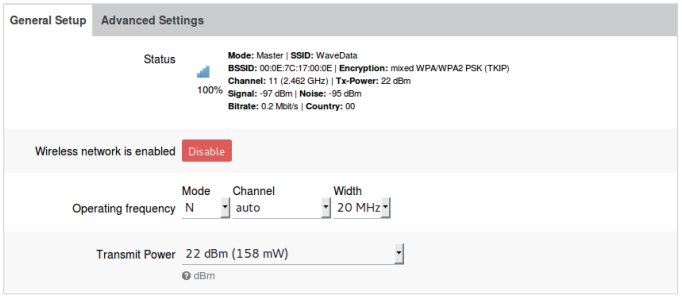


Edit Wi-Fi interface settings

Click on Edit button to setup a VAP interface.

Device Configuration section configures Device Radio and configuration affects to all vaps of Wi-Fi device.

Device Configuration

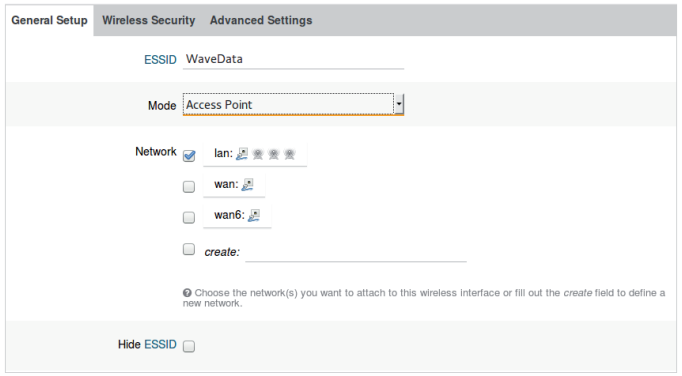


- **Mode**: Select mode 802.11/a/b/g/n/ac of
- **Channel**: Set channel of Wi-Fi device. Auto let driver to choose best channel.
- **Width**: Bandwith of Wi-Fi channel 20/40/80 MHz.
- **Power**: Transmit power of Wi-Fi channel.

Interface Configuration section configure VAP parameters between three tabs.

VAP General Setup

Interface Configuration



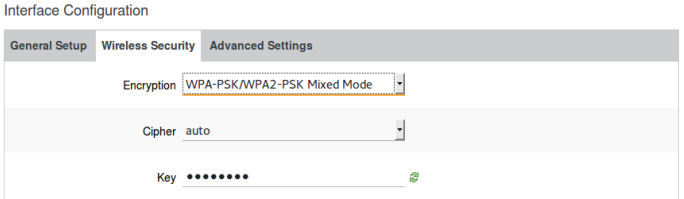
- **ESSID**: The broadcasted SSID of the wireless network (for managed mode the SSID of the network you're connecting to)
- **Network**: choose network Wi-Fi VAP belong to or create a new network.

VAP Modes

- **Access Point**: VAP mode is AP. Wi-Fi device broadcast SSID and wait for station connections.
- **Access Point (WDS)**: VAP mode is AP with WDS enabled. WDS enable Ethernet over Wi-Fi, if VAP is member of a bridge network and need propagate VAP traffic over LAN ethernet interface, choose this option.
- **Client**: VAP mode is STA and try to connect with best AP with same ESSID.
- **Client (WDS)**: VAP mode is STA and try to connect with best AP with same ESSID. WDS enable Ethernet over Wi-Fi, if VAP is member of a bridge network and need propagate VAP traffic over LAN ethernet interface, choose this option.

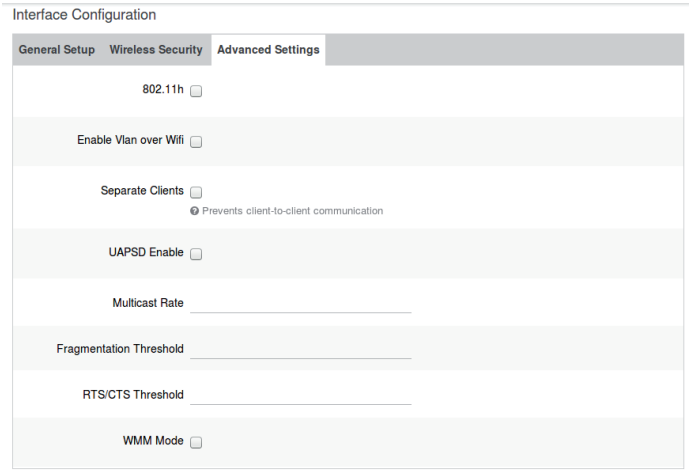
VAP Wireless Security

Interface Configuration



- **Encryption**: Open, WEP, WPA/WPA2-PSK or WPA-EAP (802.1X)
- **Cipher**: WPA-TKIP, WPA-AES or Auto for both.
- **Key**: for WEP or WPA. WEP keys must be 6 or 13 ASCII length.

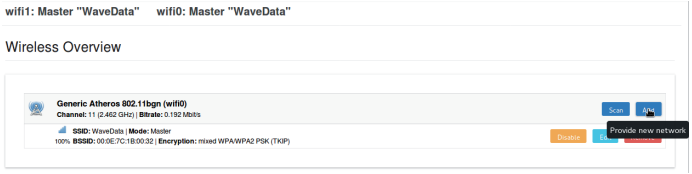
VAP Advanced Settings



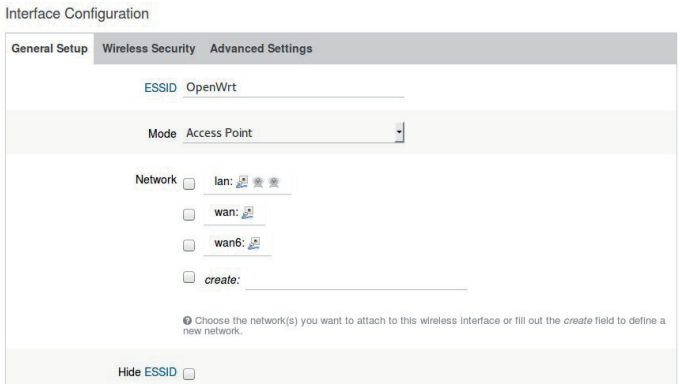
- **802.1h**: Enable IEEE 802.1h amendment added to the IEEE 802.11 standard for Spectrum and Transmit Power Management Extensions. It solves problems like interference with satellites and radar using the same 5 GHz frequency band. It was originally designed to address European regulations but is now applicable in many other countries. The standard provides Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) to the 802.11a PHY. It has been integrated into the full IEEE 802.11-2007 standard.
- **Enable VLAN over Wi-Fi**: Enable support for transmit VLAN tag over Wi-Fi. STA connected to AP must have support for VLAN too in order preserve tag to VLAN interface on STA host.
- **Separate Clients**: Avoid client to client communication on AP.
- **UAPSD**: based on the IEEE 802.11e standard new power save delivery and notification mechanisms have been introduced. APSD (automatic power save delivery) provides two ways to start delivery: 'scheduled APSD' (S-APSD) and 'unscheduled APSD' (U-APSD). With APSD, multiple frames may be transmitted together by the access point to a power-saving device during a service period.
- **WMM Mode**: Enable WMM (Wi-Fi Multimedia) based on the IEEE 802.11e standard. It provides basic Quality of service (QoS) features to IEEE 802.11 networks. WMM prioritizes traffic according to four Access Categories (AC): voice (AC_VO), video (AC_VI), best effort (AC_BE), and background (AC_BK). However, it does not provide guaranteed throughput. It is suitable for well-defined applications that require QoS, such as Voice over IP (VoIP) on Wi-Fi phones (VoWLAN).

Add new VAP interfaces

Click on *Add* Button to add a new VAP to a Wi-Fi Interface.



Web offers same GUI than Edit a connection but with predefined values. Setup new VAP as you need.



Configure Switch VLAN Interfaces

Go to *Network* > *Switch* to setup VLAN interfaces on internal switch of WaveData. Switch has following assignations with external ethernet ports:

- WAN Ethernet/SFP interface is Port5.
- LAN Ethernet port is Port4.
- CPU Port is connected internally to CPU. SoC receives switch traffic through this port.

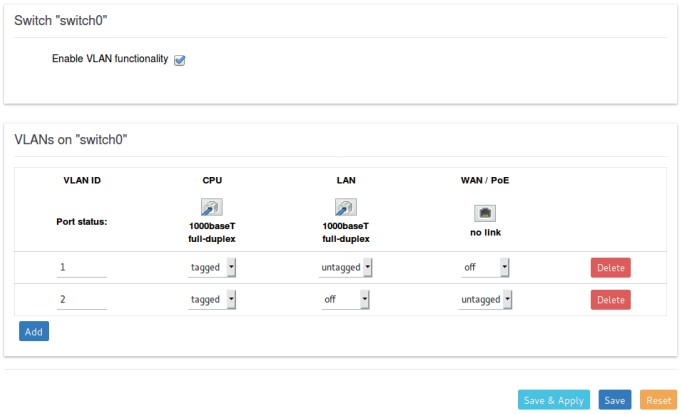
Default configuration creates two VLAN: VLAN1 and VLAN2.

VLAN2: Untagged for WAN port and tagged for port CPU. Switch receives untagged traffic from WAN port and sends to the SoC with VLAN2.

VLAN1: Untagged for LAN Port and tagged for port CPU. Switch receives untagged traffic from the LAN port and sends to the SoC with VLAN1.

The behaviour of the switch is in strict mode, only the VLANs defined in software are recognized by the switch, by default VLAN1and VLAN2.

Other VLANs are not supported by the switch as no are created on the list.



To synchronize with switch, Ethernet driver on SoC is properly configured; Behaviour of the Ethernet driver is as follows:

- Creates two devices: eth0 and eth1.
- Driver knows, through a header inserted by the switch, which port a packet comes from.
- All switch traffic is received/transmitted through CPU Port.
- Propagate received traffic (through CPU port) from WAN port to eth0 interface and vice-versa.
- Propagate received traffic (through CPU port) from LAN port to eth1 interface and vice-versa.

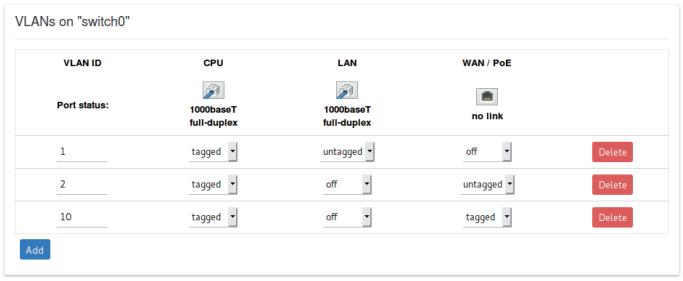
EN

Create VLAN to tag traffic from Wi-Fi

User can add more VLANs according to the needs of the network. The following example shows how to add VLAN10 tag to traffic coming from Wi-Fi interfaces before bridge traffic through WAN.

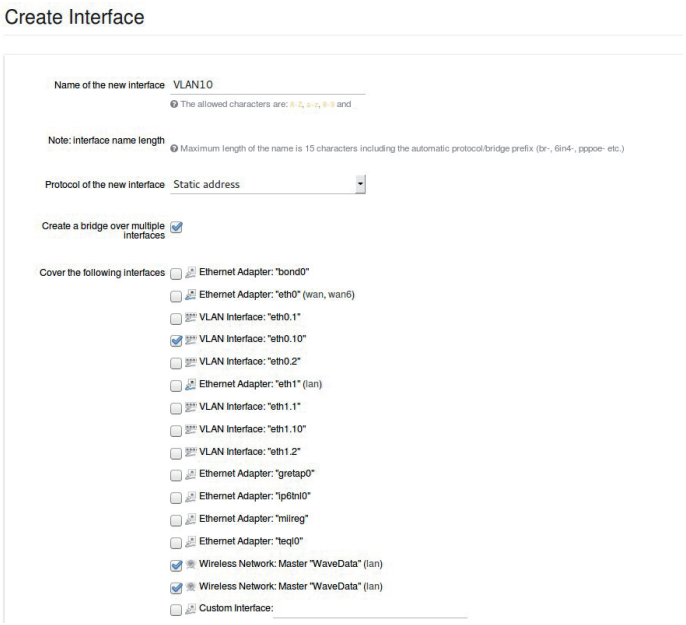
Capture shows how to create VLAN 10 on WAN port and forward tagged traffic to CPU.

Click on *Add* button to add a new VLAN on Switch. This creates new VLAN interface eth0.10 on system.



To manage new VLAN interface eth0.10, you need to create a new interface on system, named VLAN10, as a bridge.

- Go to *Network* > *Interfaces* and click on Add button.
- Check 'Create bridge over multiple interfaces' and Add VLAN Interface eth0.10 and Wi-Fi VAPa as members of new network VLAN10.

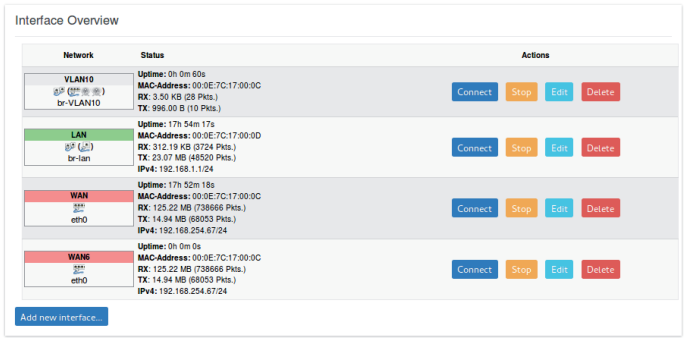


VLAN10 network propagates Wi-Fi traffic from VAPs to WAN with VLAN10 tag.

On *Network* > *Interfaces* you can see new VLAN10 interface.

VLAN10 interface bridge traffic from Wi-Fi VAPs to WAN port and insert VLAN10 tag.

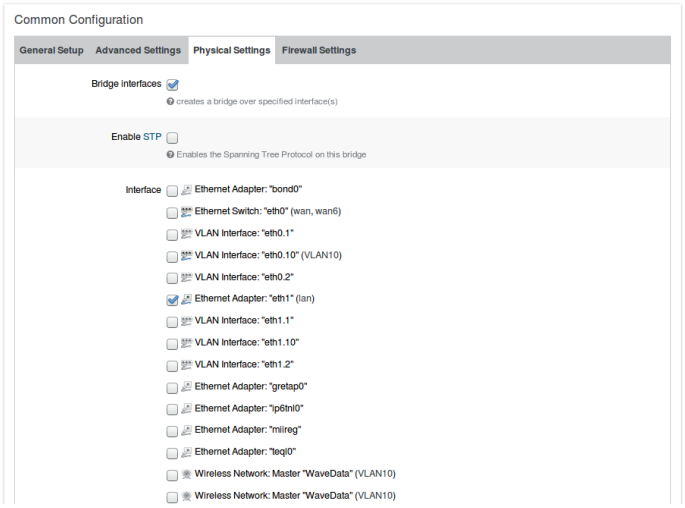
Interfaces



Note that all VAPs are LAN members by default. In order the new configuration works remove VAP interfaces from LAN network where are added by default on system.

Go To *Network* > *Interfaces* > *LAN* > *Edit* > *Physical Interfaces* and remove Wireless Network VAPS from LAN. Now VAPs only are associated with VLAN10.

Interfaces - LAN

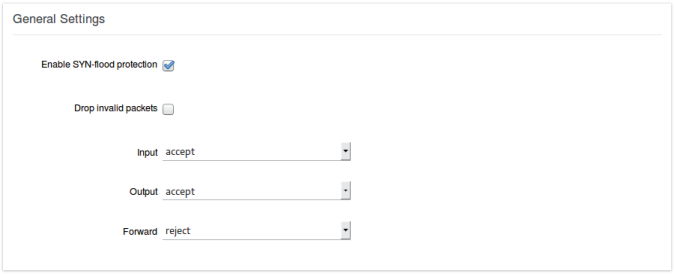


Configure Firewall

Go to *Network* > *Firewall* to configure Firewall.

Every zone has three types of traffic:

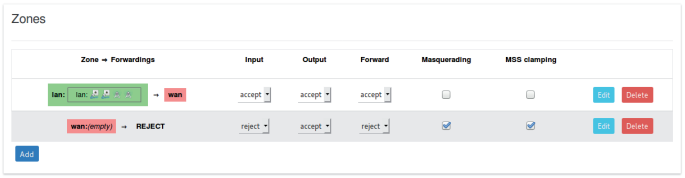
- **Input**: Traffic received from a interface with destination to CPU. Access to local services like SSH or Web.
- **Output**: Traffic send to a interface from internal CPU. For example traffic sent by CPU when connect to Web interface.
- **Forward**: Traffic is routed from one zone to another. For example traffic from LAN to WAN.



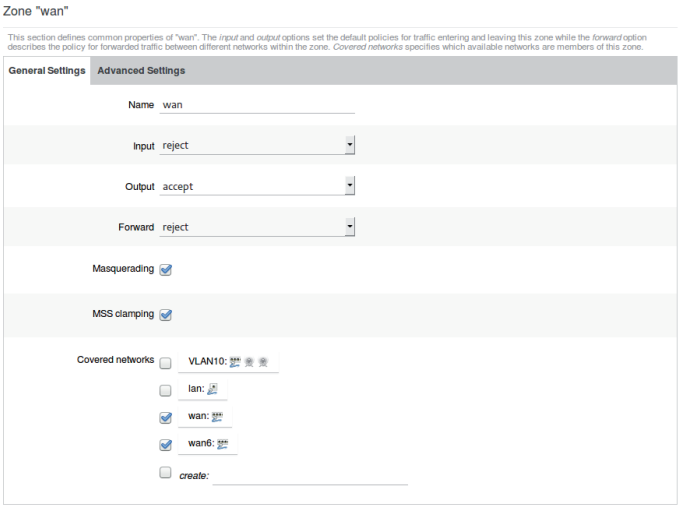
Normally packet comes from a network covered by a zone, but if router receives a packet from interface what is not covered by a firewall zone, applies default policies.

By default Firewall defines two zones

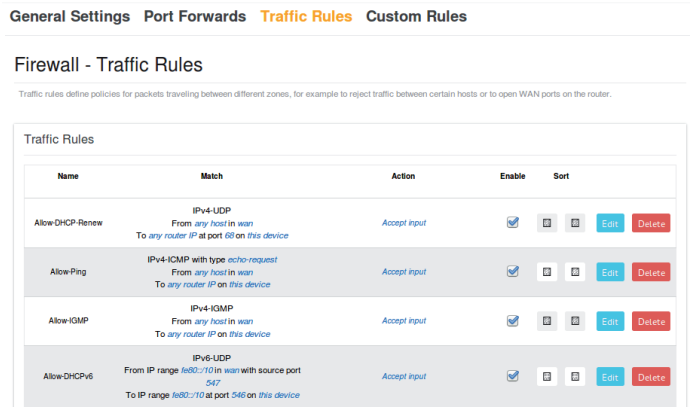
- **LAN zone**: Default policy is accept all traffic to CPU (Input and Output) and reject Forward.
- **WAN zone**: Default policy is accept only Output. Input and Forward are rejected. WAN zone also enable Masquerading (NAT) and MSS Clamping. This policy rejects all input and forwarding traffic but some exceptions are added like Port Forwarding and Traffic Rules (open Web or SSH ports by example).



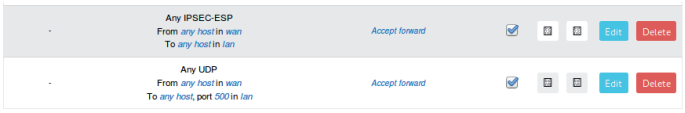
WAN Zone



- WAN zone covers WAN and WAN6 network interfaces.
- Default policy for WAN is reject input traffic (to avoid hack router services) and accept all output from CPU to WAN.
- Forwarding to unknown zones is rejected but you can use Inter-Zone Forwarding to enable forwarding to/from another zones.
- Although the input policy is reject by default, policy is override by custom rules. Figure shows some input rules defined for WAN zone that accept some input protocols like ping or DHCP.



- Although the forwarding policy is reject by default, packet is forwarded if match a Forwarding Traffic Rule or Port Forwarding rule. Figure show how IPSec is enabled to traverse from WAN to LAN.

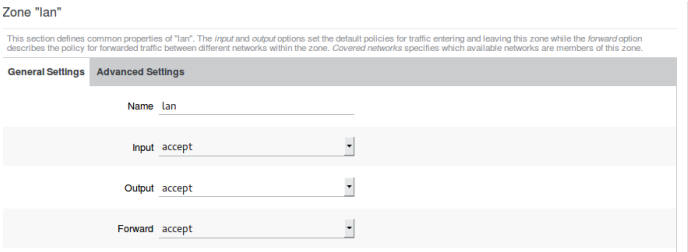


- Packet is forwarded if match an active connection (packet belong to a valid Connection with ESTABLISHED or RELATED states on Connection tracking). Most of the WAN to LAN traffic belongs to this category.
- Inter-zone forwarding: Packet is forwarded if is enabled to traverse between zones. Most of the Traffic from WAN to LAN do not need enable inter-zone forwarding since is related with an active connection but LAN packets to WAN destination need to be enabled to forward since connections are started from LAN.

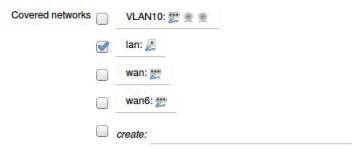
LAN Zone

LAN zone covers all traffic from and to local interfaces.

- When router receives a packet from LAN, default policy is accept input and output traffic to CPU. Local host have access to router services like web or SSH without any restrictions.
- Default policy to Forward traffic is reject traffic from unknown zones. Use Inter-Zone Forwarding to enable forwarding to/from another zones or add custom Traffic Rules.



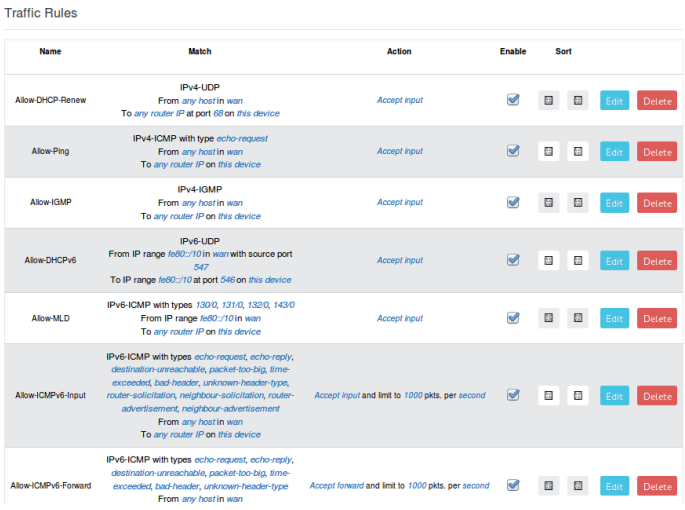
- LAN zone covers LAN network.



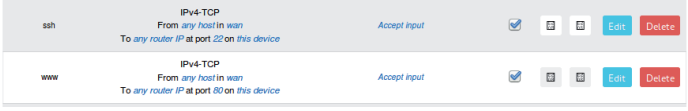
- LAN zone accepts traffic from WAN if match a active Connection or Port Forwarding Rule. WAN zone rejects forwarding from LAN (When LAN users start connections no State is available) so enable forwarding from LAN to WAN in order WAN zone can accept all traffic comes from LAN.

Traffic rules

By default, Firewall is built with traffic rules to accept some traffic classes. Following rules accept UpnP, DHCP and ping to device from WAN interfaces. This allow configure WAN via DHCP, a ping or PlugAndPlay detection.

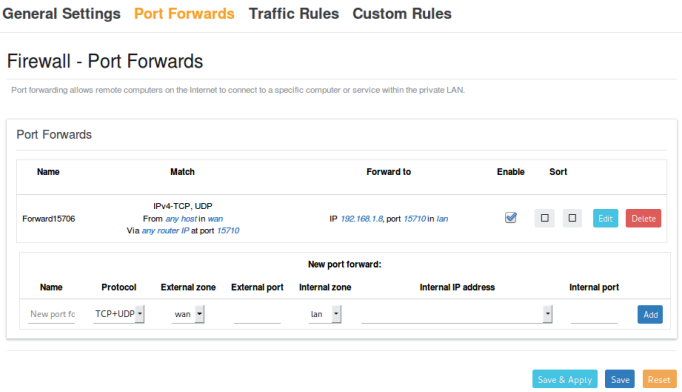


Another rules allows connection to web and SSH services from WAN.



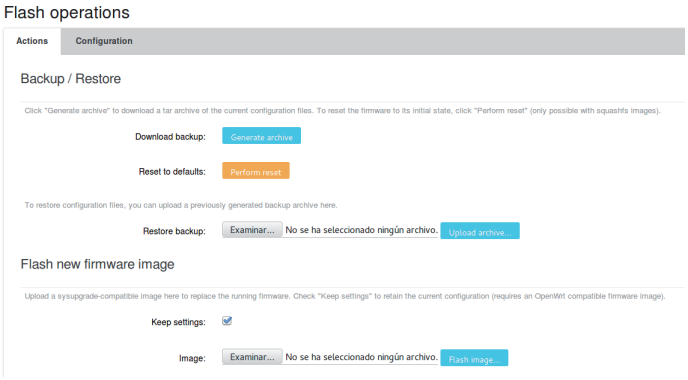
Port Forwarding

Port forwarding allows propagate traffic from WAN host to a local server on another zone. This provides visibility to local servers (LAN) on WAN network. Following example enables port forwarding of requests from WAN zone to router on port 15710 will be propagated to local 192.168.1.8 host. External hosts can use router 15710 port to connect with 192.168.1.8:15710 service hosted on LAN.



Upgrade Firmware and Configuration

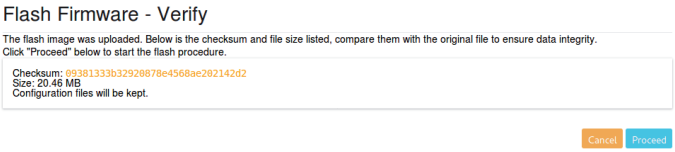
Go to *System>Backup/Flash Firmware*. Below image shows screenshot of upgrade interface.



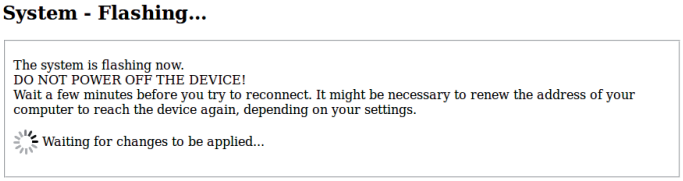
Device flash operations include:

- **Download Backup:** Save device configuration on a compressed file.
- **Reset to Defaults**: Configure device to defaults and reboot.
- **Restore Backup**: upgrade device configuration with a previous saved backup.
- **Upgrade Firmware**: Upgrade whole filesystem and kernel to latest release. Firmware releases are provided by Televes. Check Option to keep current settings after upgrade (checked by default).

Firmware Upgrade Firmware is performed on two-stage, first performs a firmware validation.



After check firmware is valid, Click on *Proceed* to upgrade firmware.



EN

List of acronyms

ACRONYM	MEANING
AES-CCMP	Advanced Encryption Standard-Counter. Cipher Mode Protocol
AES-GCMP	Advanced Encryption Standard-Counter.
AP	Wireless access point, known by the acronym WAP or AP
Auto-MDIX	Auto Medium Dependent Interface crossover
BPSK	Binary phase-shift keying
CPU	Central Processing Unit
DCHP	Dynamic Host Configuration Protocol
DDR	Double Data Rate Synchronous Dynamic Random-Access Memory
DNS	Domain Name System
eMMC	embedded MultiMediaCard
GPRS	General Packet Radio Service
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
MIMO	Multiple-Input and Multiple-Output
MLD	Multicast Listener Discovery
MU-MIMO	Multi-user MIMO
NAT	Network Address Translation
NTP	Network time protocol
OFDM	Orthogonal Frequency Division Multiplexing
PAP/CHAP	Password Authentication Protocol /Challenge Handshake Authentication Protocol
PoE	Power over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase-Shift Keying
RGB	Red Green Blue
RRM	Radio Resource Management
SFP	Small Form-factor Pluggable
SSH	Secure Shell
SSID	Service Set Identifier
STA	STATION.A client device in an 802.11 (Wi-Fi) wireless network such as a computer, laptop
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol
UPNP	Universal Plug and Play
USB	Universal Serial Bus
VAP	Virtual Access Point
VLAN	Virtual LAN
WAN	Wide Area Network
WDS	Wireless distribution System
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN
WMM	Wi-Fi Multimedia
WPA-EAP	Wi-Fi Protected Access - Protected Extensible Authentication Protocol
WPA-PSK	Wi-Fi Protected Access - Pre-Shared Key
WPS	Wi-Fi Protected Setup

WaveData Characteristics

CPU	Processor	QCA IPQ
System Memory	DDR, NOR, eMMC	512MB DDR, 32MB NOR, 4GBytes eMMC
Interfaces	Power, Ethernet, USB	1x USB 3.0 1x Jack Power 12-24Vdc. 12V/2A 1x RJ45 Gigabit (10/100/1000). Auto MDI-X 1x PoE RJ45 Gigabit Ethernet 802.11af/at. Auto MDI-X (only ref. 769001) 1x SFP IEEE 1000BASE-X (only ref. 769002)
Wireless	Interfaces	2.4G and 5G WLAN interfaces with following features 1x2.4G IEEE 802.11nbg 2x2 MIMO 1x5G IEEE 802.11nac Wave2 5G 2x2 MIMO
	Max. TX Power	2.4 GHz 23.5dBm @ MCS0 HT20 16.5dBm @ MCS9 HT40 5 GHz 22 dBm @ MCS0 HT20 15.5 dBm @ MCS9 HT40 14.5 dBm @ MCS9 HT80
	Wireless PHY Rate	1.73 Gbps max. 2x2 On-Board 5 GHz radio, up to 867 MBps physical data rate 2x2 On-Board 2.4 GHz radio, up to 300 MBps physical data rate
	MIMO	2.4 GHz 2x2 and 5 GHz 2x2
	Frequency range	2.412 - 2.472 GHz and 5.180 - 5.825 GHz
	Channel Bandwidth	5 GHz radio: 20/40/80 MHz 2.4 GHz radio: 5/10/20/40 MHz
	Modulations	OFDM: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM
	Antennas	4xDual Band Antenna, Polarization Linear, Beamforming
	Antenna Gain	2.4 GHz +4dBi, 5 GHz +4dBi
	Security	Encryption: Open, WEP, WPA-PSK, 802.1X WPA-EAP Ciphers: TKIP, AES-CCMP, AES-GCMP
Leds	RGB Led	Tri-color to indicate device status. • Green: Device OK and Wi-Fi up. • Blue: Device OK and Wi-Fi off. • Orange: Device OK and myNETWi-Fi (max 10dBm power). • Blink Blue: System upgrade in progress.
Buttons	Reset Button	Hardware Reset Button
	WPS/Factory Defaults	• 0-3secs: WPS • >3secs: Factory Defaults
	MyNETWi-Fi switch	Tri-state: Off, Normal (22dBm), myNETWi-Fi(10dBm).
Device Access	IP address	Default IP: 169.254.1.254
	Login account	User: root, Password: 76Wave90Data01
OS	Linux/OpenWRT	Linux kernel 4.4.60, QCA QSDK based on OpenWRT CC 15.05
Power	Jack Adapter	1x DC Jack Connector: 12-24 V. 12V/2A
	Power over Ethernet (PoE)	Passive PoE 24V, IEEE 802.3af/at
	Max. Power Consumption	2xWi-Fi Interfaces: max. 7W
Temp range.		-5 ... +45 ° C
Dimensions, Weight		146 x 146 x 43 mm 300 g

- Hereby, Televes S.A.U. declares that the radio equipment type Wave Data is in compliance with Directive 2014/53/EU. The full text of the EU declaration of conformity is available at the following internet address: https://doc.televes.com.

European technology **Made in EUrope**

Manufacturer: **Televes S.A.U.** Rúa B. de Conxo, 17 - 15706 Santiago de Compostela, A Coruña. Spain www.televes.com

769001, 769002_001_EN