HIKVISION

User Manual

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to DS-3WF01C-2N (Product Series).

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (http://overseas.hikvision.com/en/).

Please use this user manual under the guidance of professionals.

Trademarks Acknowledgement

HIKVISION and other Hikvision’s trademarks and logos are the properties of Hikvision in various jurisdictions. Other trademarks and logos mentioned below are the properties of their respective owners.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Regulatory Information

FCC Information

Please take attention that changes or modification not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

FCC compliance: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Conditions

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.

2. This device must accept any interference received, including interference that may cause undesired operation.

EU Conformity Statement

This product and - if applicable - the supplied accessories too are marked with "CE" and comply therefore with the applicable harmonized European standards listed under the EMC Directive 2014/30/EU, the LVD Directive 2014/35/EU, the RoHS Directive 2011/65/EU.

2012/19/EU (WEEE directive): Products marked with this symbol cannot be disposed of as unsorted municipal waste in the European Union. For proper recycling, return this product to your local supplier upon the purchase of equivalent new equipment, or dispose of it at designated collection points. For more information see: www.recyclethis.info

2006/66/EC (battery directive): This product contains a battery that cannot be disposed of as unsorted municipal waste in the European Union. See the product documentation for specific battery information. The battery is marked with this symbol, which may include lettering to indicate cadmium (Cd), lead (Pb), or mercury (Hg). For proper recycling, return the battery to your supplier or to a designated collection point. For more information see: www.recyclethis.info

Industry Canada ICES-003 Compliance

This device meets the CAN ICES-3 (A)/NMB-3(A) standards requirements.

Applicable Models

This manual is applicable to switches below: DS-3WF01C-2N (product series).

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
ℹ NOTE	Provides additional information to emphasize or supplement important points of the main text.
⚠ WARNING	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
⚠ DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.

⚠ **WARNING**

- During the installation and utilization of the device, please strictly conform to electrical safety rules in different nations and regions.
- You shall acknowledge that the use of the device with Internet access might be under network security risks, please strengthen protection for your personal information and data security. If you find the device might be under network security risks, please contact with us.

Catalog

Chapter 1 Introduction

1.1 Overview

The DS-3WF01C-2N wireless bridge can be applied to elevator internal monitoring video transmission, and can use the multi-network port to connect to the elevator advertising machine for real-time data update.

1.2 Packing List

The packing list is shown as below. If any accessories are damaged or lost, keep the package intact and contact your dealer for replacement.

Table 1-1 Packing List of DS-3WF01C-2N

Name	Item	Quantity
Device	DS-3WF01C-2N	2
Power Adapter	12V, 1A	2
Mounting Bracket	For installing device	2
Pole Mounting Straps	For installing device	4
Quick Start Guide	Instruction manual	1

1.3 Appearance

1.3.1 Front Panel

Front panel of DS-3WF01C-2N is shown as below.

Front Panel of DS-3WF01C-2N

Figure 1-1 DS-3WF01C-2N Front Panel

Physical Interface

The hardware interfaces of the DS-3WF01C-2N are as follows.

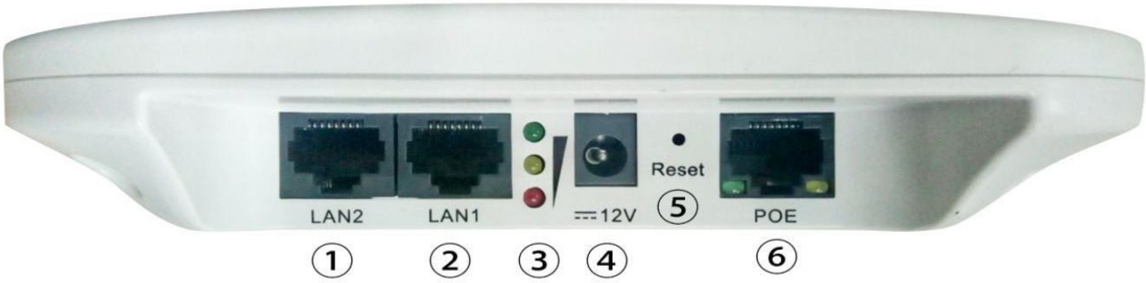


Figure 1-2 Physical Interface

Table 1-1 Physical Interface

Index	Description
1	Access to the camera, digital signage and other equipments
2	Access to the camera, digital signage and other equipments
3	Signal strength indicator
4	12 V DC power supply port
5	Restore default factory settings
6	PoE port connection with PoE power supply

Chapter 2 Installation

Step 1 First install the mounting bracket on the main unit. The supporting bracket of the device contains a magnet to help the device automatically adsorb on the surface of the iron-containing material.

NOTE

- If the surface of the mounting device does not contain iron, please install it with the plastic ties.

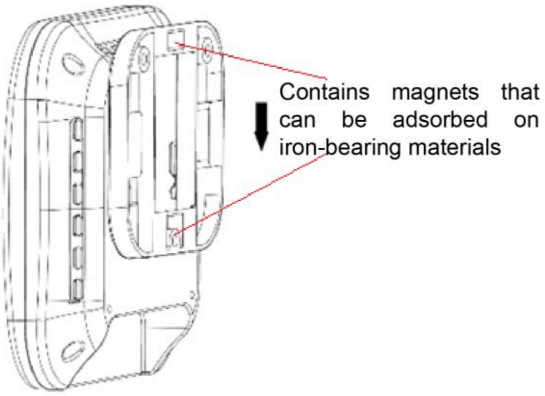

Contains magnets that can be adsorbed on iron-bearing materials

Figure 2-1 Install host

Step 2 Install the AP device on top of the shaft of the elevator shaft as shown below:

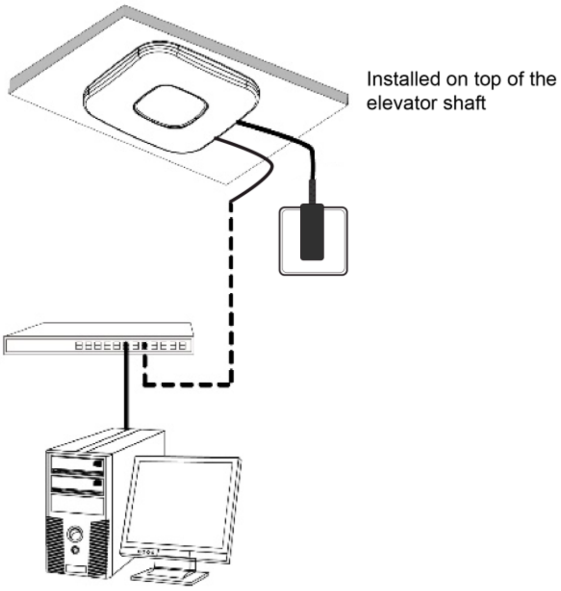


Figure 2-2 Power on the device

Step 3 Install the CPE device on top of the elevator, as shown below:

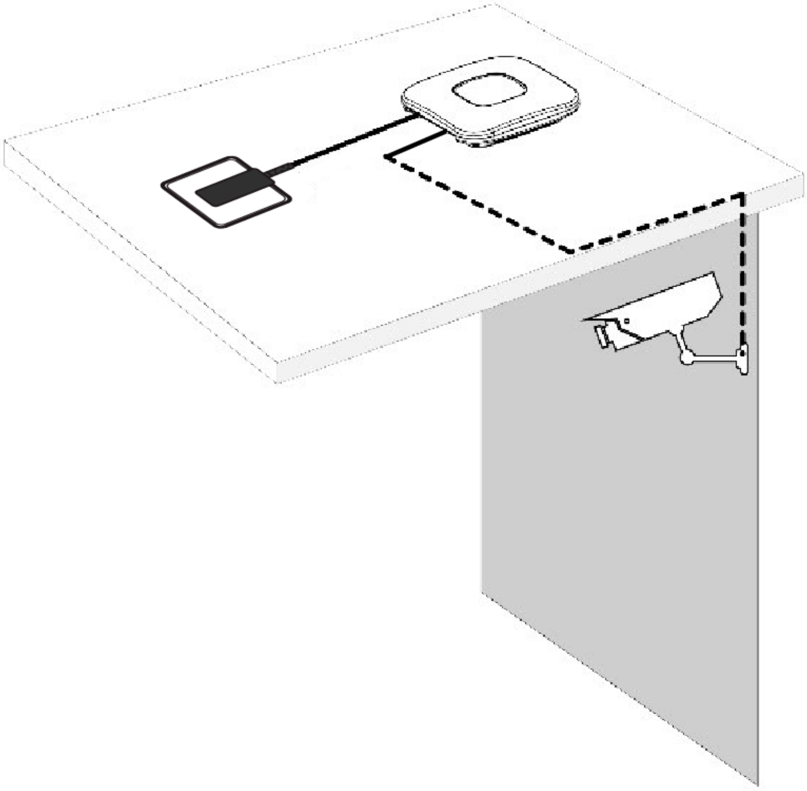


Figure 2-3 Finish installation

NOTE

- The device must be installed without direct obstruction and the two devices are aligned up and down.

Chapter 3 Quick Configuration

3.1 Log in

To log in the device, you need to configure the TCP/IP of your computer first as the following steps:

Step 1 Use a network cable to connect the computer to the LAN interface of the device to prepare the device. First, you need to configure the computer IP address and the device's default IP address to be on the same network segment. Take the Windows 7 system as an example. Click the network logo in the lower right corner of the desktop and click Open Network & Internet settings-Network and Sharing Center. As shown below.

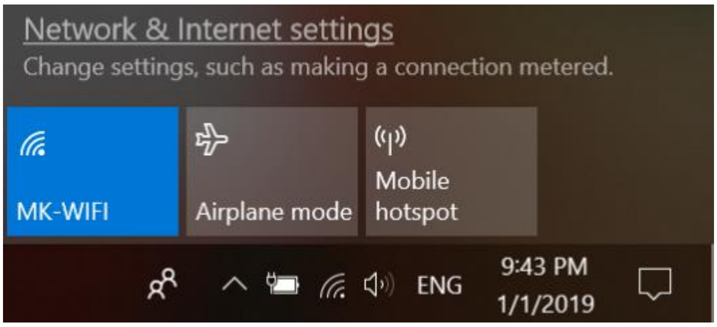
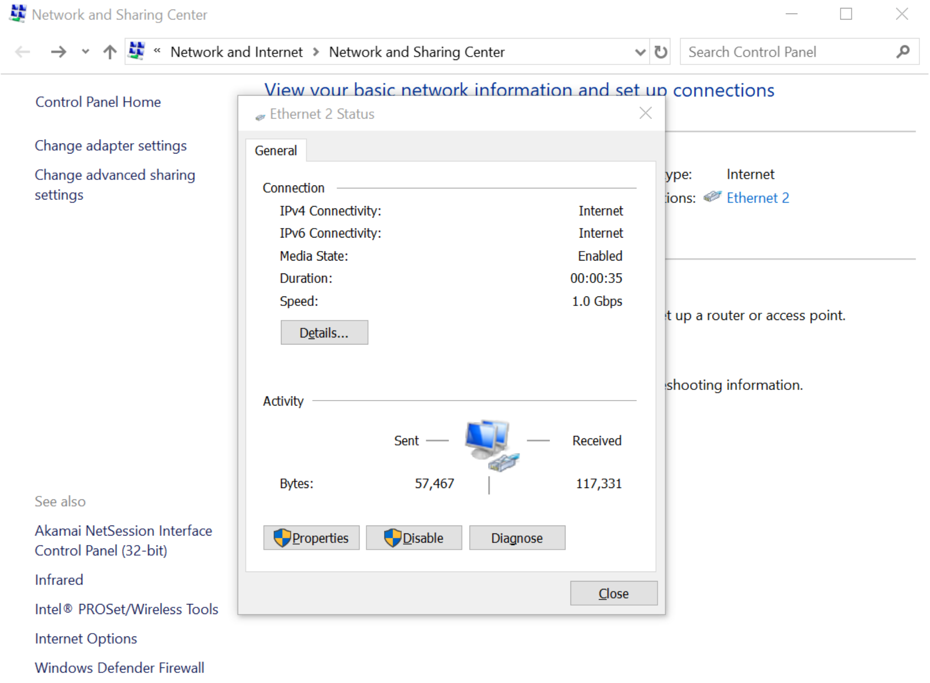

Network & Internet settings
Change settings, such as making a connection metered.
MK-WIFI
Airplane mode
Mobile hotspot
ENG
9:43 PM
1/1/2019

Figure 3-1 Network & Internet settings

Step 2 Click "Local Area Connection" on the right and click "Properties". As shown below.


Network and Sharing Center
Network and Internet > Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
Akamai NetSession Interface Control Panel (32-bit)
Infrared
Intel® PROSet/Wireless Tools
Internet Options
Windows Defender Firewall
View your basic network information and set up connections
ype: Internet
ions: Ethernet 2
t up a router or access point.
shooting information.
Ethernet 2 Status
General
Details...
Properties
Disable
Diagnose
Close

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: Internet

Media State: Enabled

Duration: 00:00:35

Speed: 1.0 Gbps

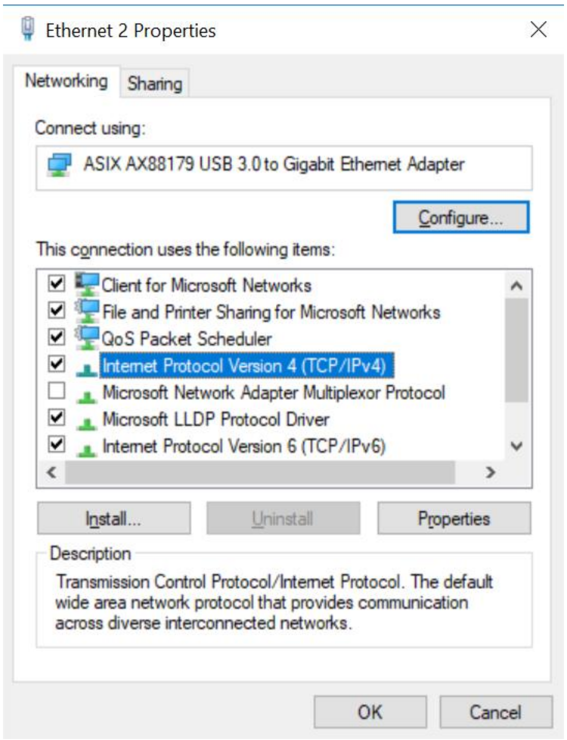
Activity

Sent — — Received

Bytes: 57,467 | 117,331

Figure 3-2 Local Area Connection

Step 3 Double-click Internet Protocol Version 4 (TCP/IPv4). As shown below.



Ethernet 2 Properties

Connect using:

ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

This connection uses the following items:

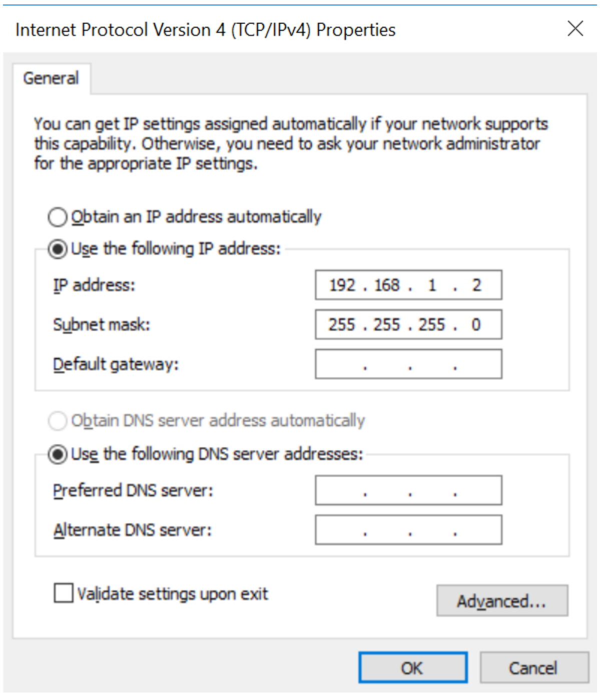
- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Figure 3-3 Internet Protocol Version 4 (TCP/IPv4)

Step 4 Configure the IP address of the computer to be the unused 192.168.1.X address in the LAN. X is any integer other than 35, 36 in 2 to 253. The subnet mask is 255.255.255.0. Click "OK" as shown below.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

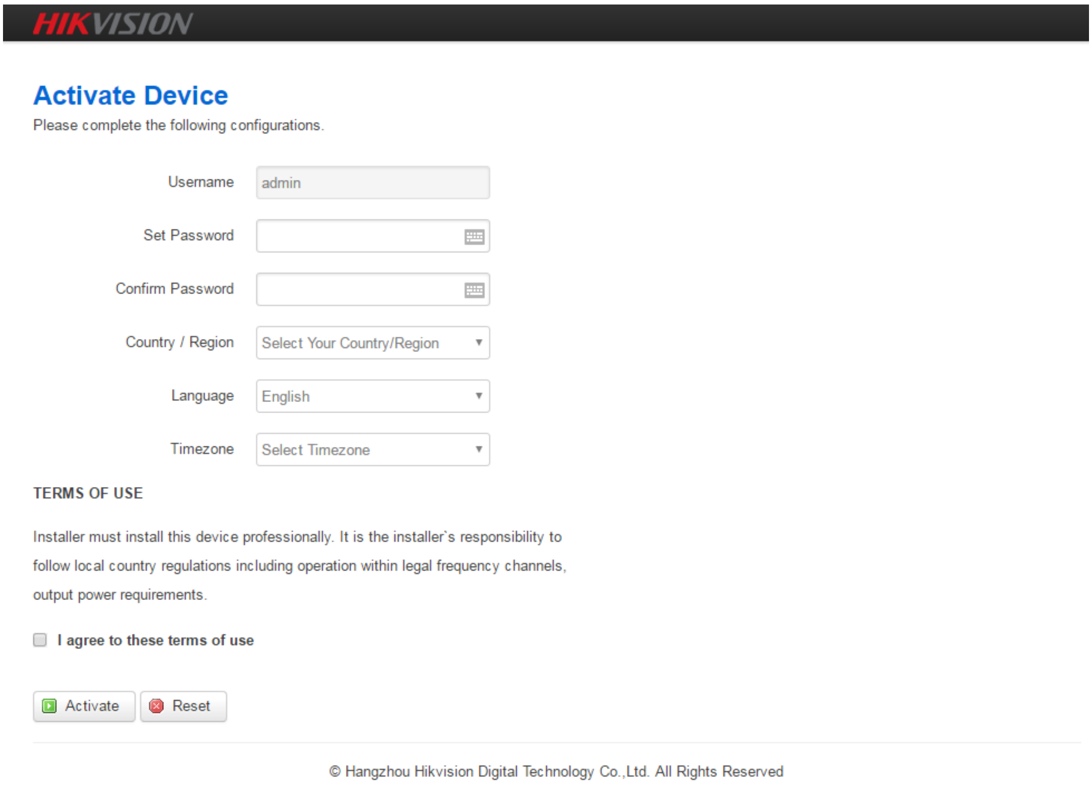
□ Validate settings upon exit

Figure 3-4 Configure the IP

Make sure that the IP address of the computer is inconsistent with the default IP address of the device. On the same network segment, use a browser to log in to the device, open a browser, and enter the default IP address of the device in the address bar: 192.168.1.35 / 192.168.1.36.

NOTE

- When you log in to the device for the first time, click Enter, enter the device activate page. The user name is admin, and the user password is set by the user. You also need to select your password, country, language and time zone, as shown in Figure 3-5. Check "I agree to these terms of use" and click "Activate" to jump to login page, as shown in Figure 3-6. Take the AP device as an example.



Activate Device

Please complete the following configurations.

Username admin

Set Password

Confirm Password

Country / Region Select Your Country/Region

Language English

Timezone Select Timezone

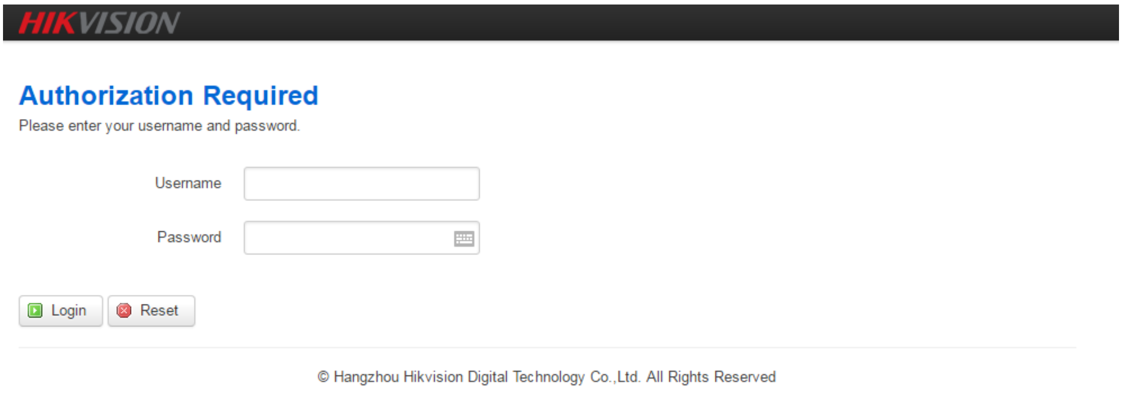
TERMS OF USE

Installer must install this device professionally. It is the installer`s responsibility to follow local country regulations including operation within legal frequency channels, output power requirements.

□ I agree to these terms of use

© Hangzhou Hikvision Digital Technology Co.,Ltd. All Rights Reserved

Figure 3-5 Activate



Authorization Required

Please enter your username and password.

Username

Password

© Hangzhou Hikvision Digital Technology Co.,Ltd. All Rights Reserved

Figure 3-6 login

3.2 Wizard

Users can quickly configure the device according to the following steps through the wizard in this chapter.

The first page shown after log in is the Wizard page, and this page helps to set the basic network parameters. The default mode is Bridge mode, and the default LAN IP address of AP device is 192.168.1.35, the default LAN IP address of CPE device is 192.168.1.36.

NOTE

- If there are several devices connected in the Point-to-Point or Point-to-Multi-Point topologies, they must be configured to different IP address to avoid conflicts.

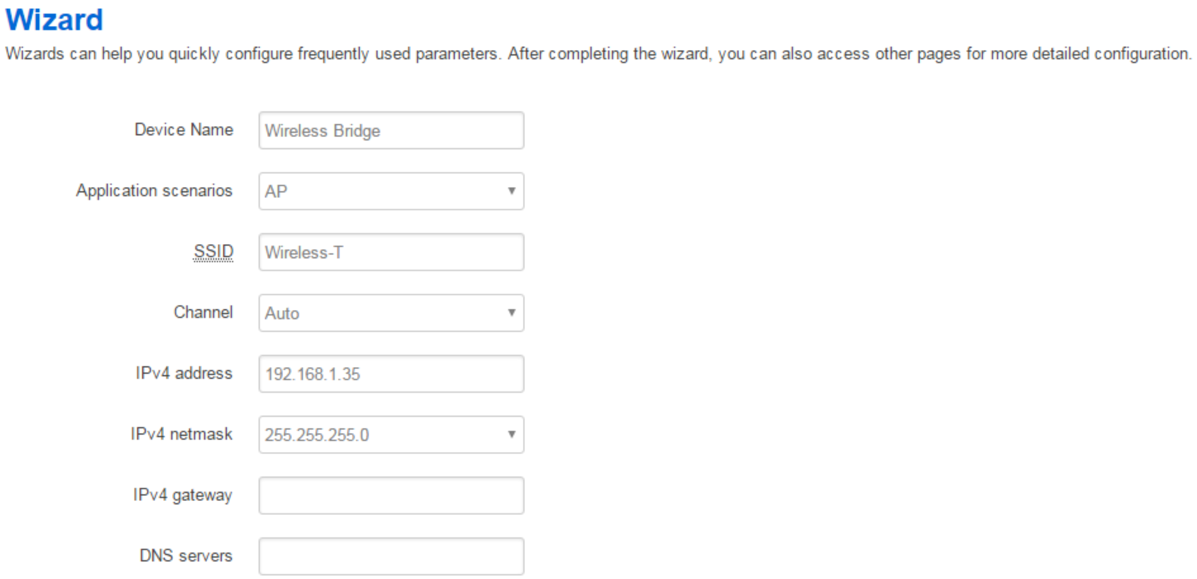
AP: In this scenario mode, the device will be set to access point mode; it can be connected to a client device. When you close the TDMA function, your phone or laptop can connect to the device. If you need other wireless configurations in detail, please refer to chapter 6.

CPE: In this scenario mode, the device will be set to client mode; it can be connected to an access point device.

NOTE

- The default SSID of the AP device and the CPE device must be the same to directly interconnect and transmit audio, video or data. If there are other DS-3WF01C-2N devices within 500 meters, the SSID should be changed to be different in order to avoid connection confusion. Please refer to chapter 6 to see how to modify the SSID.

Click Save & Apply button, the device will reboot and apply your configuration.



Wizard

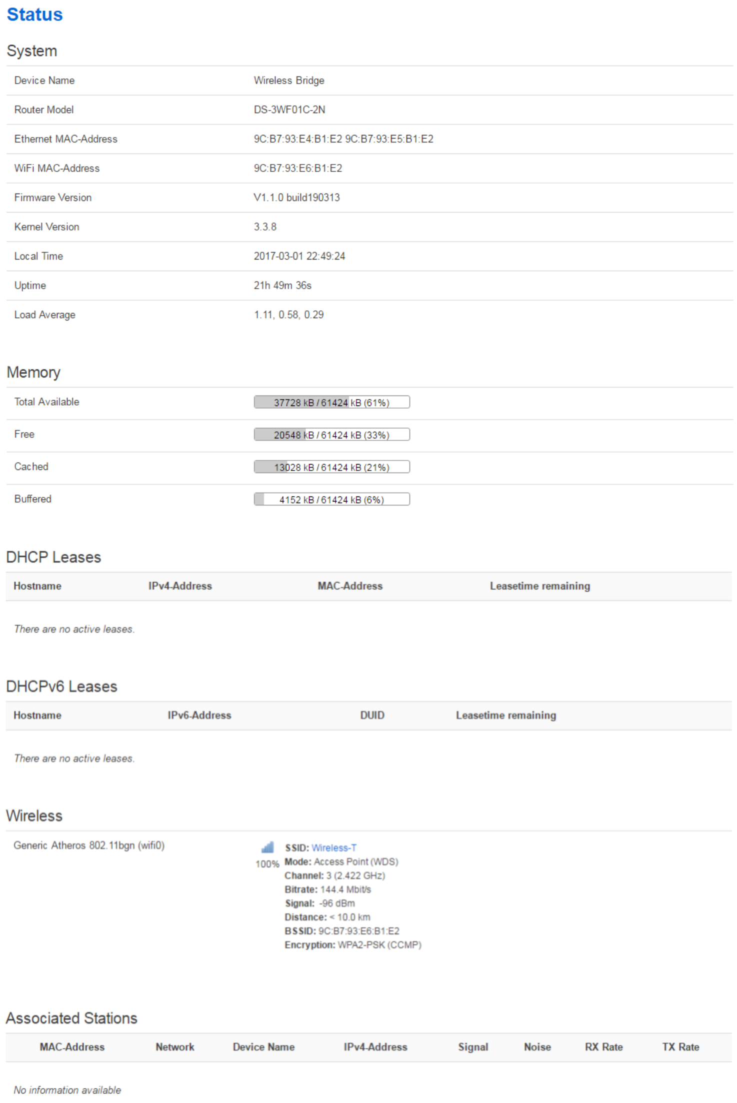
Wizards can help you quickly configure frequently used parameters. After completing the wizard, you can also access other pages for more detailed configuration.

Device Name	Wireless Bridge
Application scenarios	AP
SSID	Wireless-T
Channel	Auto
IPv4 address	192.168.1.35
IPv4 netmask	255.255.255.0
IPv4 gateway	
DNS servers	

Figure 3-7 Wizard

Chapter 4 Status

The status page displays the current configuration and working status of the device. It is the second item in the menu bar, as shown in figure:



Status

System

Device Name	Wireless Bridge
Router Model	DS-3WF01C-2N
Ethernet MAC-Address	9C:B7:93:E4:B1:E2 9C:B7:93:E5:B1:E2
WiFi MAC-Address	9C:B7:93:E6:B1:E2
Firmware Version	V1.1.0 build190313
Kernel Version	3.3.8
Local Time	2017-03-01 22:49:24
Uptime	21h 49m 36s
Load Average	1.11, 0.58, 0.29

Memory

Total Available	37728 kB / 61424 kB (61%)
Free	20548 kB / 61424 kB (33%)
Cached	13028 kB / 61424 kB (21%)
Buffered	4152 kB / 61424 kB (6%)

DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining

There are no active leases.

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining

There are no active leases.

Wireless

Generic Atheros 802.11bgn (wifi0)	100% **SSID:** Wireless-T **Mode:** Access Point (WDS) **Channel:** 3 (2.422 GHz) **Bitrate:** 144.4 Mbit/s **Signal:** -96 dBm **Distance:** < 10.0 km **BSSID:** 9C:B7:93:E6:B1:E2 **Encryption:** WPA2-PSK (CCMP)

Associated Stations

MAC-Address	Network	Device Name	IPv4-Address	Signal	Noise	RX Rate	TX Rate

No information available

Figure 4-1 Status

Overview: Status->Overview, This page shows the current configuration information of the system, including the system, memory, network, DHCP leases, wireless, associated stations.

System log: displaying the system log information of the device.

Real time Graphs: display the real-time load, traffic, and wireless and link information of the device.

Chapter 5 System

System page includes: System, Administration, LED Configuration, Backup / Flash Firmware and Reboot sub-pages. The following are descriptions of the system, Administration, backup / upgrade and reboot sub-pages.

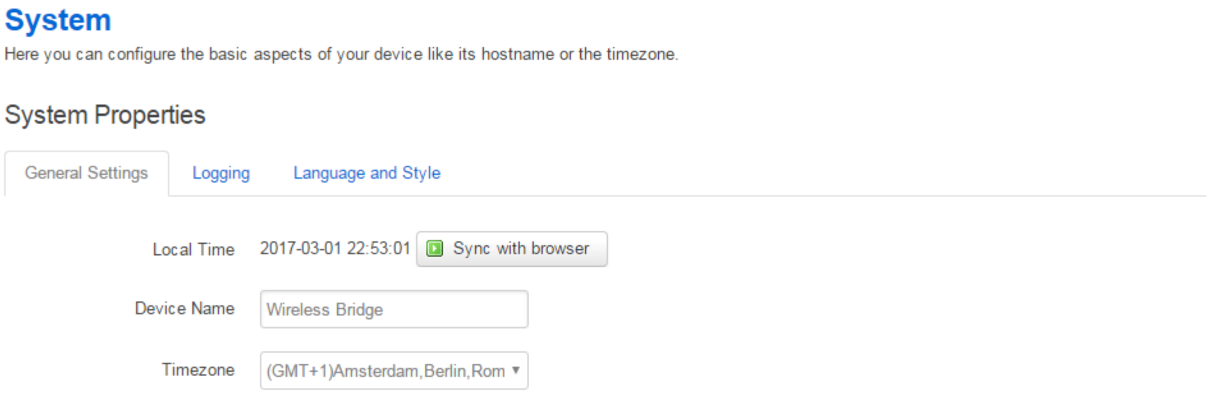
5.1 System

Here you can configure the basic aspects of your device like its hostname or the time zone.

General Settings: some basic information is supported to configure on this page, including time, log, language and interface style.

Click on the "general settings" page, click on "Sync with browser" to synchronize the local time to the device, and it will be displayed in the status page too. The time synchronization can help network administrator check equipment operation status and log information conveniently, and can also help tracking running status of the device.

Host name is corresponding to the Router Name of the status page; users can change it according to their own needs as shown in the figure.



System

Here you can configure the basic aspects of your device like its hostname or the timezone.

System Properties

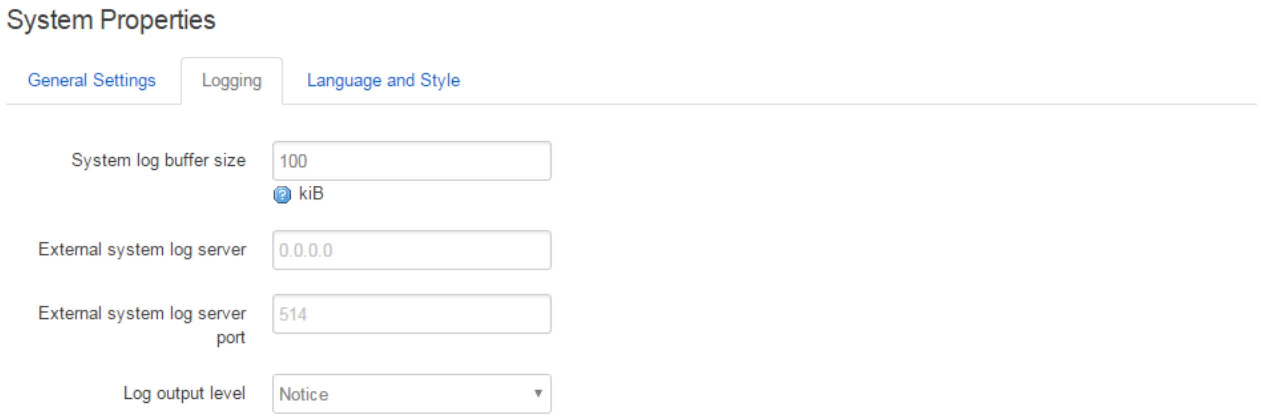
Local Time 2017-03-01 22:53:01

Device Name Wireless Bridge

Timezone (GMT+1)Amsterdam,Berlin,Rom

Figure 5-1 System Properties – General Settings

Logging: When Syslog is enabled, and the System Log server’s IP is also set here, the log information will be output to the Syslog server automatically.



System Properties

System log buffer size: 100 kiB

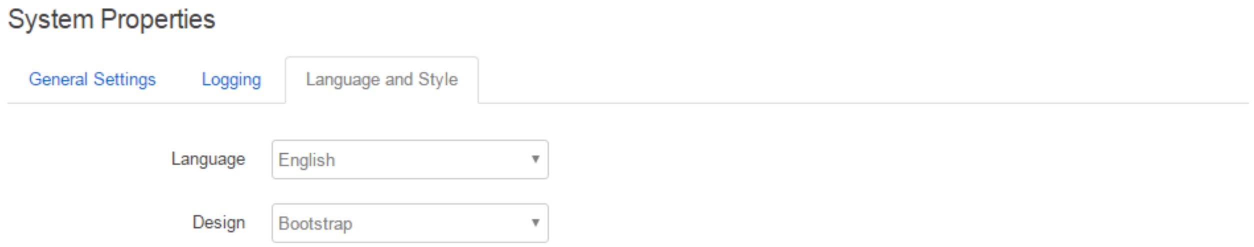
External system log server: 0.0.0.0

External system log server port: 514

Log output level: Notice

Figure 5-2 System Properties - Logging

Language and Style: choose the language of the web page you want. You can modify the Language into English or Chinese. The default Design is bootstrap style.



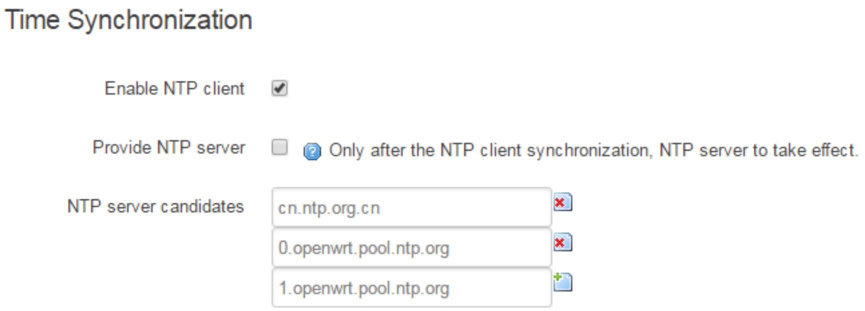
System Properties

Language: English

Design: Bootstrap

Figure 5-3 System Properties – Language and Style

Time Synchronization: when the device can surf the Internet, you can enable the NTP client and fill in the NTP server candidates. DS-3WF01C-2N will get time automatically from the NTP server and displayed in the status page. At this point you can also tick the Provide NTP server and make the device as a NTP server for other devices connected to the DS-3WF01C-2N to acquire time.



Time Synchronization

Enable NTP client ☑

Provide NTP server ☐ Only after the NTP client synchronization, NTP server to take effect.

NTP server candidates:
cn.ntp.org.cn
0.openwrt.pool.ntp.org
1.openwrt.pool.ntp.org

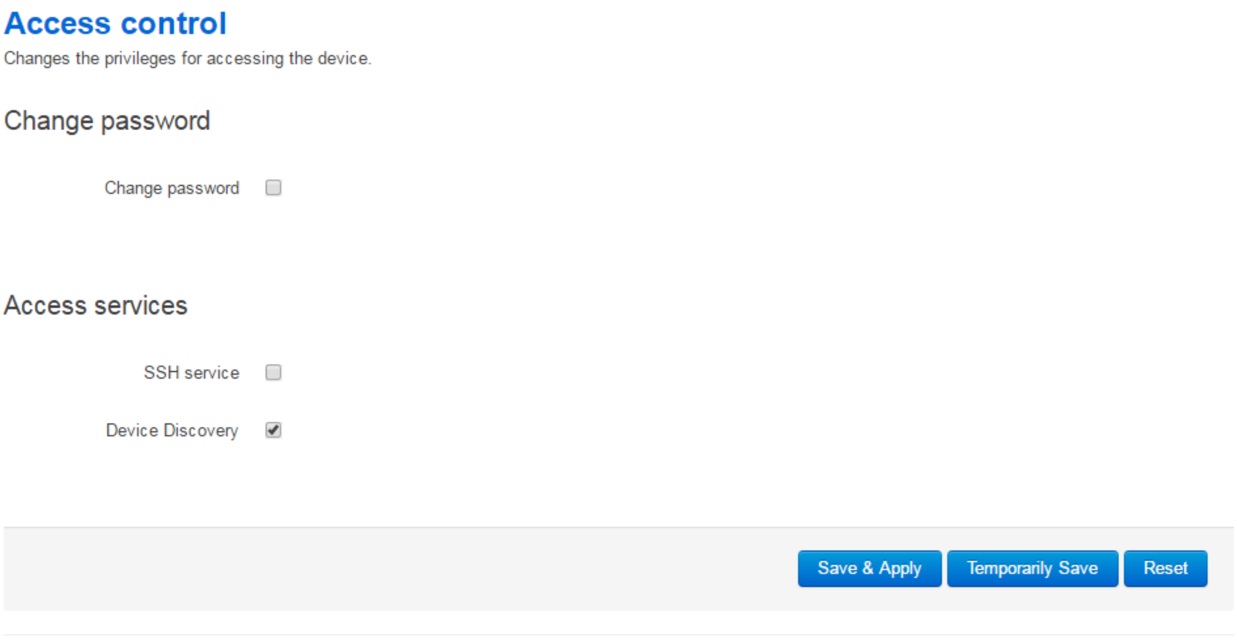
Figure 5-4 System Properties – Time Synchronization

5.2 Administration

Password: Changes the administrator password for accessing the device.

SSH service: Drop bear offers SSH2 network shell access and an integrated SCP server. The user can login the device through more secure SSH.

Device Discovery: This feature is enabled by default and needs to be used with the device discovery tool.



Access control

Changes the privileges for accessing the device.

Change password

Change password □

Access services

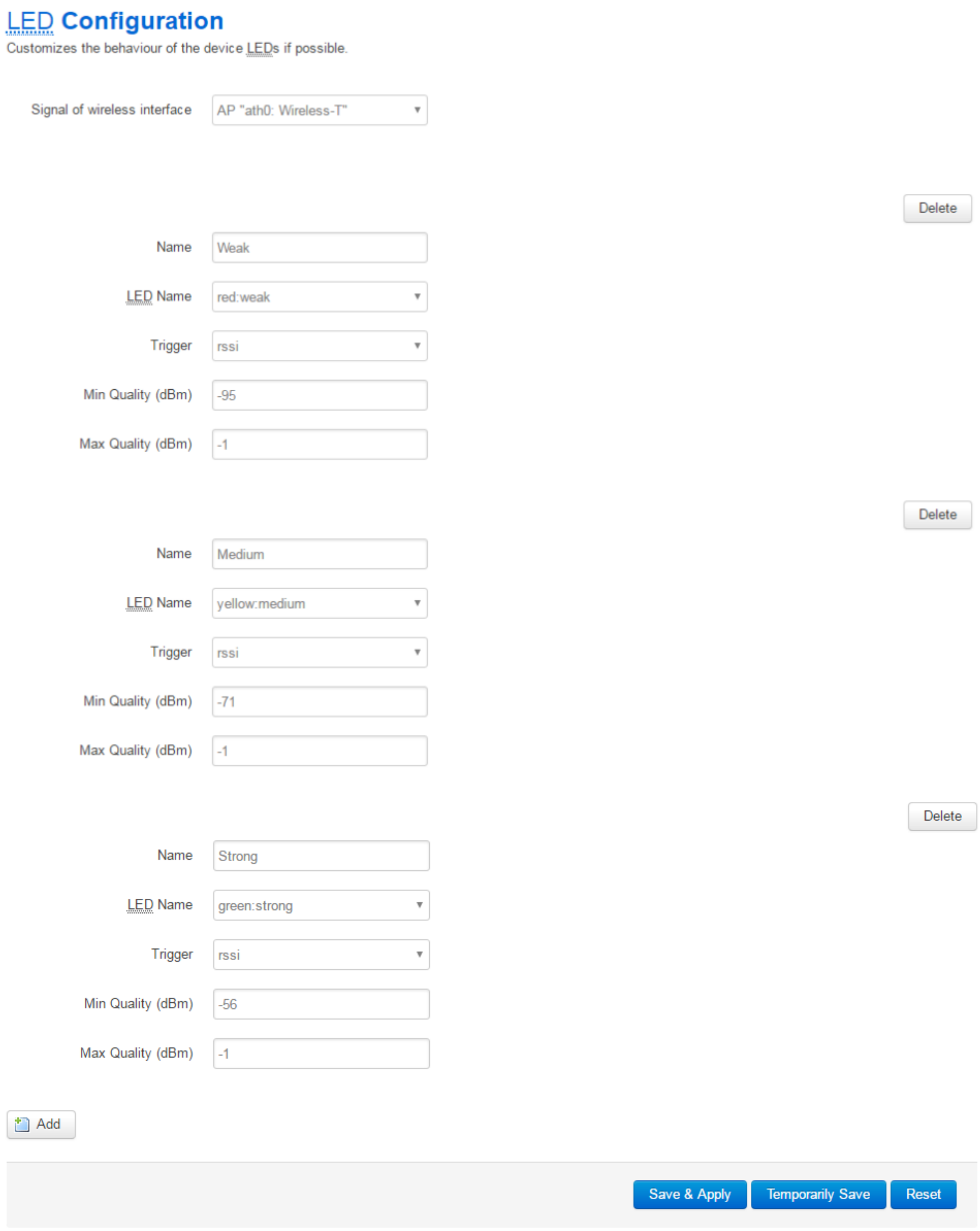
SSH service □

Device Discovery ☑

Figure 5-5 Administration

5.3 LED Configuration

Click on System->LED Configuration, in this page you can customize the behavior of the device LEDs if possible; it defines the value of the signal strength required for the light of the 3 LEDs, which works only on the CPE mode device.



LED Configuration

Customizes the behaviour of the device LEDs if possible.

Signal of wireless interface: AP "ath0: Wireless-T"

Name: Weak
LED Name: red:weak
Trigger: rssi
Min Quality (dBm): -95
Max Quality (dBm): -1

Name: Medium
LED Name: yellow:medium
Trigger: rssi
Min Quality (dBm): -71
Max Quality (dBm): -1

Name: Strong
LED Name: green:strong
Trigger: rssi
Min Quality (dBm): -56
Max Quality (dBm): -1

Figure 5-6 LED Configuration

The red LED intensity value is the smallest of the 3 LEDs (red < yellow < green), the default range of red LED: -95~-1dBm, yellow: -71~-1dBm, green: -56~-1dBm. When the signal strength is higher than -95dB and below -71dBm, red light; when the signal strength is higher than -71dB and below -56dBm, both red and yellow light; when the signal strength is higher than -56dBm, all the 3 LEDs light.

5.4 Backup / Flash Firmware

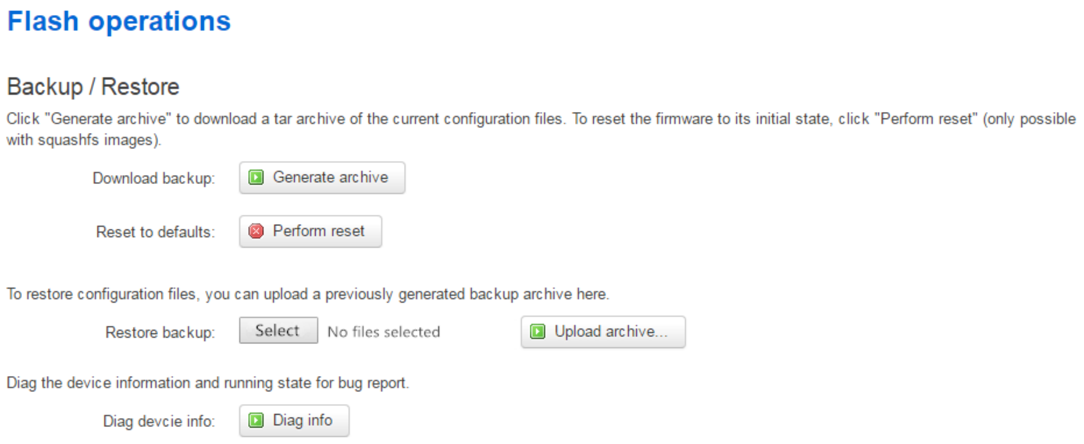
System->Backup / Flash Firmware page is very simple to use. It is divided into the following 2 parts:

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files.

Click "Perform reset" to reset the firmware to its initial state.

To restore configuration files, you can upload a previously generated backup archive.



Flash operations

Backup / Restore

Click "Generate archive" to download a tar archive of the current configuration files. To reset the firmware to its initial state, click "Perform reset" (only possible with squashfs images).

Download backup: Generate archive

Reset to defaults: Perform reset

To restore configuration files, you can upload a previously generated backup archive here.

Restore backup: Select No files selected Upload archive...

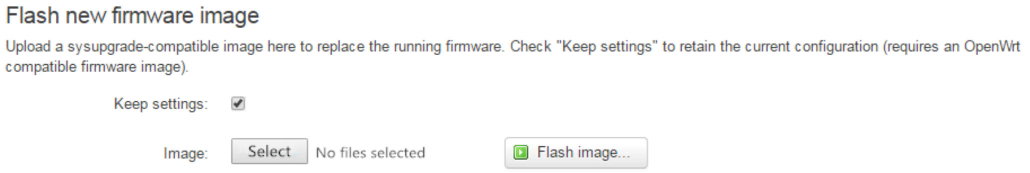
Diag the device information and running state for bug report.

Diag devcie info: Diag info

Figure 5-7 Backup / Restore

Flash new firmware image

Upload a sysupgrade - compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).



Flash new firmware image

Upload a sysupgrade-compatible image here to replace the running firmware. Check "Keep settings" to retain the current configuration (requires an OpenWrt compatible firmware image).

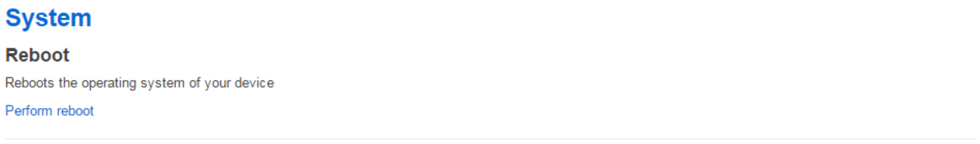
Keep settings: ☑

Image: Select No files selected Flash image...

Figure 5-8 Flash new firmware image

5.5 Reboot

Click Perform reboot to reboot the operating system of your device.



System

Reboot

Reboots the operating system of your device

Perform reboot

Figure 5-9 Reboot

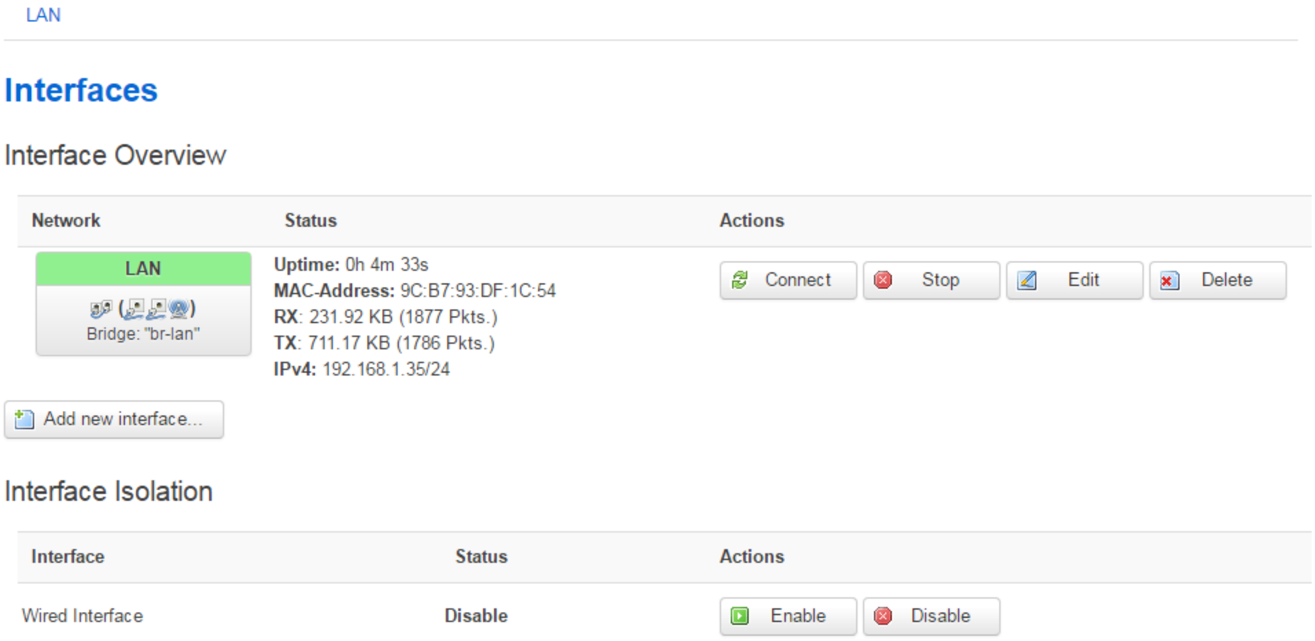
Chapter 6 Network

The network settings page is divided into the Interface, Wifi, Static Routes, Firewall, VLAN, Ping Watchdog.

6.1 Interface

6.1.1 Common Configuration

Open the network interface page, you'll see the overview of the current interface.



LAN

Interfaces

Interface Overview

Network	Status	Actions
LAN Bridge: "br-lan"	**Uptime:** 0h 4m 33s **MAC-Address:** 9C:B7:93:DF:1C:54 **RX**: 231.92 KB (1877 Pkts.) **TX**: 711.17 KB (1786 Pkts.) **IPv4:** 192.168.1.35/24	Connect Stop Edit Delete

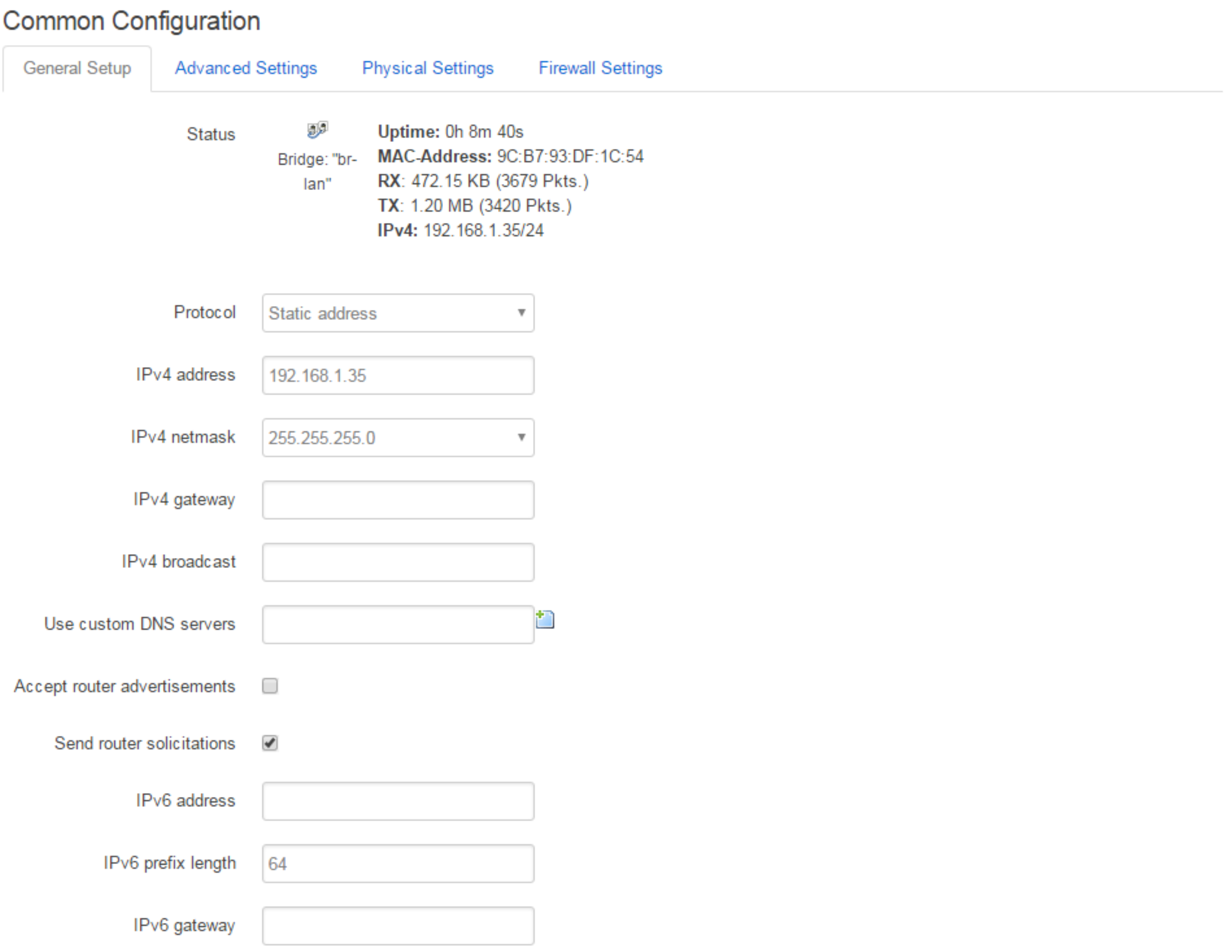
Add new interface...

Interface Isolation

Interface	Status	Actions
Wired Interface	**Disable**	Enable Disable

Figure 6-1 Interfaces

Click "Edit" button, you will enter the Interfaces-LAN page. On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).



Common Configuration

Status

Bridge: "br-lan"

Uptime: 0h 8m 40s
MAC-Address: 9C:B7:93:DF:1C:54
RX: 472.15 KB (3679 Pkts.)
TX: 1.20 MB (3420 Pkts.)
IPv4: 192.168.1.35/24

Protocol: Static address

IPv4 address: 192.168.1.35

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers:

Accept router advertisements ☐

Send router solicitations ☑

IPv6 address:

IPv6 prefix length: 64

IPv6 gateway:

Figure 6-2 Common Configuration

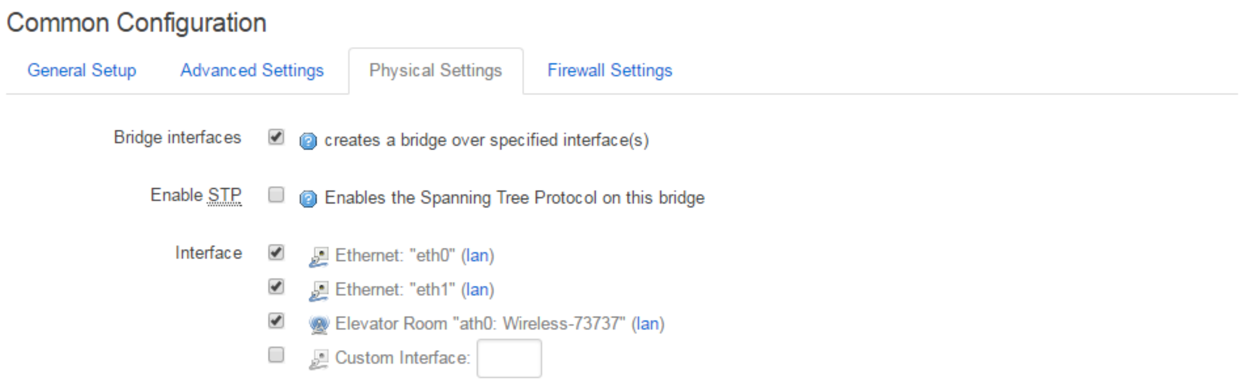
Protocol: the interface access IP address options, it divided into static address, DHCP client (to obtain the IP dynamically) and a variety of other ways. If you set a static IP, you need to set the IP, subnet mask, etc.; when set to DHCP client, the device can obtain IP from DHCP server automatically.

IPv4 address: IP address of this interface, you can configure it according to your own needs, but to ensure that IP cannot be the same as other devices in the same network, so as not to cause IP address conflict.

IPv4 netmask: the subnet mask of this interface, you can set it according to your own needs.

Use custom DNS server: It should be set to the value of the local DNS server.

Click on “Physical Settings” of the “Interface – LAN” page, you can modify the current interface configuration which contains the wired interface and wireless interface.



Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

Bridge interfaces ☑ creates a bridge over specified interface(s)

Enable STP ☐ Enables the Spanning Tree Protocol on this bridge

Interface
☑ Ethernet: "eth0" (lan)
☑ Ethernet: "eth1" (lan)
☑ Elevator Room "ath0: Wireless-73737" (lan)
☐ Custom Interface:

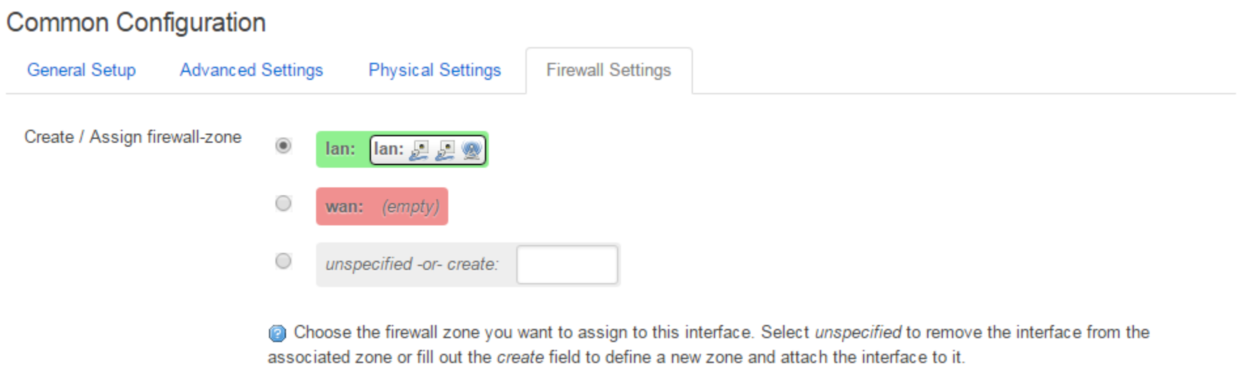
Figure 6-3 Physical settings

Bridge interfaces: creates a bridge over specified interface(s). Unchecking the Bridge interfaces and you could only choose one interface.

Enable STP: Enables the Spanning Tree Protocol on this bridge

Interface: Ethernet adapter "eth0" corresponds to the POE power supply LAN port of the device, Ethernet adapter "eth1" corresponds to the other two LAN port of the device.

Click to enter the firewall settings page. Choose the firewall zone you want to assign to this interface. Select unspecified to remove the interface from the associated zone or fill out the create field to define a new zone and attach the interface to it. Please refer to the Manual Section 6.4 firewall.



Common Configuration

General Setup | Advanced Settings | Physical Settings | Firewall Settings

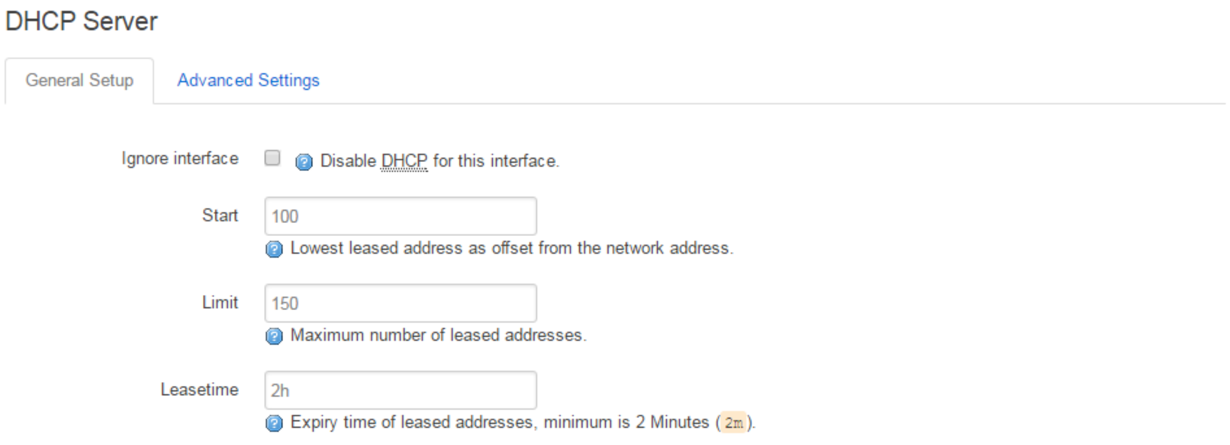
Create / Assign firewall-zone
● lan: lan:
○ wan: *(empty)*
○ *unspecified -or- create:*

Choose the firewall zone you want to assign to this interface. Select *unspecified* to remove the interface from the associated zone or fill out the *create* field to define a new zone and attach the interface to it.

Figure 6-4 Firewall Settings

6.1.2 DHCP Server

Drop down the interface page, you can see the basic settings of the DHCP server.



DHCP Server

Ignore interface □ Disable DHCP for this interface.

Start: 100
Lowest leased address as offset from the network address.

Limit: 150
Maximum number of leased addresses.

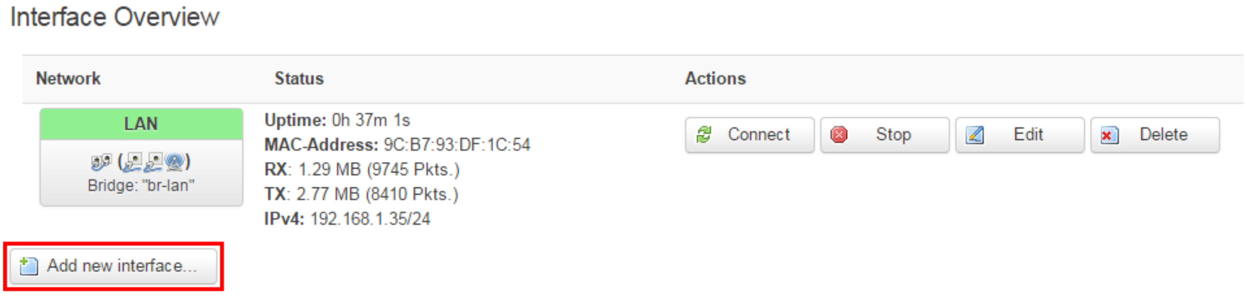
Leasetime: 2h
Expiry time of leased addresses, minimum is 2 Minutes (2m).

Figure 6-5 DHCP Server

DHCP: Assign IP address to client device, such as phones, laptops etc. A device should enable DHCP client mode to get IP automatically.

6.1.3 Add New Interface

Click on the “Add new interface” button to add a new interface.

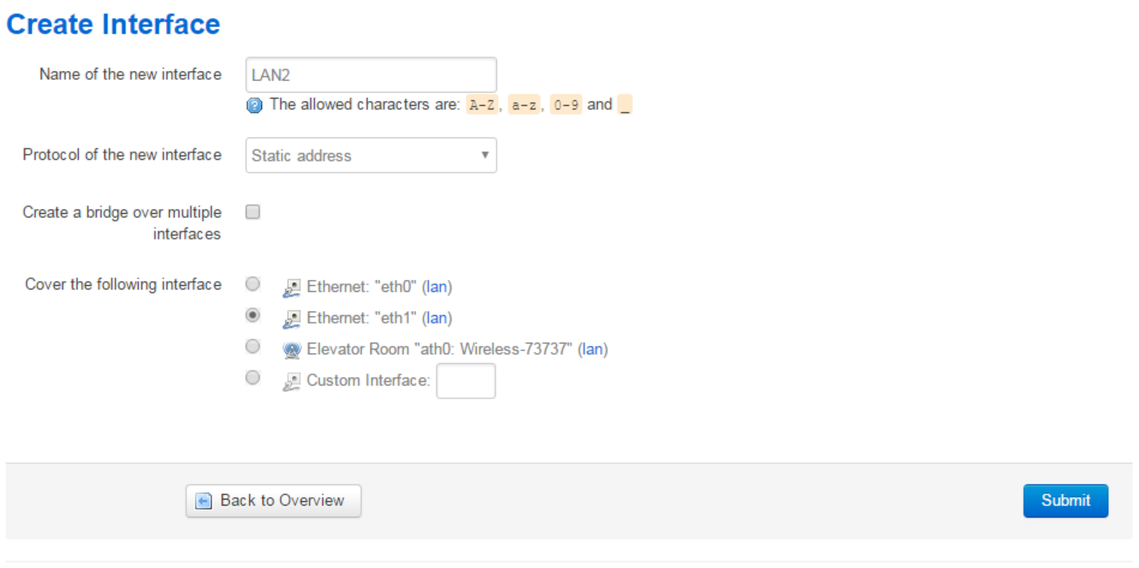


Interface Overview

Network	Status	Actions
LAN Bridge: "br-lan"	**Uptime:** 0h 37m 1s **MAC-Address:** 9C:B7:93:DF:1C:54 **RX**: 1.29 MB (9745 Pkts.) **TX**: 2.77 MB (8410 Pkts.) **IPv4:** 192.168.1.35/24	Connect Stop Edit Delete

Figure 6-6 Add new interface

Fill in the name of the new interface, such as LAN2, select the Ethernet adapter eth1 interface, all of the configuration in this page can be modified again in the subsequent pages.



Create Interface

Name of the new interface: LAN2

The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Static address

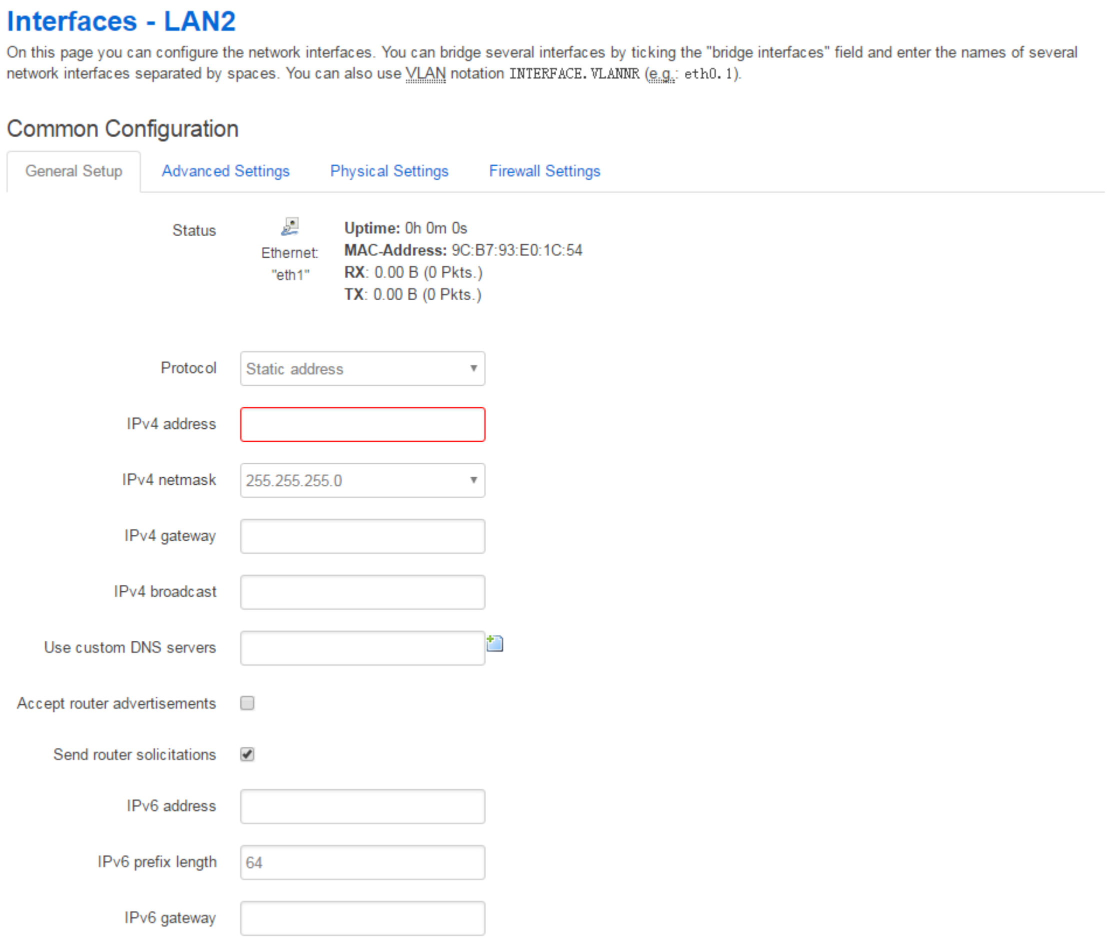
Create a bridge over multiple interfaces: □

Cover the following interface:

- ○ Ethernet: "eth0" (lan)
- ● Ethernet: "eth1" (lan)
- ○ Elevator Room "ath0: Wireless-73737" (lan)
- ○ Custom Interface:

Figure 6-7 Create Interface

Click Submit, will enter the new LAN2 interface configuration page. This page can be configured for all the existing interfaces, as shown below, you can still see the original LAN interface.



Interfaces - LAN2

On this page you can configure the network interfaces. You can bridge several interfaces by ticking the "bridge interfaces" field and enter the names of several network interfaces separated by spaces. You can also use VLAN notation INTERFACE.VLANNR (e.g.: eth0.1).

Common Configuration

Status: Ethernet: "eth1" **Uptime:** 0h 0m 0s **MAC-Address:** 9C:B7:93:E0:1C:54 **RX**: 0.00 B (0 Pkts.) **TX**: 0.00 B (0 Pkts.)

Protocol: Static address

IPv4 address:

IPv4 netmask: 255.255.255.0

IPv4 gateway:

IPv4 broadcast:

Use custom DNS servers:

Accept router advertisements: □

Send router solicitations: ☑

IPv6 address:

IPv6 prefix length: 64

IPv6 gateway:

Figure 6-8 Interfaces - LAN2

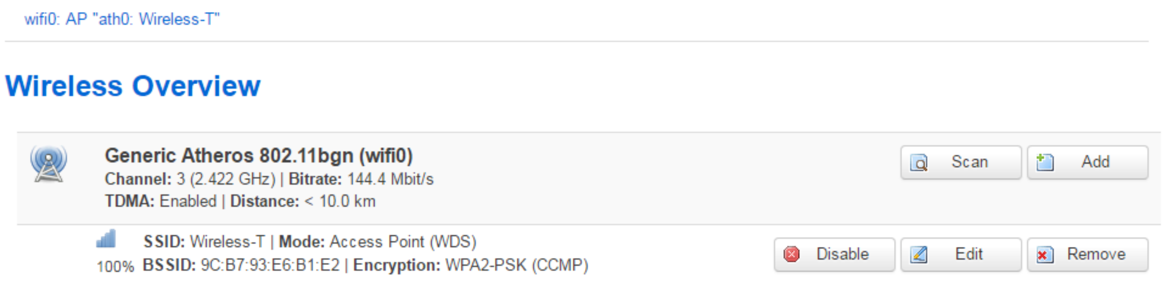
Please refer to chapter 6.1.1 to see how to configure the interface.

6.2 Wifi

6.2.1 Device Configuration

The Device Configuration section covers physical settings of the radio hardware such as channel, transmit power.

Open the Network -> Wifi page, you will see the current wireless profile and the information of associated stations.



wifi0: AP "ath0: Wireless-T"

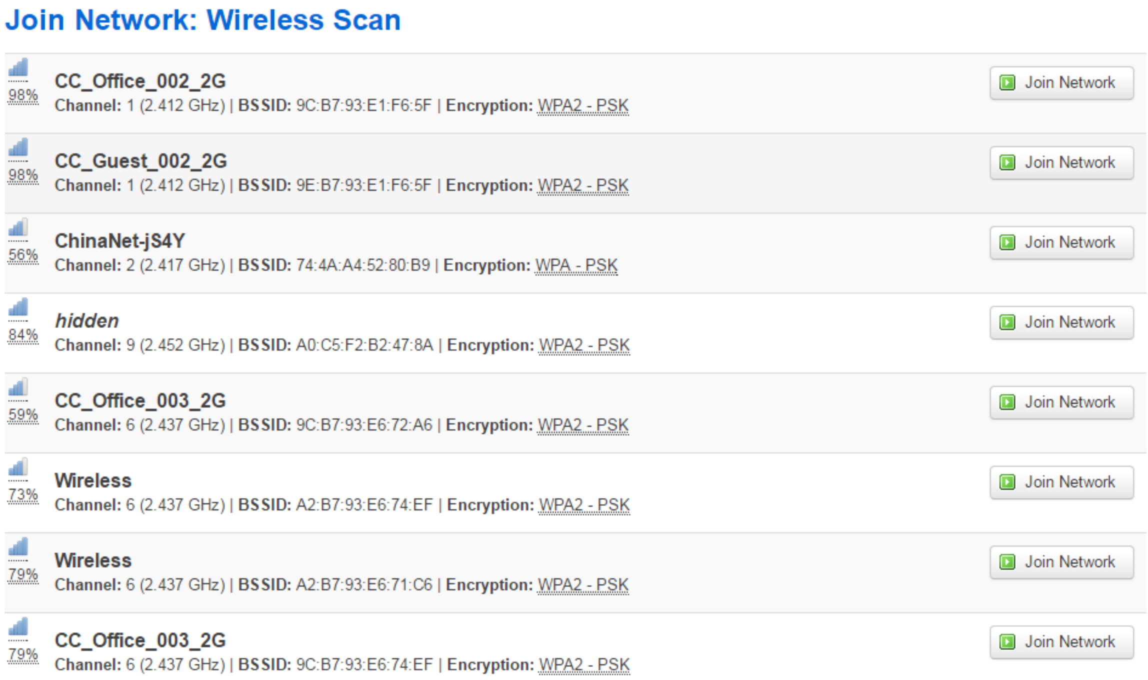
Wireless Overview

Generic Atheros 802.11bgn (wifi0)
Channel: 3 (2.422 GHz) | **Bitrate:** 144.4 Mbit/s
TDMA: Enabled | **Distance:** < 10.0 km

100% **SSID:** Wireless-T | **Mode:** Access Point (WDS)
BSSID: 9C:B7:93:E6:B1:E2 | **Encryption:** WPA2-PSK (CCMP)

Figure 6-9 Wireless Overview

The AP device and the CPE device can both scan nearby SSIDs and you can connect CPE device to the appropriate wireless network as needed.



Join Network: Wireless Scan

98% **CC_Office_002_2G**
Channel: 1 (2.412 GHz) | **BSSID:** 9C:B7:93:E1:F6:5F | **Encryption:** WPA2 - PSK

98% **CC_Guest_002_2G**
Channel: 1 (2.412 GHz) | **BSSID:** 9E:B7:93:E1:F6:5F | **Encryption:** WPA2 - PSK

56% **ChinaNet-jS4Y**
Channel: 2 (2.417 GHz) | **BSSID:** 74:4A:A4:52:80:B9 | **Encryption:** WPA - PSK

84% ***hidden***
Channel: 9 (2.452 GHz) | **BSSID:** A0:C5:F2:B2:47:8A | **Encryption:** WPA2 - PSK

59% **CC_Office_003_2G**
Channel: 6 (2.437 GHz) | **BSSID:** 9C:B7:93:E6:72:A6 | **Encryption:** WPA2 - PSK

73% **Wireless**
Channel: 6 (2.437 GHz) | **BSSID:** A2:B7:93:E6:74:EF | **Encryption:** WPA2 - PSK

79% **Wireless**
Channel: 6 (2.437 GHz) | **BSSID:** A2:B7:93:E6:71:C6 | **Encryption:** WPA2 - PSK

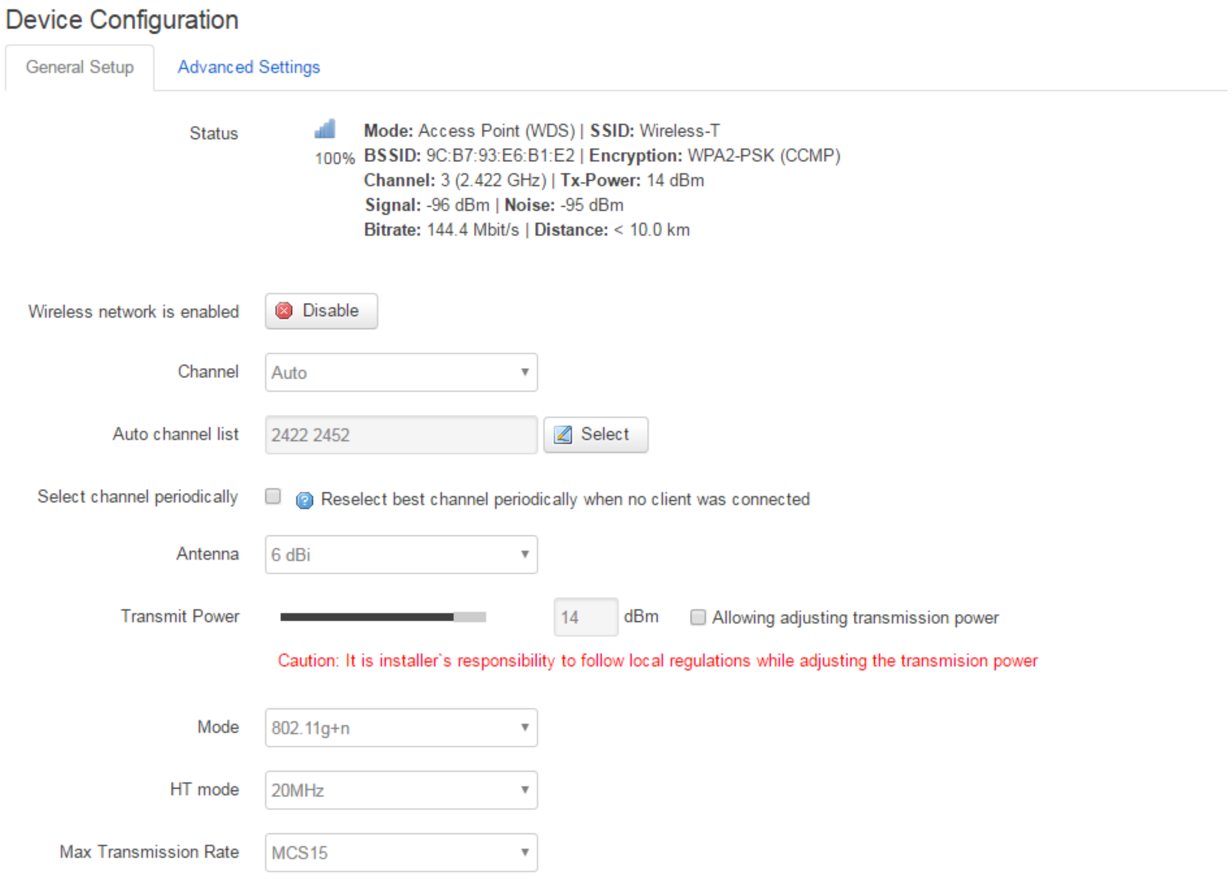
79% **CC_Office_003_2G**
Channel: 6 (2.437 GHz) | **BSSID:** 9C:B7:93:E6:74:EF | **Encryption:** WPA2 - PSK

Figure 6-10 Join Network: Wireless Scan

Click the SSID your CPE device need, if you check "Replace the wireless configuration", click on the Confirmation will cover all current wireless template settings, please choose carefully.

When the device has been added 8 wireless profiles, or there is a client mode wireless profile in the 8 profiles, click on Join Network will appear “The hardware is Max. 8 multi-SSID capable and only 1 client capable and existing configuration will be replaced if you proceed.”, the device can add up to eight wireless profiles, and the device can only have one client mode profile, you can choose to enable or disable the added wireless profiles.

Click the Edit button, you can enter the wireless configuration page. The basic settings page as shown below.



Device Configuration

Status: 100% **Mode:** Access Point (WDS) | **SSID:** Wireless-T
BSSID: 9C:B7:93:E6:B1:E2 | **Encryption:** WPA2-PSK (CCMP)
Channel: 3 (2.422 GHz) | **Tx-Power:** 14 dBm
Signal: -96 dBm | **Noise:** -95 dBm
Bitrate: 144.4 Mbit/s | **Distance:** < 10.0 km

Wireless network is enabled: Disable

Channel: Auto

Auto channel list: 2422 2452 Select

Select channel periodically: □ Reselect best channel periodically when no client was connected

Antenna: 6 dBi

Transmit Power: 14 dBm □ Allowing adjusting transmission power

Caution: It is installer`s responsibility to follow local regulations while adjusting the transmision power

Mode: 802.11g+n

HT mode: 20MHz

Max Transmission Rate: MCS15

Figure 6-11 General Setup

Channel: The channel can be modified when the device is configured to AP mode. The device can only work on one channel at the same time.

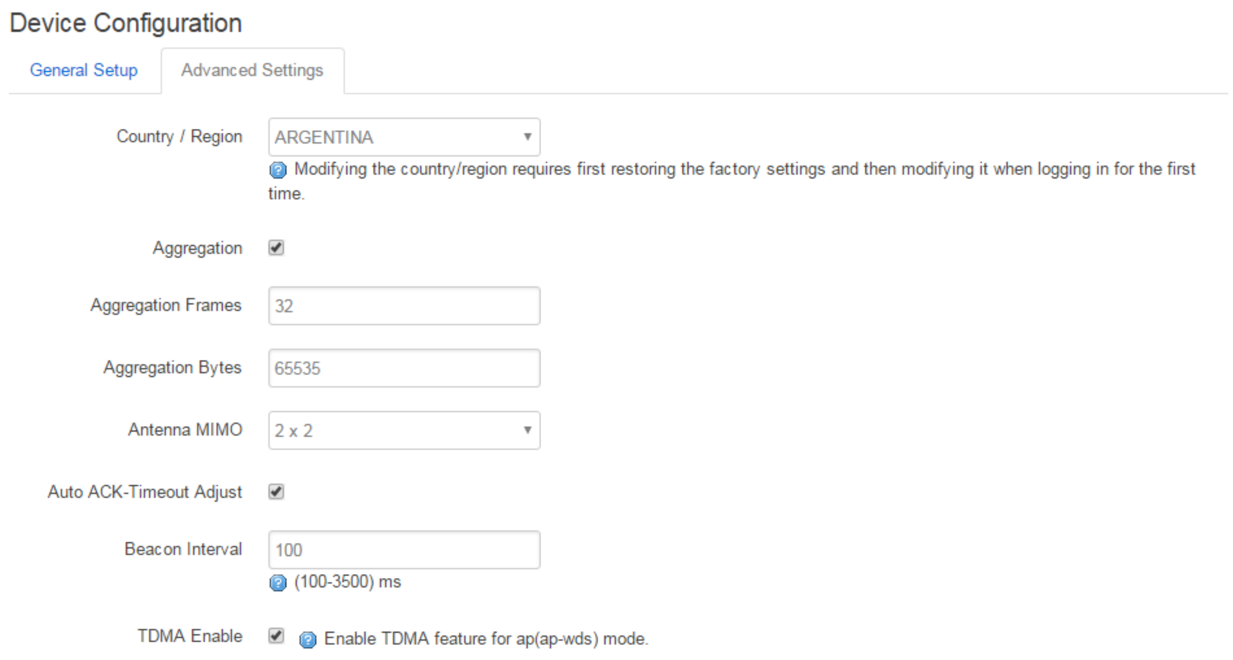
Transmit Power: The device output power. When the output power is increased, the signal distance and signal strength will be improved.

Mode: You can keep the default 802.11g+n mode to guarantee optimal transmission rate.

HT Mode: Channel width selection, the device supports 20/40MHz bandwidth. In general, the wider the bandwidth is, the greater the data throughput rate.

Max Transmission Rate: It can be used to limit the max transmission rate of a device.

Click on Device Configuration->Advanced Settings, you can configure the advanced settings of the device in this section.



Device Configuration

Country / Region: ARGENTINA ▾

Modifying the country/region requires first restoring the factory settings and then modifying it when logging in for the first time.

Aggregation: ☑

Aggregation Frames: 32

Aggregation Bytes: 65535

Antenna MIMO: 2 x 2 ▾

Auto ACK-Timeout Adjust: ☑

Beacon Interval: 100

(100-3500) ms

TDMA Enable: ☑ Enable TDMA feature for ap(ap-wds) mode.

Figure 6-12 Advanced Settings

Country Code： Different countries allows different channels, you can choose the country code to allow the device works at the channels only permitted in the particular country. When you set Compliance Test mode, the frequency will extend to 2312-2732 MHz.

Aggregation: It enables several data frames of 802.11 to be aggregated and transmitted out, thus improve the throughput. The larger the set value, the higher the throughput.

TDMA：

Currently, most of the outdoor bridge products are developed based on 802.11 protocols, however, it has the limitations of short-distance, hidden node problems, and poor point-to-multi-point performance.

VTrans technologies utilizes a series of advanced technologies such as TDMA, intelligent rate control, Auto ACK Time-out Adjust, having the advantage of long transmission range, high date rate and robust transmission.

VTrans technology solves the problems of hidden-node problem in the 802.11 network infra-structure. Intelligent rate control algorithm can be adapted to quick channel quality variations, while stabilize the wireless throughput, thus suitable for long-distance transmission. ACK Time-out Auto Adjust can automatically detect the distances of the devices, and adjust the wireless parameters to achieve the best link quality.

To use the TDMA, the user needs to enable TDMA mode in the AP device, and set a priority level in the station device. When several stations are connected to one AP, different stations demand different throughput. If the station demands higher throughput, its priority level can be set to High, otherwise set to Low. When the client demands the same throughput, their priority level can be set to the same level.

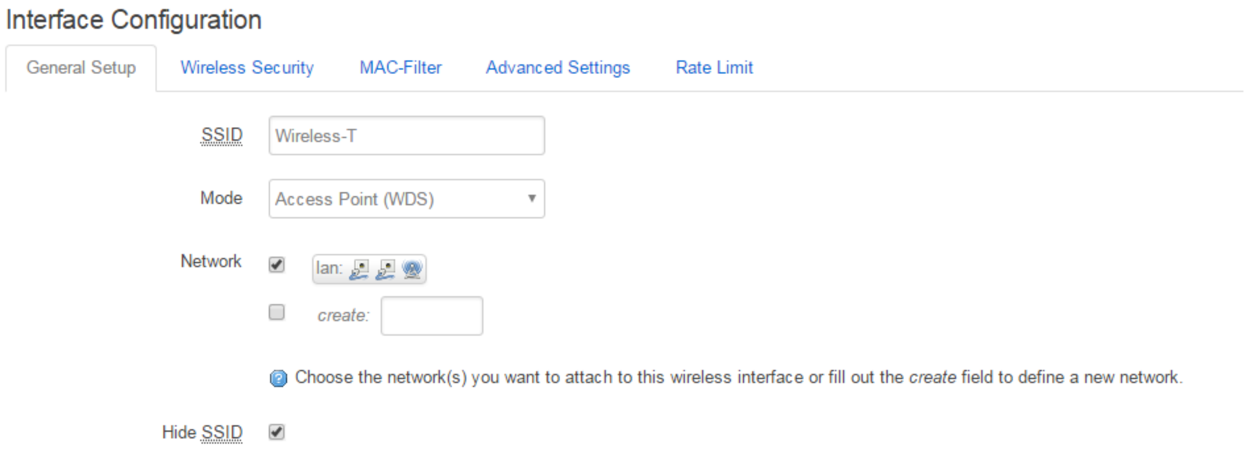
NOTE

- When using TDMA mode, the TDMA button need to be enabled at AP devices in the web-based configuration menu. The devices from other vendors cannot be connected to DS-3WF01C-2N in the TDMA mode. When TDMA is enabled, your phone or laptop cannot be able to connect to the device.

Auto ACK-Timeout Adjust： It is suggested to enable this function, so that the distance between 2 devices can be detected and all the related parameters can be optimized to achieve the best link quality.

6.2.2 Interface Configuration

Per network settings like encryption or operation mode are grouped in the Interface Configuration.



Interface Configuration

SSID: Wireless-T

Mode: Access Point (WDS)

Network: ☑ lan:

☐ *create:*

Choose the network(s) you want to attach to this wireless interface or fill out the *create* field to define a new network.

Hide SSID: ☑

Figure 6-13 Interface Configuration – General Setup

SSID: Name of a wireless. It is used to control the access to the wireless network, only the same SSID can communicate with each other to establish a local area network.

Mode: There are totally 4 wireless modes, including: Client, Access Point, Client (WDS) and Access Point (WDS).

Access Point: Access point.

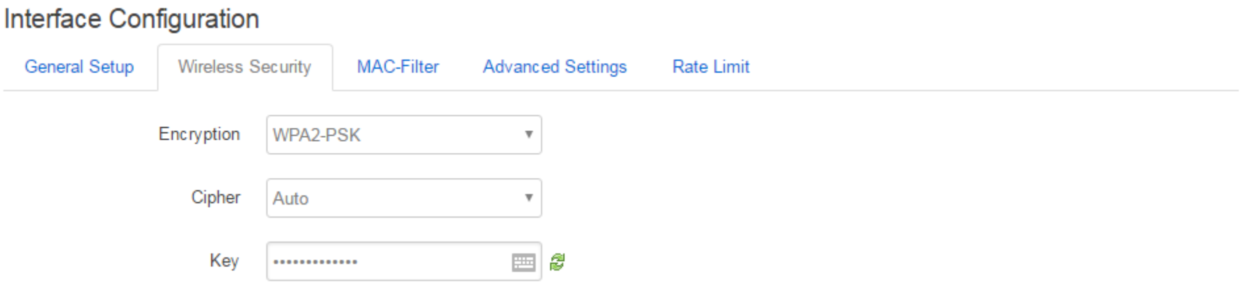
Client: A client device that can connect to an AP.

Client (WDS): Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. Client (WDS) means this device is a client in WDS mode.

Access Point (WDS)： Use WDS feature to link multiple APs in a network, all associated stations from any AP can communicate with each other like in ad-hoc mode. WDS AP means this device is an AP in WDS mode.

Network: Choose the network(s) you want to attach to this wireless interface or fill out the create field to define a new network.

Hide SSID: to hide the broadcast name of the wireless network to avoid being connected to others. Check this function; others will not be able to search the SSID.



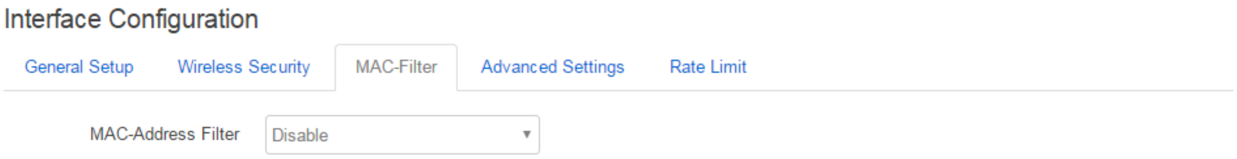
Encryption: WPA2-PSK

Cipher: Auto

Key: •••••••••••••

Figure 6-14 Interface Configuration – Wireless Security

Security: User can set the security based on needs to guarantee the wireless security. The wireless encryption of the device to be connected to each other must be set to the same encryption.



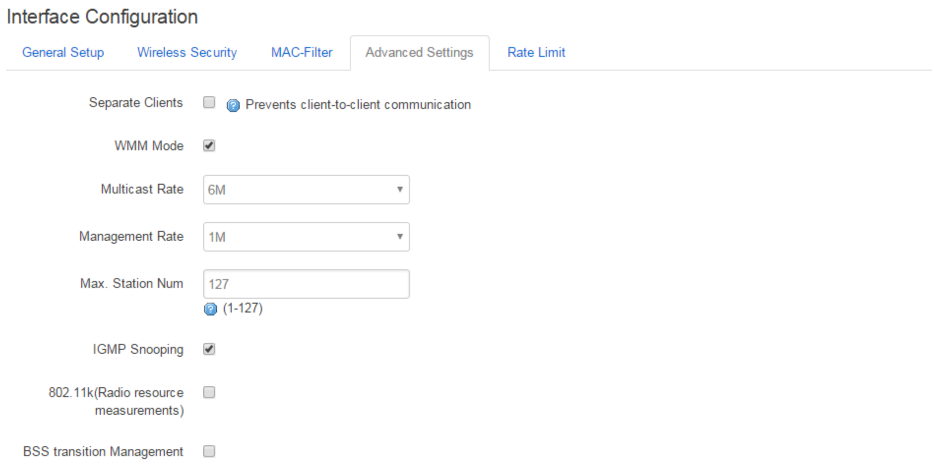
MAC-Address Filter: Disable

Figure 6-15 MAC Filter

MAC - Address Filter: used to control communication between the device and other devices.

Allow listed only: only the list of devices that are allowed to connect to the access point and the other device does not allow access to the access point.

Allow all except listed: allow the device to connect to the access point outside the list, and the other device does not allow access to the access point.



Interface Configuration

Separate Clients □ Prevents client-to-client communication

WMM Mode ☑

Multicast Rate 6M

Management Rate 1M

Max. Station Num 127
(1-127)

IGMP Snooping ☑

802.11k(Radio resource measurements) □

BSS transition Management □

Figure 6-16 Interface Configuration – Advanced Settings

Separate Clients: Enable this function to prevent devices connected to the same access point AP from communicating with each other. Even if the IP of each client is duplicated, there will be no impact on communication. This feature only exists in access point mode.

WMM Mode: Check to speed up Wi-Fi multimedia.

Multicast Rate: The transmission rate in a wireless multicast communication system.

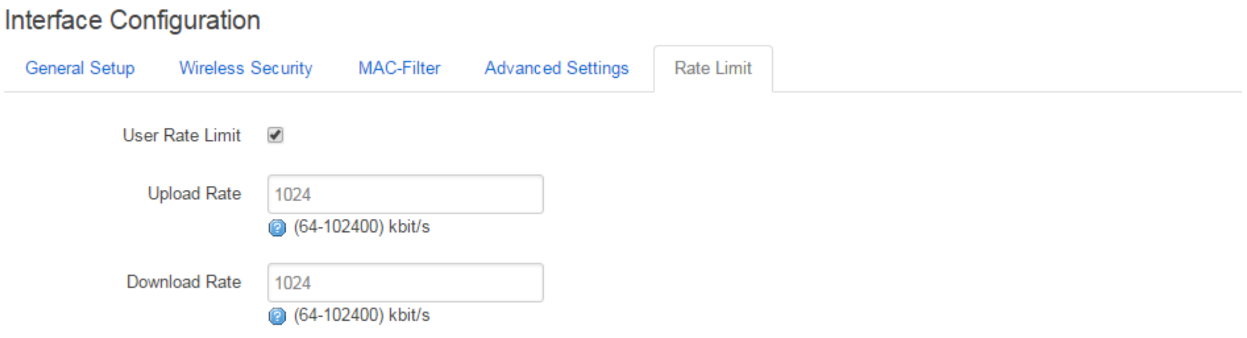
Management Rate: The transmission rate of the management frame.

Max. Station Num: Set it to limit the number of clients and clients (WDS) connected to the access points, access points (WDS).

IGMP snooping: The device analyzes the received IGMP messages to establish a mapping relationship between the port and the MAC multicast address, and forwards the multicast data according to the mapping relationship. When the device is not running IGMP snooping, the multicast data is broadcast on Layer 2. After the device runs IGMP Snooping, the multicast data is not broadcast on Layer 2 and is multicast to the specified receiver on Layer 2.

802.11k: 802.11k provides a standard for how wireless LANs should perform channel selection, roaming services, and transmission power control. It provides wireless resource management, allowing the frequency band, channel, carrier and other flexible and dynamic adjustment and scheduling, so that the limited frequency band can be improved in overall application efficiency. Within a wireless LAN, each device is typically connected to an access point that provides the strongest signal. This management can sometimes lead to excessive demand for one access point and reduce the utilization of other access points, resulting in lower performance of the entire network, which is mainly determined by the number of access users and geographical location. In a network that complies with the 802.11k specification, if the access point with the strongest signal is loaded with its maximum capacity and a wireless device is connected to a lower utilization access point, in this case even its signal it may be weak, but the overall throughput is still relatively large, because network resources are used more efficiently.

BSS transition Management: Migration management between basic service sets.



Interface Configuration

User Rate Limit ☑

Upload Rate: 1024
(64-102400) kbit/s

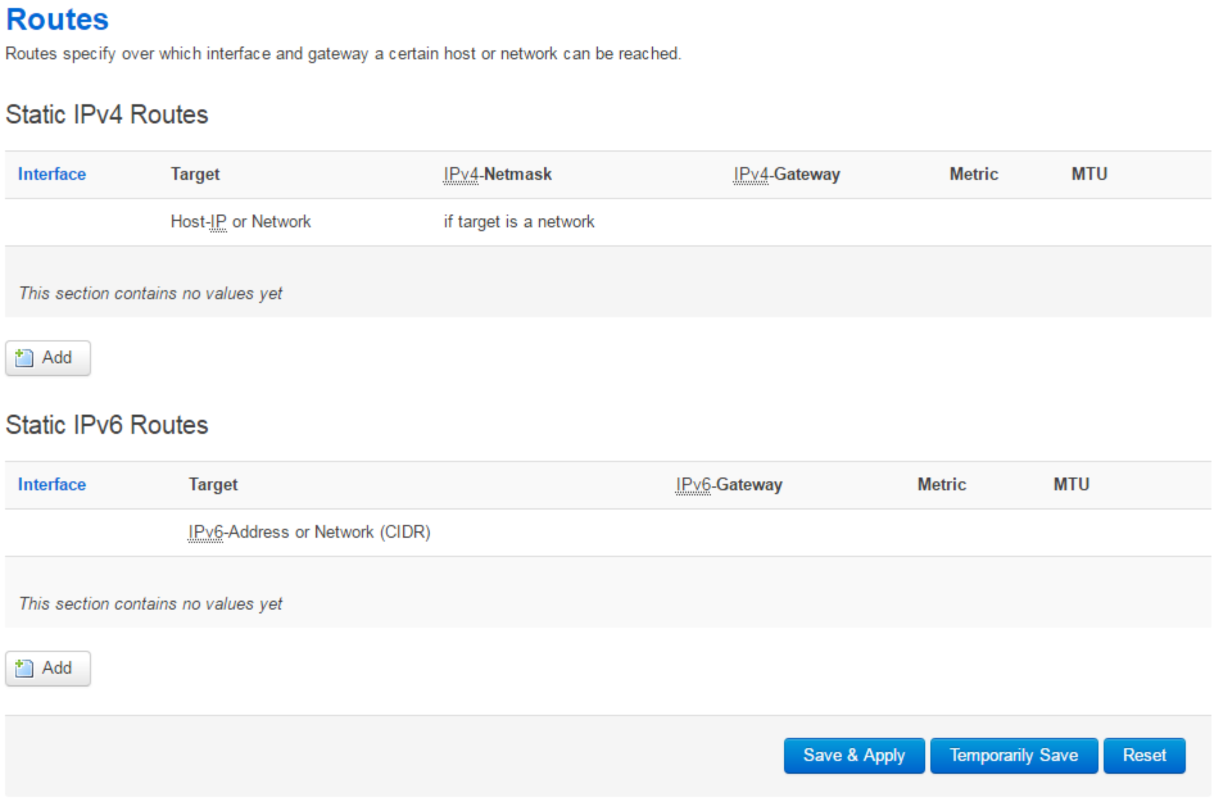
Download Rate: 1024
(64-102400) kbit/s

Figure 6-17 Rate Limit

Rate Limit: the rate limit for each user.

6.3 Static Routes

This feature allows you to set up a static route. The routing table describes the reachable path of the packet.



Routes

Routes specify over which interface and gateway a certain host or network can be reached.

Static IPv4 Routes

Interface	Target	IPv4-Netmask	IPv4-Gateway	Metric	MTU
	Host-IP or Network	if target is a network			

This section contains no values yet

Static IPv6 Routes

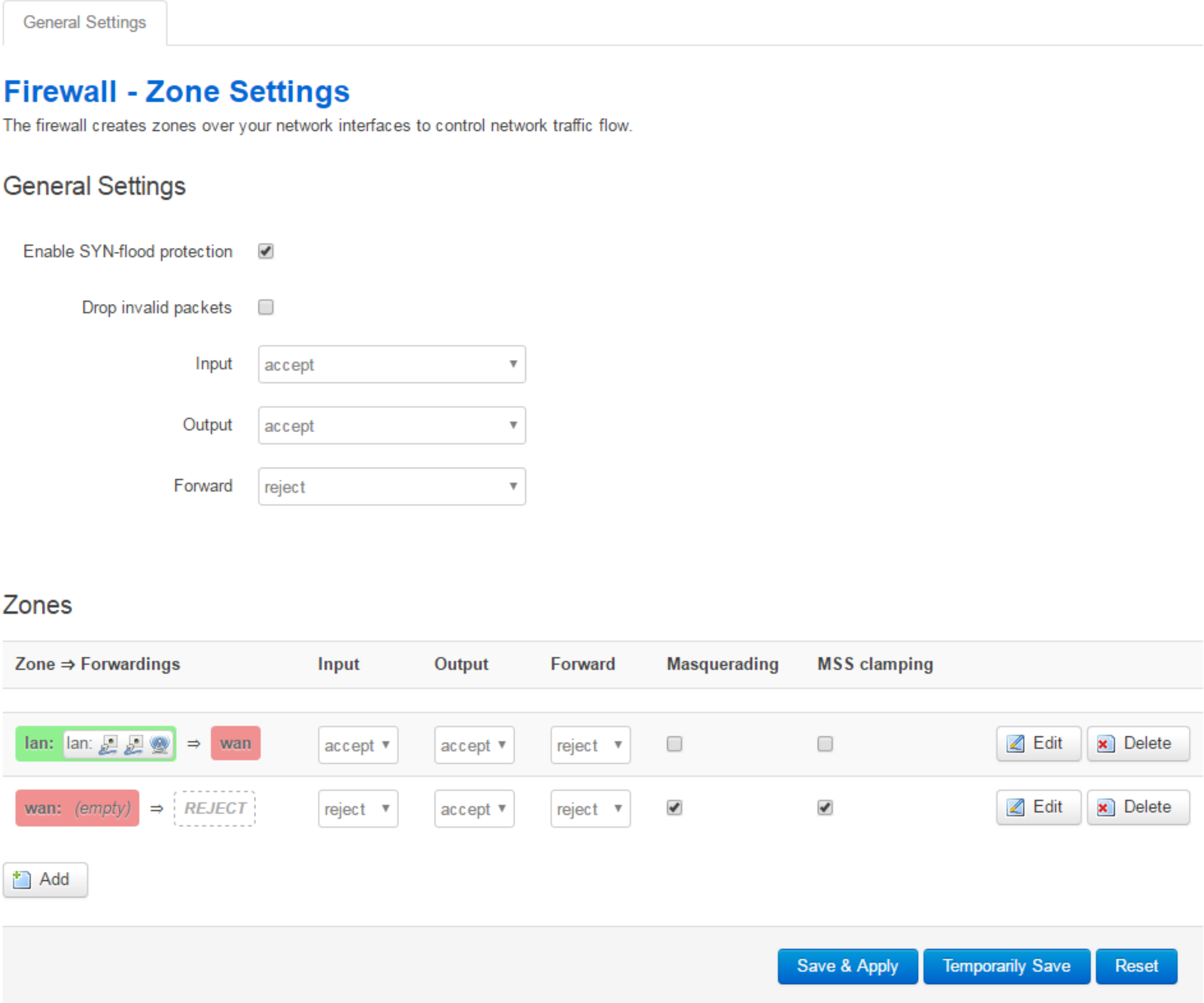
Interface	Target	IPv6-Gateway	Metric	MTU
	IPv6-Address or Network (CIDR)			

This section contains no values yet

Figure 6-18 Static Routes

6.4 Firewall

The firewall creates zones over your network interfaces to control network traffic flow. The default settings of firewall zone as shown below.



Firewall - Zone Settings

The firewall creates zones over your network interfaces to control network traffic flow.

General Settings

Enable SYN-flood protection ☑

Drop invalid packets ☐

Input: accept

Output: accept

Forward: reject

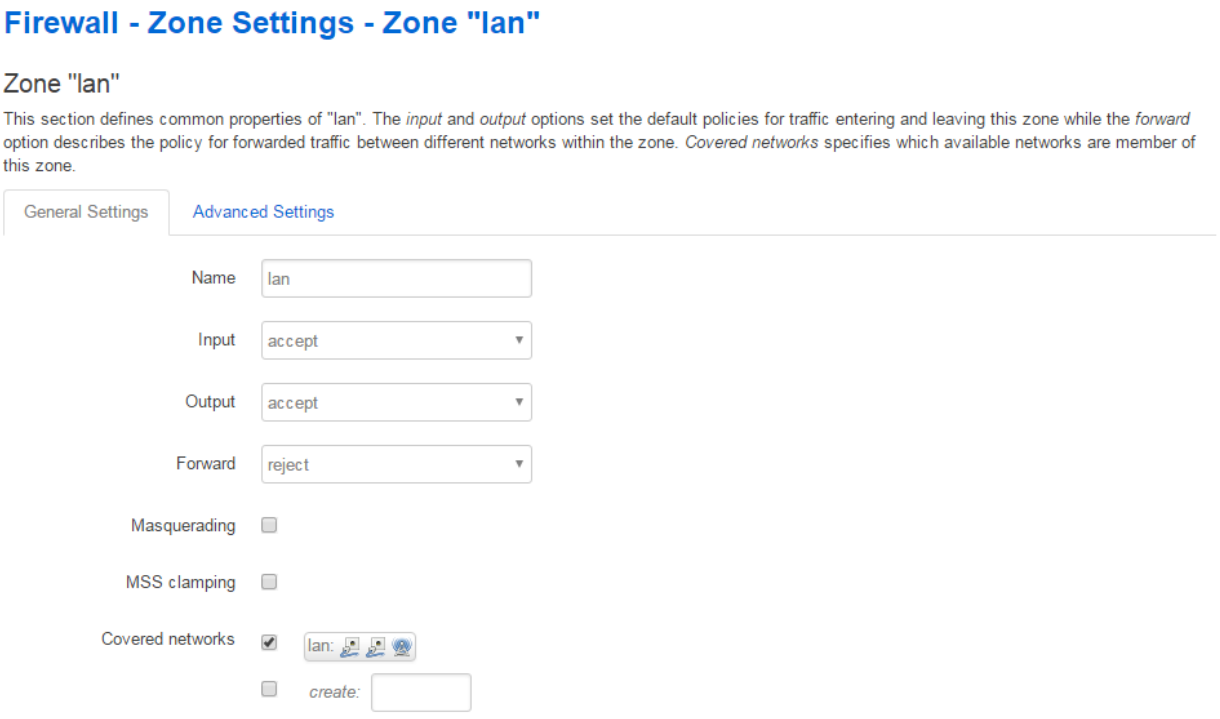
Zones

Zone ⇒ Forwardings	Input	Output	Forward	Masquerading	MSS clamping	
lan: lan: ⇒ wan	accept	accept	reject	☐	☐	Edit Delete
wan: (empty) ⇒ REJECT	reject	accept	reject	☑	☑	Edit Delete

Figure 6-19 Firewall - Zone Settings

Click "modify" or "add" to define the generic properties of the zone. In the port trigger section, the forwarding rules for the current area and other areas can be modified.

For example, click on Edit button of LAN zone; as shown below, this section defines common properties of "lan". The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. A covered network specifies which available networks are member of this zone.



Firewall - Zone Settings - Zone "lan"

Zone "lan"

This section defines common properties of "lan". The *input* and *output* options set the default policies for traffic entering and leaving this zone while the *forward* option describes the policy for forwarded traffic between different networks within the zone. *Covered networks* specifies which available networks are member of this zone.

Name: lan

Input: accept

Output: accept

Forward: reject

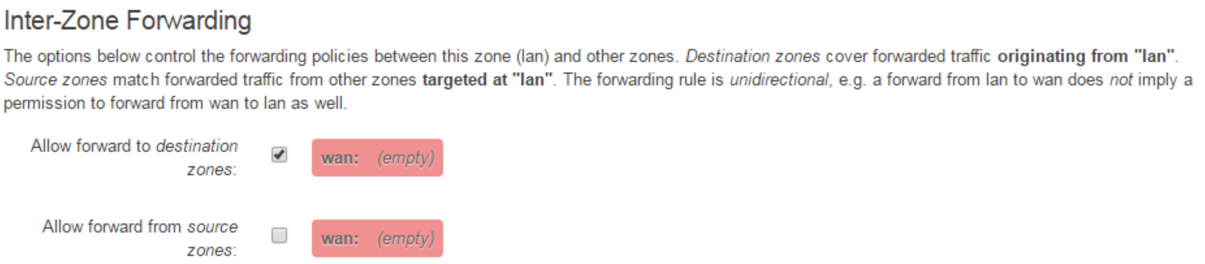
Masquerading: □

MSS clamping: □

Covered networks: ☑ lan:
□ *create:*

Figure 6-20 Firewall - Zone Settings - Zone "lan"

The options below control the forwarding policies between this zone (lan) and other zones. Destination zones cover forwarded traffic originating from "lan". Source zones match forwarded traffic from other zones targeted at "lan". The forwarding rule is unidirectional, e.g. a forward from lan to wan does not imply a permission to forward from wan to lan as well.



Inter-Zone Forwarding

The options below control the forwarding policies between this zone (lan) and other zones. *Destination zones* cover forwarded traffic **originating from "lan"**. *Source zones* match forwarded traffic from other zones **targeted at "lan"**. The forwarding rule is *unidirectional*, e.g. a forward from lan to wan does *not* imply a permission to forward from wan to lan as well.

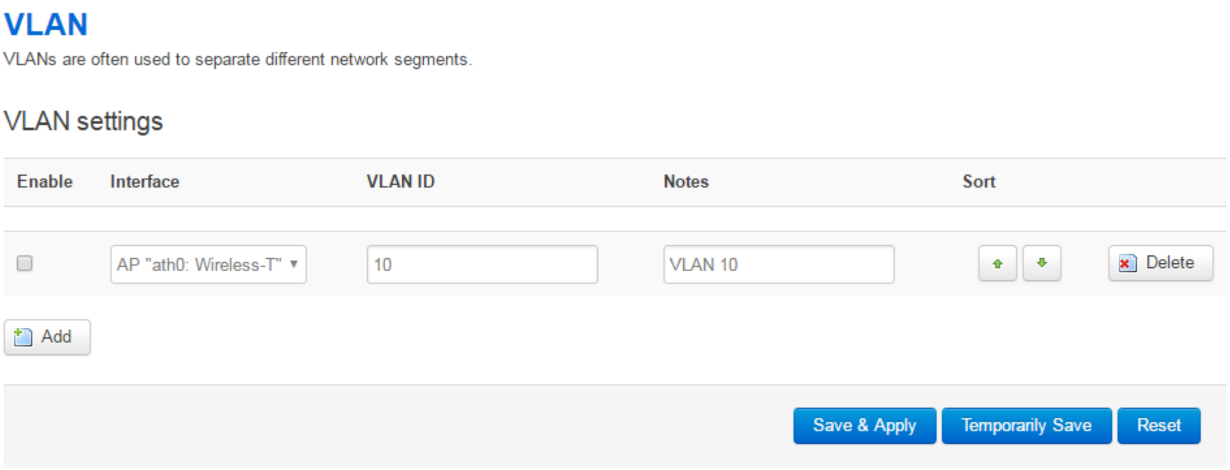
Allow forward to *destination zones*: ☑ **wan:** *(empty)*

Allow forward from *source zones*: □ **wan:** *(empty)*

Figure 6-21 Inter-Zone Forwarding

6.5 VLAN

VLANs are often used to separate different network segments. The VLAN function allows user to create multiple virtual local area network. As shown in figure, we add a VLAN on port ath0 (wireless network port). The VLAN ID is 10. The range of VLAN ID is 2~4094. Each VLAN ID represents a different VLAN.



VLAN

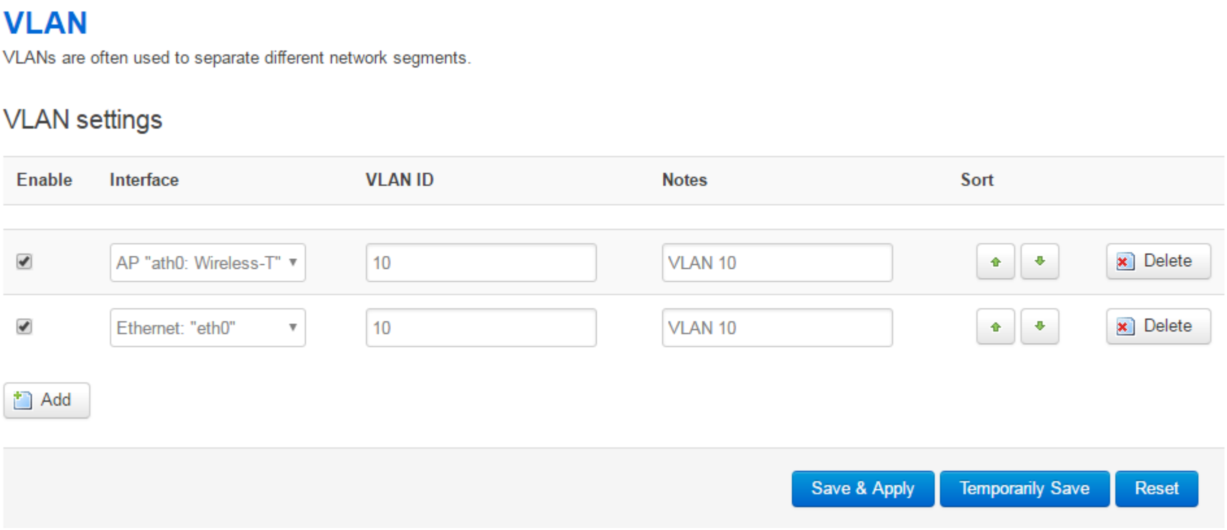
VLANs are often used to separate different network segments.

VLAN settings

Enable	Interface	VLAN ID	Notes	Sort
☐	AP "ath0: Wireless-T"	10	VLAN 10	

Figure 6-22 VLAN settings

Bridge function is needed to use together with VLAN. As show below, we add VLAN 10 on port eth0 and ath0, they are eth0.10 and ath0.10



VLAN

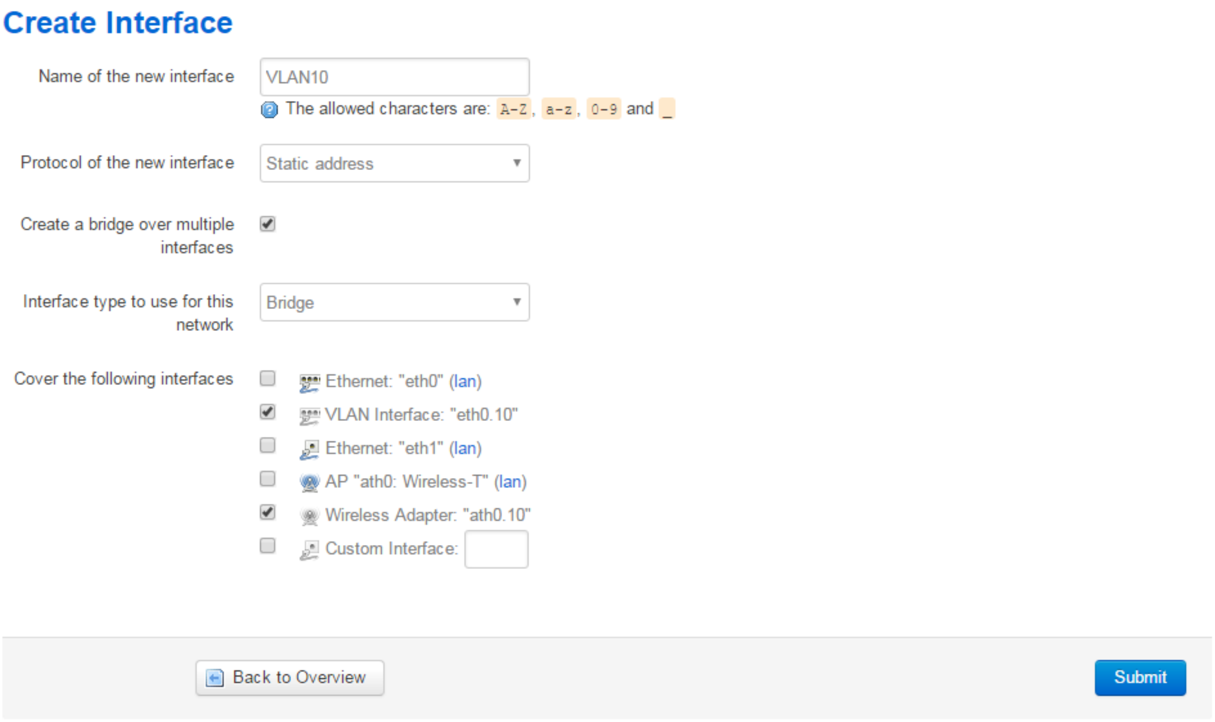
VLANs are often used to separate different network segments.

VLAN settings

Enable	Interface	VLAN ID	Notes	Sort
☑	AP "ath0: Wireless-T"	10	VLAN 10	
☑	Ethernet: "eth0"	10	VLAN 10	

Figure 6-23 Add VLAN ID

Then we create a new interface and put eth0.10 and ath0.10 into the same bridge in Network->Interfaces page as shown below.



Create Interface

Name of the new interface: VLAN10

The allowed characters are: A-Z, a-z, 0-9 and _

Protocol of the new interface: Static address

Create a bridge over multiple interfaces: ☑

Interface type to use for this network: Bridge

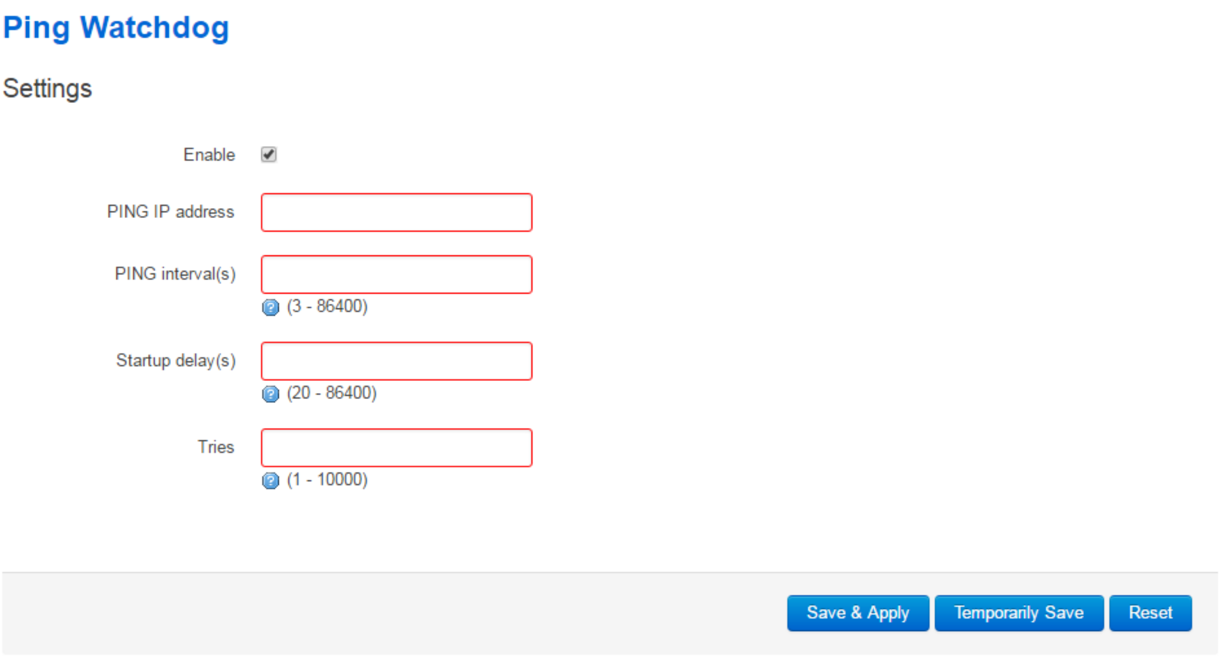
Cover the following interfaces:
- □ Ethernet: "eth0" (lan)
- ☑ VLAN Interface: "eth0.10"
- □ Ethernet: "eth1" (lan)
- □ AP "ath0: Wireless-T" (lan)
- ☑ Wireless Adapter: "ath0.10"
- □ Custom Interface:

Figure 6-24 Binding VLAN Interfaces

The packets from eth0.10 or ath0.10 will be added a VLAN label which ID is 10. That requires: the opposite wireless connection side must support VLAN 10, the device which connects with eth0 is also need to support VLAN 10 (such as a VLAN Switch).

6.6 Ping Watchdog

Ping Watchdog： The ping watchdog sets the Device to continuously ping a user-defined IP address (for example, it can be the IP address of the AP the Client is connecting to). If it is unable to ping under the user defined constraints, the device will automatically reboot. It is highly recommended that users enable this feature at the side of “CPE” and disable this feature at the side of “AP”.


Ping Watchdog

Settings

Enable ☑

PING IP address

PING interval(s)
(3 - 86400)

Startup delay(s)
(20 - 86400)

Tries
(1 - 10000)

Figure 6-25 Ping Watchdog

Ping IP Address： Specify an IP address of the target which will be monitored by Ping Watchdog. If this feature is enabled at the side of “CPE”, Ping IP Address should be the IP address of the AP the Client is connecting to.

Ping Interval： Specify time interval (in seconds) between the pings requests are sent by the Ping Watchdog

Startup Delay: specify initial time delay (in seconds) until first ping request is sent by the Ping Watchdog

Tries： Specify the number of ping replies. If the specified number of ping replies is not received continuously, the Ping Watchdog will reboot the device.

NOTE

- If users want to modify the parameters of Ping Watchdog, please disable it first and then apply. When the web page shows that Ping Watchdog is really disabled, users can now re-enable it with modified parameters.

Chapter 7 Logout

Click the logout button, it will logout the device and return to the login page.

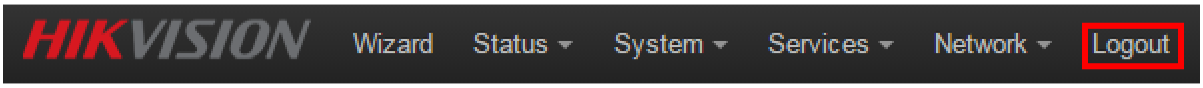


Figure 7-1 Logout

See Far, Go Further