



EKSELANS BY ITS

# USER MANUAL

## TR2200

### 331001

Access point 2.4 / 5GHz. 2200Mbps  
(400+900Mbps+900Mbps), 27dBm, 2 ports,  
PoE 48V. Wave2. High concurrency

V02

# TABLE OF CONNTENS

Introduction.....	6
Description:.....	6
Content:.....	6
Interfaces, connection and access to the computer.....	6
Interfaces:.....	6
Connection:.....	7
Access to the equipment: .....	7
Interface in AP mode .....	8
Home: Status.....	8
Operation Mode: Change Mode.....	9
Setting Ap mode.....	10
Setting Gateway mode.....	11
Setting the Repeater mode.....	12
Setting Wisp mode.....	14
Wi-Fi Settings.....	15
2.4G Wi-Fi.....	15
5G Wi-Fi 1 and 2.....	16
MAC Access Control List (ACL).....	17
Advanced Config.....	19
Network Settings.....	21
LAN.....	21
VLAN.....	23
Management Options.....	23
Configure.....	23
Reboot.....	23
Modify password.....	23
Upgrade.....	24
Time.....	24
Log.....	24
Interface in Gateway mode.....	25

Home Status.....	25
Operation Mode Change Mode.....	25
Wi-Fi Settings:.....	25
2.4G Wi-Fi.....	25
5G Wi-Fi.....	25
MAC Access Control.....	25
Advanced Config.....	25
Network Settings.....	26
LAN.....	26
Static DHCP.....	28
VLAN.....	28
WAN.....	29
WAN Advanced Settings.....	30
URL Mapping.....	31
Security Settings.....	32
URL Filter.....	32
IP Filter.....	33
MAC Filter.....	35
Port Mapping.....	36
DMZ.....	38
Management Options.....	38
Configure.....	38
Reboot.....	38
Modify password.....	38
Upgrade.....	38
Time.....	38
Log.....	38
Flow control.....	39
IP group.....	41
Time group.....	42
DDNS configuration.....	43
Interface in Repeater mode.....	44
Home Status.....	44
Operation Mode Change Mode.....	44
Wi-Fi: Configuration.....	44
2.4G Wi-Fi.....	44
5G Wi-Fi.....	44



MAC Access Control .....	44
Advanced Config. ....	44
Repeater configuration. ....	45
Network Settings. ....	46
LAN. ....	46
VLAN. ....	46
Management Options .....	46
Configure. ....	46
Reboot. ....	46
Modify password. ....	46
Upgrade. ....	46
Time. ....	46
Log. ....	46
Interface in WISP mode. ....	47
Home: Status. ....	47
Operation Mode Change Mode. ....	47
Wi-Fi: Configuration. ....	47
2.4G Wi-Fi. ....	47
5G Wi-Fi. ....	47
MAC Access Control .....	47
Advanced Config. ....	47
Repeater configuration. ....	48
Network: Configuration. ....	49
LAN. ....	49
Static DHCP. ....	49
VLAN. ....	49
WAN. ....	49
WAN Advanced. ....	49
URL Mapping. ....	49
Security: Settings. ....	49
Url Filter. ....	49
IP Filter. ....	49
MAC Filter. ....	49
Port Mapping. ....	49
DMZ. ....	49
Administration: Options. ....	49
Configuration. ....	49

Reboot.....	49
Modify password.....	49
Upgrade.....	49
Time.....	49
Log.....	50
Flow Control.....	50
IP Group.....	50
Time Group.....	50
DDNS Settings.....	50
FAQ.....	51

## Introduction.

### Description:

Access point 2.4 / 5GHz. 1300Mbps (400+900Mbps), 27dBm, 2 ports, PoE 48V. Wave2. High concurrency.

### Content:

1. 1 X TR2200.
2. 1 X UTP cable.

## Interfaces, connection and access to the computer.

### Interfaces:

 <p>DC</p> <p>LED</p> <p>WAN POE</p> <p>LAN</p> <p>RESET</p>	<ul style="list-style-type: none"><li>• DC: Power supply 12V 2A.</li><li>• LED: WAN port status (bottom) and LAN (top).</li><li>• WAN POE: WAN port, POE 48V.</li><li>• LAN: LAN port.</li><li>• RESET: Button to perform factory reset. Press for 10 seconds.</li></ul>
---	--

### Connection:

- **AP Mode:** WAN port from AP to internet network. LAN port to the equipment that is intended to serve by LAN.
- **Gateway:** WAN port from AP to internet network. LAN port to the equipment that is intended to serve by LAN.
- **Repeater mode:** WAN or LAN port to the equipment that I intended to serve. Never connect to the client network where the repeater is getting signal.
- **WISP mode:** WAN or LAN port to the equipment that I intended to serve. Never connect to the client network where the repeater is getting signal.

If a 12V 2A power supply is not used, you can feed device by using a POE 48V injector connected to WAN port of device.

### Access to the equipment:

#### Method 1: The TR is not connected to the network.

To access the TR, follow these steps:

1. Connect to the TR with a network cable or wirelessly. By default, the wireless network are AP\_EK... Default password is 123456789.
2. Configure the pc's network adapter with a static IP as it appears in the image. To facilitate the configuration in EK we have the Ek NET Adapter application, with which we can easily configure the network adapter. It can be downloaded for free from <https://ek.plus/software/>, in the "EK NET ADAPTER" section.

General

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 . 188 . 200

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 1 . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternative DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

3. Open a web browser and go to the URL: <http://192.168.188.253>.
4. Password: admin.

## Method 2 The TR is connected to the NETWORK.

By default, the TR acquires an IP if there is a DHCP server on the network. To access and configure it, you can locate the IP through our controller, either through the physical device or the version installable on the pc (the CSW). The installable version can be located at the following link <https://www.ek.plus/product/csw/>.

## Interface in AP mode.

Home: Status.

We will be able to visualize the general information of the equipment and the Wi-Fi's. It will also allow us to see the equipment connected to the AP's.

1. Device information.
2. Current operating mode.
3. Network information (LAN).
4. Wi-Fi information (2G Wi-Fi). We can click on **'Number of Clients'** to see the connected computers and their MAC's.
5. Wi-Fi information (5G Wi-Fi). We can click on **'Number of Clients'** to see the connected computers and their MAC's.

## Operation Mode: Change Mode.

We will be able to select the mode in which we want the device to work. To make the changes you must click apply.

- **Change Mode:**
  - **Gateway Mode:** In this mode, it is assumed that the device connects to the Internet via ADSL/Cable Modem. NAT is enabled and PCs on the LAN ports share the same IP with the ISP over the WAN port. The connection type can be configured on the WAN page using PPPOE, DHCP Client, or Static IP.
  - **Repeater Mode:** In this mode, the user can access the wireless access point, the devices can be connected to another wireless network using wireless technology, all interfaces are united. No NAT, firewall, and all network-related features.
  - **WISP Mode:** In this mode, all ethernet ports are bridged and the wireless client will connect to the ISP access point. NAT is enabled and PCs on the ethernet port share the same IP with the ISP over the wireless LAN. You must first configure the wireless connection in client mode and connect to the ISP AP on the Site-Survey page. The connection type can be configured on the WAN page using PPPOE, DHCP client, and static IP.
  - **AP Mode:** In this mode, the wireless AP interface and the wired interface are joined. No NAT, firewall, and all network-related features.

Depending on the mode we select, different configurable options will appear.

### Setting Ap mode.

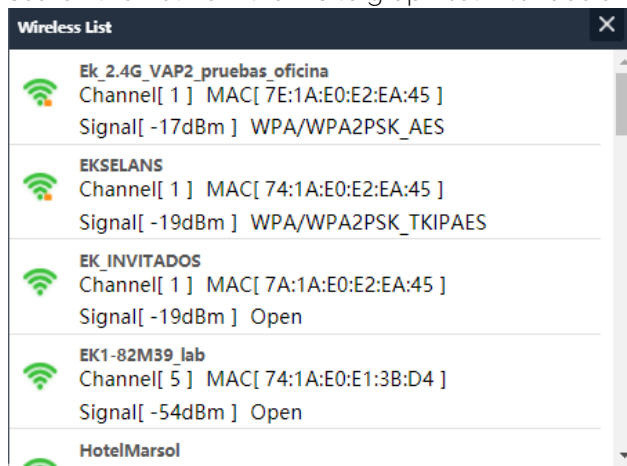
- LAN network configuration:
  - IP Mode:
    - **Static IP:** A management IP is configured statically.
    - **Get IP from AC:** The management IP is given by an EK controller.
    - **Get IP from the gateway:** The management IP is given by the Router installed on the client.
  - Lan IP: We set the desired static IP. **Only in 'static IP' IP mode.**
  - Subnet: We put the mask for the management IP. **Only in 'static IP' IP mode.**
  - Gateway: We select the gateway of the computer. **Only in 'static IP' IP mode.**
  - Primary DNS: The primary "Domain Name System" is selected. **Only in 'static IP' IP mode.**
  - Secondary DNS: The secondary "Domain Name System" is selected. **Only in 'static IP' IP mode.**
- 2G Wi-Fi configuration:
  - **Wi-Fi Status:** You can enable or disable the broadcast of 2G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M, 40M, 20M/40M) and the channel (1 to 13).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
- Wi-Fi /5G Wi-Fi configuration):
  - **Wi-Fi Status:** You can enable or disable the broadcast of 5G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M, 40M, 80M, 20M/40M, 20M/40M/80M) and the channel (36 to 140).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi Password:** Allows us to configure the password for the selected SSID.
- Timing: allows us to configure a scheduled restart.
  - **Reboot time:** We can schedule every day of the week or one in particular and one time for you to perform the restart.
  - **Restart interval:** Allows us to configure an interval of days for the computer to restart.

### Setting Gateway mode.

1. WAN network configuration:
  - **Internet mode:**
    - **Static IP:** We can assign a static IP to the WAN port.
    - **PPPoE:** We can configure a password user that has been configured on a PPPoE server that is in the configured installation.
    - **DHCP:** It is configured to automatically acquire the IP from the Client Router.
2. 2G Wi-Fi configuration:
  - **Wi-Fi Status:** You can enable or disable the broadcast of 2G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M, 40M, 20M/40M) and the channel (1 to 13).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
3. Wi-Fi /5G Wi-Fi configuration:
  - **Wi-Fi Status:** You can enable or disable the broadcast of 5G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M, 40M, 80M, 20M/40M, 20M/40M/80M) and the channel (36 to 140).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
4. Timing: allows us to configure a scheduled restart.
  - **Reboot time:** We can schedule every day of the week or one in particular and one time for you to perform the restart.
  - **Restart interval:** Allows us to configure an interval of days for the computer to restart.

## Setting the Repeater mode.

- Repeater settings:
  - **Select Network:** We must select the network band that we are going to repeat either 2G or 5G.
  - **Repeater SSID:** We select the SSID we want to repeat. We can use the SCAN button to search the network thanks to graphical interface and select it.



- **Lock BSSID:** You can close by MAC the configuration of the repeater. In this way if another issuer is configured with the SSID to repeat, not having the same MAC that we have blocked does not make the link.
- **Encryption:** Allows us to select the encryption mode or set it free if desired.
- **Password:** Allows us to configure the password for the selected SSID.
- **Bandwidth:** The desired bandwidth is configured, depending on the network we choose (2G or 5G) we can select some values or others.
- **P2P:** Allows you to propagate WDS configuration between terminals (It is recommended to disable it).
- LAN network configuration:
  - **IP mode:**
    - **Static IP:** A management IP is configured statically.
    - **Get IP from AC:** The management IP is given by an EK controller.
    - **Get IP from the gateway:** The management IP is given by the Router installed on the client.
  - **Lan IP:** We set the desired static IP. **Only in 'static IP' IP mode.**
  - **Subnet:** We put the mask for the management IP. **Only in 'static IP' IP mode.**
  - **Gateway:** We select the gateway of the computer. **Only in 'static IP' IP mode.**
  - **Primary DNS:** The primary "Domain Name System" is selected. **Only in 'static IP' IP mode.**
  - **Secondary DNS:** The secondary "Domain Name System" is selected. **Only in 'static IP' IP mode.**

- 2G Wi-Fi configuration:
  - **Wi-Fi Status:** You can enable or disable the broadcast of 2G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M,40M,20M/40M) and the channel (1 to 13).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
- Wi-Fi /5G Wi-Fi configuration):
  - **Wi-Fi Status:** You can enable or disable the broadcast of 5G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M,40M,80M,20M/40M,20M/40M/80M) and the channel (36 to 140).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
- Timing: allows us to configure a scheduled restart.
  - **Reboot time:** We can schedule every day of the week or one in particular and one time for you to perform the restart.
  - **Restart interval:** Allows us to configure an interval of days for the computer to restart.

### Setting Wisp mode.

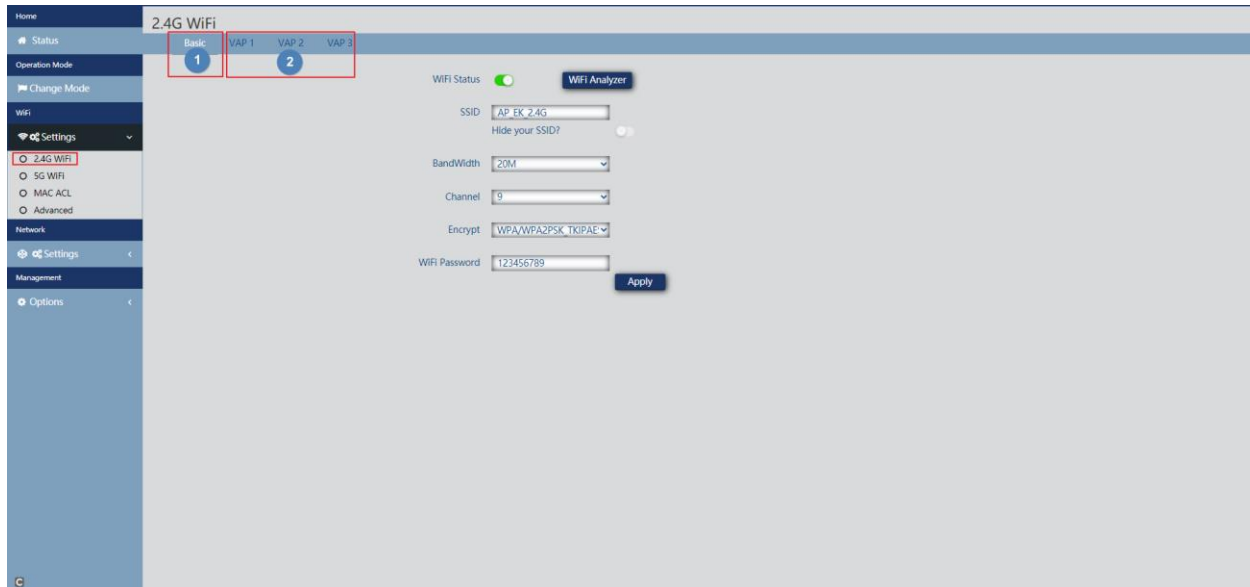
- Repeater configuration:
  - **Select Network:** We must select the network band that we are going to repeat either 2G or 5G.
  - **Repeater SSID:** We select the SSID we want to repeat.
  - **Lock BSSID:** You can close by MAC the configuration of the repeater. In this way if another issuer is configured with the SSID to repeat, not having the same MAC that we have blocked does not make the link.
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Password:** Allows us to configure the password for the selected SSID.
  - **Bandwidth:** The desired bandwidth is configured, depending on the network we choose (2G or 5G) we can select some values or others.
  - **P2P:** Allows you to propagate WDS configuration between terminals (It is recommended to disable it).
- WAN Network Configuration:
  - **Internet Mode:**
    - **Static IP:** We can assign a static IP to the WAN port.
    - **PPPoE:** We can configure a password user that has been configured on a PPPoE server that is in the configured installation.
    - **DHCP:** It is configured to automatically acquire the IP from the Client Router.
- 5. 2G Wi-Fi configuration:
  - **Wi-Fi Status:** You can enable or disable the broadcast of 2G Wi-Fi.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M, 40M, 20M/40M) and the channel (1 to 13).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
- 6. Wi-Fi /5G Wi-Fi configuration:
  - **Wi-Fi status:** You can enable or disable the broadcast of 5G Wi-Fi
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** Allows us to configure the width of the channel (20M, 40M, 80M, 20M/40M, 20M/40M/80M) and the channel (36 to 140).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.

7. Timing: allows us to configure a scheduled restart.
  - o **Reboot time:** We can schedule every day of the week or one in particular and one time for you to perform the restart.
  - o **Restart interval:** Allows us to configure an interval of days for the computer to restart.

## Wi-Fi Settings.

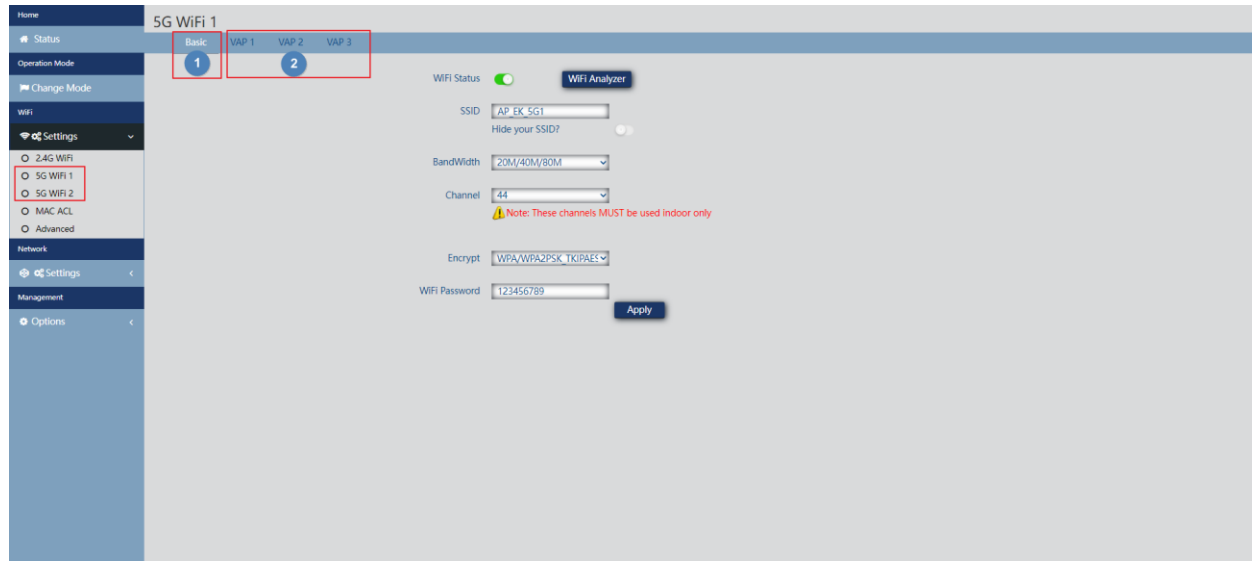
We can manage everything related to Wi-Fi from the following options. To make the changes you must click apply.

### 2.4G Wi-Fi.



1. Basic: It is the main SSID that is issued, by default it is always enabled.
    - o **Wi-Fi Status:** You can enable or disable the broadcast of 2G Wi-Fi.
    - o **Wi-Fi Analyzer:** It allows us to see the networks that are emitting around us.
    - o **SSID:** The 2G Wi-Fi name is configured.
    - o **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
    - o **Channel:** Allows us to configure the width of the channel (20M, 40M, 20M/40M) and the channel (1 to 13).
    - o **Encryption:** Allows us to select the encryption mode or set it free if desired.
    - o **Wi-Fi password:** Allows us to configure the password for the selected SSID.
  2. VAP1, VAP2 and VAP3: These are different virtual SSIDs that can be activated depending on your needs. If we activate them, we will have other SSIDs broadcasting on the same channel as the basic one, but with another password if desired.
    - o **Wi-Fi status:** You can enable or disable the broadcast of 2G Wi-Fi
    - o **SSID:** The 2G Wi-Fi name is configured.
    - o **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
    - o **Encryption:** Allows us to select the encryption mode or set it free if desired.
- Wi-Fi password: Allows us to configure the password for the selected SSID.

## 5G Wi-Fi 1 and 2.

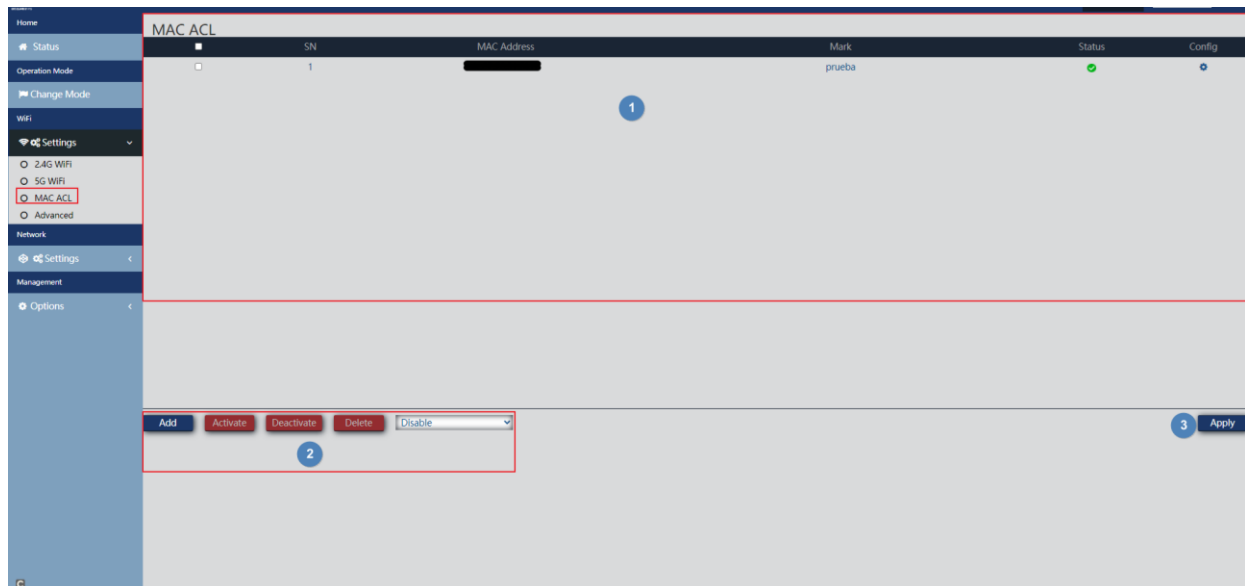



1. Basic: It is the main SSID that is issued, by default it is always enabled.
  - **Wi-Fi Status:** You can enable or disable the broadcast of 5G Wi-Fi.
  - **Wi-Fi Analyzer:** It allows us to see the networks that are emitting around us.
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Channel:** It Allows us to configure the channel width (20M,40M,80M,20M/40M,20M/40M/80M) and the channel (36-64 wifi 1 and from 100 to 140 wifi 2).
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.
  - **Wi-Fi password:** Allows us to configure the password for the selected SSID.
2. VAP1, VAP2 and VAP3: These are different virtual SSIDs that can be activated depending on your needs. If we activate them, we will have other SSIDs broadcasting on the same channel as the basic one, but with another password if desired.
  - **Wi-Fi status:** You can enable or disable the broadcast of 2G Wi-Fi
  - **SSID:** The 2G Wi-Fi name is configured.
  - **Hide your SSID:** Allows you to hide the SSID so that, although it is emitting the SSID, it does not appear when making a simple Wi-Fi search to make a connection.
  - **Encryption:** Allows us to select the encryption mode or set it free if desired.

Wi-Fi password: Allows us to configure the password for the selected SSID

## MAC Access Control List (ACL).

From this menu we can allow or not that the teams can connect to the AP.



1. Main interface: We will be able to see the added devices, as well as if the list is being applied or not. It could be modified thanks to the wheel under '**config**' .
2. Management buttons.
  - o **Add**: Allows us to add a device to the list.
  - o **Activate**: Active ACL selected in main interface.
  - o **Deactivate**: Deactivate ACL selected in main interface.
  - o **Delete**: Allows us to delete a device from the list.
  - o Drop-down:
    - o **Disable**: No rules apply on this MAC (all computers can connect).
    - o **Allow Listed Whitelist**: A whitelist is applied on this MAC (only this computer will be able to connect).
    - o **Deny Listed Blacklist**: A blacklist is applied on this MAC (this computer will not be able to connect, but the rest will).
3. **Apply**: We apply the selected list from drop-down to the selected devices in main interface.


The steps to configure it are as follows:

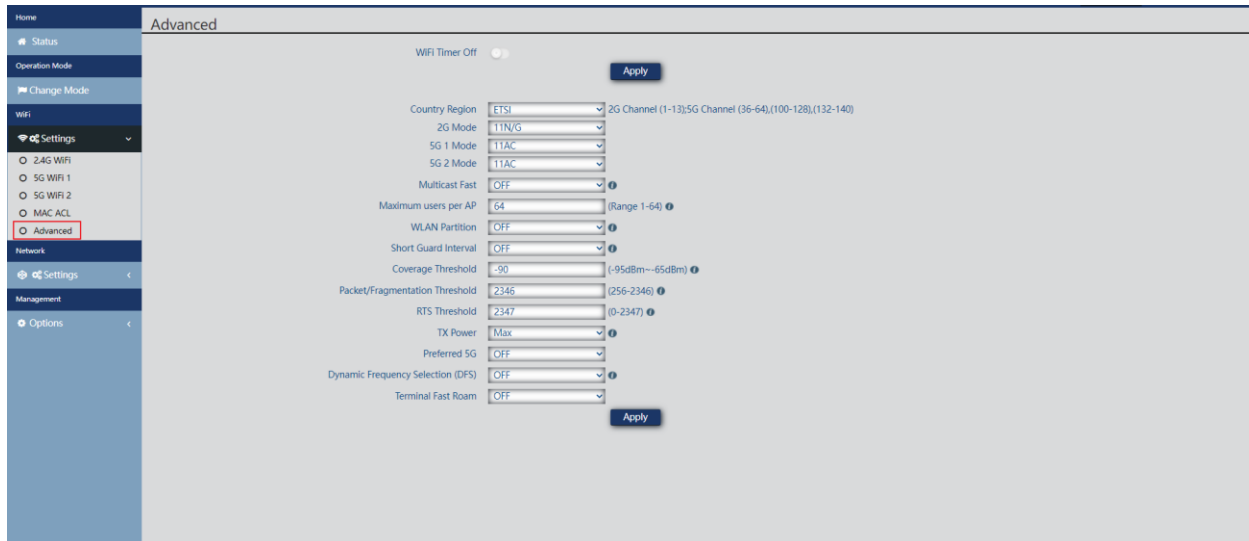
1. Click **add**. And we configure the parameters that it asks us for.



- **MAC address:** Add the MAC of the computer by hand or select the **Scan** option. Thanks to the **Scan** option we will see the registered MAC and we will only have to select the MAC.
  - **Note:** We add the note we want so that it appears in the notes part of the main interface.
- 2. We select "Whitelist" or "Blacklist".
- 3. Apply.

## Advanced Config.

In this section we can configure different advanced parameters that affect the Wi-Fi of the computer. We have a brief description of the options in the TR itself, if we put the mouse on the icon 



- **Wi-Fi timer disabled:** by default, it is disabled, if it is activated it will allow us to configure a time range in which the equipment will not emit Wi-Fi.
- **Country/Region:** Allows us to configure the country/region which modifies the channels on which the equipment broadcasts. The channels will be based on the ones that that country uses.
- **2G Mode:** Standard that uses 2G Wi-Fi.
- **5G Mode:** Standard that uses 5G Wi-Fi 1.
- **5G 2 Modo:** Standard that uses 5G Wi-Fi 2.
- **Multicast Fast:** This option is useful when there is presence of multicast traffic (example, video over IP) on the LAN network and you want to carry it through the Wi-Fi interfaces. To do this, simply deselect the OFF option (default option) and select a Wi-Fi multicast transmission speed, being recommended the speeds of 6, 12 and 24 Mbps, as they are basic speeds of the device.
- **Maximum users pe AP:** Allows you to configure the maximum number of computers that will connect to the AP.
- **WLAN partition:** It is a security option that allows you to isolate the Wi-Fi terminals in such a way that they cannot establish a direct communication between SSID.
- **Short Guard interval:** The guard interval (GI) is a parameter that regulates the time that elapses between two different symbols. It typically takes a value of 800ns, but can be reduced to 400ns. This optimization allows you to gain speed in n and ac modes, although it may not be adequate in environments with high interference level
- **Coverage threshold:** It is a quality parameter on the power required of a terminal in reception on the AP, so that those users received with less power are automatically disassociated. The resulting effect is equivalent to limiting the range in distance and, consequently, that the connected terminals have a better performance service.

- **Packet/Fragmentation threshold:** This is the maximum value that packets reached before being fragmented. The maximum value is 2346 (no fragmentation) and it is advisable to reduce it a little only if you experience media access problems or collisions.
- **RTS Threshold:** It is the packet size threshold above which the RTS/CTS mechanism is activated. **'RTS'** (Send Request)/**'CTS'** (Ready to Send) is a mechanism to reduce collision between stations, but the use of RTS/CTS will add more overhead to the network; so, by default, the AP uses only RTS/CTS when transmitting a 2347-byte packet. Having this default value does not use the mechanism.

Thanks to this mechanism, we can minimize the number of collisions between hidden stations (final equipment that communicates only with the WiFi AP and does not communicate with other final equipment connected to the AP, since they are not within its reach).
- **Output Power:** Allows you to configure the power with which the equipment emits.
- **Preferred 5G:** In case of configuring the same SSID for the two networks, if the device has good signal it will connect to the 5G SSID whenever it can preferentially.
- **Dynamic frequency selection (DFS):** The DFS function is suitable for those environments with nearby radars (ex. ports or airports) in which strong interference is generated. This function, when detecting an anomaly, analyzes the rest of the radio channels in 5GHz and, after a scan time, identifies and migrates the communications to a new channel. Except in cases of proven need, it is generally recommended to deactivate them.
- **Terminal Fast Roam:** Allows equipment compatible with 802.11 k/v/r protocols to make transitions between APs quickly and efficiently, avoiding the connection losses inherent in this type of transitions typical of APs that do not support the aforementioned protocols.

## Network Settings.

We can configure the LAN part of the computer. To make the changes you must click apply.

### LAN.

We will be able to configure the access IP of the equipment. If we want the NTP function, with which the equipment is put in time automatically, we must have an operation within our network.

- LAN settings.
  - IP Mode:
    - **Static IP:** A management IP is configured statically.
    - **Get IP from AC:** The management IP is given by an EK controller.
    - **Get IP from the gateway:** The management IP is given by the Router installed on the client.
  - **IP Lan:** We set the desired static IP. **Only in 'static IP' IP mode.**
  - **Subnet:** We put the mask for the management IP. **Only in 'static IP' IP mode.**
  - **Gateway:** We select the gateway of the computer. **Only in 'static IP' IP mode.**
  - **Primary DNS:** The primary "Domain Name System" is selected. **Only in 'static IP' IP mode.**
  - **Secondary DNS:** The secondary "Domain Name System" is selected. **Only in 'static IP' IP mode.**
- SAP/SDP announcements:
  - **SAP/SDP announcement:** By default, it is activated. Allows you to activate the protocol so that the CAP is able to recognize the AP on the same network in which they are connected. It also allows us to see the IP with the Wireshack tool.
  - **Delay between packets (seconds):** Default is 10. It allows us to modify the shipping delay between SAP SDP packages. The smaller the number, the faster packets will be resent and the greater the network load, This will also offer faster discovery/configuration of devices.

- **Security:**
  - **HTTPS:** It allows us to configure a more secure connection with the AP using the https protocol, which is a version with an encryption in the connection to avoid possible security problems.
- **DHCP server.**
  - **DHCP server:** Enables/disables the DHCP server.
  - **Start address:** The first address in DHCP pool.
  - **Maximum number:** The maximum number of IPs to be allocated.
  - **DHCP lease time:** How long devices will retain the assigned IP. After the time a new IP will be assigned.
  - **Assigned IP Number:** Displays the number of IPs assigned at the time. Using the "DHCP list" button we can see the devices that are there and that IP has been assigned to home one.

## VLAN.

Through this option we can configure different VLANs in the Wi-Fi networks that best suit us. For the configuration to be applied we will have to give in the drop-down and put it in '**ON**', then we give in 'apply'.

## Management Options.

In the following menus we will find different options to manage our EK team. To make the changes you must click apply.

### Configure.

- **Backup:** We will back up the current configuration of the access point.
- **Restore:** Allows us to upload a previously made backup copy.
- **Reset default:** Allows us to return the computer to its default values.
- **Telnet:** Enables access to the computer using telnet or not.

### Reboot.

- **Reboot:** Allows us to restart the computer at the time we give it.
- **Timed Reboot:** Allows us to configure a scheduled restart either by:
  - **Reboot time:** We configure the day/days and times to restart the computer.
  - **Restart interval:** Allows us to configure it to restart in an interval of days. It will always restart one day later from the time these settings are applied.

### Modify password.

We may modify the previous password for access to the computer. If we lose the modified password, we will have to perform a factory reset with its button and reconfigure from 0.

### Upgrade.

It allows us to load a new firmware version. You can find the latest versions on our <https://ek.plus/software/page>.

Please note that we advise checking the 'Resume factory settings' option. This will leave the computer with the default values.

### Time.

It allows us to configure the time of the computer. We have two possibilities:

- **Enable NTP:** The computer will upgrade its time automatically at boot time. It is necessary that the computer has configured an IP within our network and a correct Gateway. This will be configured on the LAN side.
- **If we disable NTP:** It will allow us to synchronize the time with our PC.

### Log.

We can enable or not the LOG to see if errors happen on the computer. It also allows us to use a remote LOG server, but we will need a syslog client

Through the following options we can perform different actions:

1. **Export:** We export the Log in a file type .bin.
2. **Delete:** We delete the information on the Log screen
3. **Refresh:** We refresh the information on the Log screen.
4. **Apply:** We apply if we make any changes.

## Interface in Gateway mode.

### Home Status.

It is similar to AP mode but with the **WAN** part added. This will show us the status of the WAN link as well as its IP, among other data:

### Operation Mode Change Mode.

It's exactly the same as it's treated in the interface AP part. Look at [Operation Mode: Change Mode.](#)

### Wi-Fi Settings:

#### 2.4G Wi-Fi.

It's exactly the same as how it's treated in the AP. Look at [2.4G Wi-Fi part.](#)

#### 5G Wi-Fi.

It's exactly the same as how it's treated in the AP. Look at [5G Wi-Fi part.](#)

### MAC Access Control.

It's exactly the same as it's treated in the AP interface part. Look at [MAC Access Control.](#)

### Advanced Config.

It's exactly the same as it's treated in the AP interface part. Look at [Advanced Config.](#)

## Network Settings.

We can configure the LAN part of the computer. To make the changes you must click apply.

### LAN.

We can configure different parameters for the LAN part of the computer. Being in Gateway mode, you must connect the WAN port to the internet network. The LAN port will give us service to the equipment we connect. All the computers that we connect on the LAN or the Wi-Fi will be given an IP within the range configured by DHCP.

The screenshot displays the web interface for configuring the TR 2200 device. The left sidebar contains a navigation menu with options: Home, Status, Operation Mode, Change Mode, Wifi, Settings (selected), Network, LAN (selected), Static DHCP, VLAN, WAN, WAN Advanced, URL Mapping, Security, Settings, Management, and Options. The main content area is divided into four sections:
 

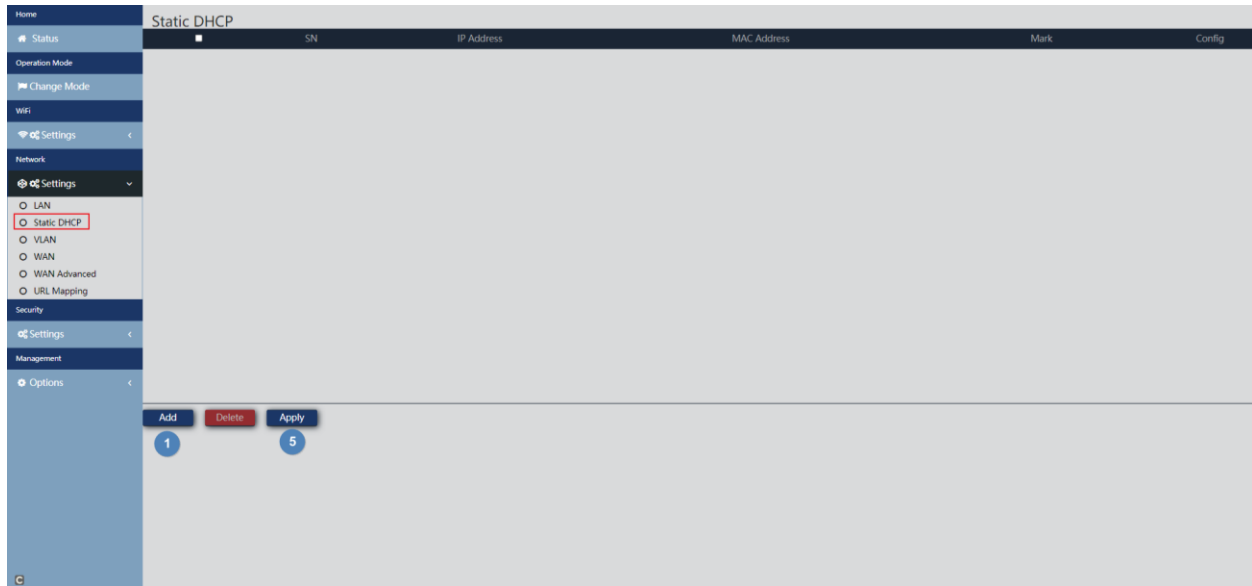
- LAN Settings:** Includes fields for Lan IP (192.168.188.253), Subnet (255.255.255.0), and a toggle for STP (enabled).
- SAP/SDP announcements:** Includes a toggle for SAP/SDP announcements (enabled) and a field for Delay between packets(seconds) (10).
- Security:** Includes a toggle for HTTPS (disabled).
- DHCP Server:** Includes a toggle for DHCP Server (enabled), fields for Start Address (2) and Max Number (251), a dropdown for DHCP Lease Time (24/Hours), and a table showing Assigned IP Number (1) with buttons for DHCP List and Apply.

- **LAN Settings.**
  - **IP Lan:** IP configured on the LAN part computer.
  - **Subnet:** Network mask that we have on the configured computer of the LAN part.
  - **STP:** We can enable Spanning tree protocol so as not to generate loops on the network.
- **SAP/SDP announcements:**
  - **SAP/SDP announcement:** By default, it is activated. Allows you to activate the protocol so that the CAP is able to recognize the AP on the same network in which they are connected. It also allows us to see the IP with the Wireshack tool.
  - **Delay between packets (seconds):** Default is 10. It allows us to modify the shipping delay between SAP SDP packages. The smaller the number, the faster packets will be resent and the greater the network load, This will also offer faster discovery/configuration of devices.

- **Security:**
  - **HTTPS:** It allows us to configure a more secure connection with the AP using the https protocol, which is a version with an encryption in the connection to avoid possible security problems.
- **DHCP server.**
  - **DHCP server:** Enables/disables the DHCP server.
  - **Start address:** The first address in DHCP pool.
  - **Maximum number:** The maximum number of IPs to be allocated.
  - **DHCP lease time:** How long devices will retain the assigned IP. After the time a new IP will be assigned.
  - **Assigned IP Number:** Displays the number of IPs assigned at the time. Using the "DHCP list" button we can see the devices that are there and that IP has been assigned to home one.

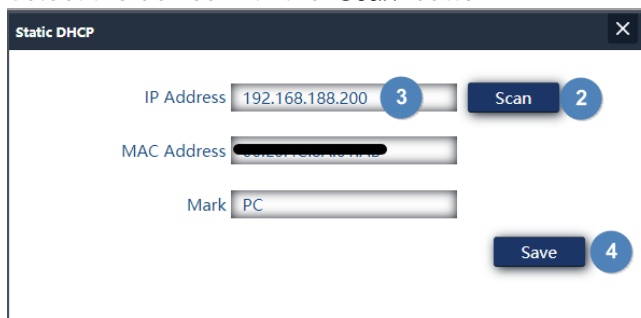
## Static DHCP.

It allows us to assign a static IP to the computers that have been connected. In this way, even if we have the devices with DHCP, they will retain the IP that we assign.



The steps to configure are:

1. Add.
2. Select the device with the 'Scan' button.



3. We assign the desired IP.
4. Save.
5. Apply.

If we select a created computer and give to delete it will be given a random IP again.

## VLAN.

It's exactly the same as it's treated in the AP interface part. Look at [VLAN](#).

## WAN.

We can configure the WAN part of the device.

The screenshot displays the 'WAN Settings' configuration page. On the left, a sidebar menu lists various settings, with 'WAN' selected and highlighted. The main configuration area includes the following fields:

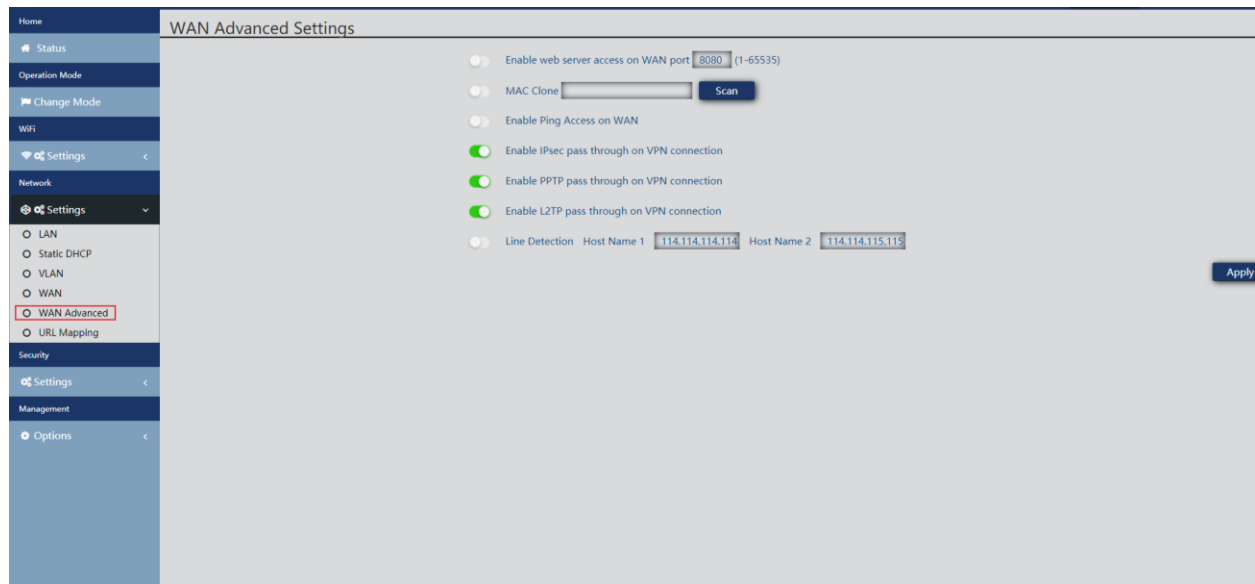
- Connect Method:** A dropdown menu set to 'DHCP'.
- MTU:** A text input field containing '1492', with a range '(1400-1500)' indicated.
- Set DNS Manually:** A toggle switch that is currently turned off.
- Primary DNS:** A text input field containing '192.168.1.1'.
- Secondary DNS:** A text input field containing '192.168.1.1'.
- Band Type:** A dropdown menu set to '1000M Fiber'.
- Upstream:** A text input field containing '1000000' Kbps.
- Downstream:** A text input field containing '1000000' Kbps.

An 'Apply' button is located at the bottom right of the configuration area.

- **Connection method:**
  - **Static IP:** We can assign a static IP to the WAN port.
  - **PPPoE:** We can configure a password user that has been configured on a PPPoE server that is in the configured installation.
  - **DHCP:** It is configured to automatically acquire the IP from the Client Router.
- **MTU:** We can determine the size of the frames. MTU, the maximum size of the packets we send to the internet. The value 1492 would match the calculation that an information packet of 1464bytes+20bytes (IP header) +8 bytes (ICMP) is used.
- **Set DNS manually:** Allows us to enable the option to assign Domain Name Service manually.
- **Primary DNS:** If we enable DNS manually, we will have to configure the primary DNS.
- **Secondary DNS:** If we enable DNS manually, we will have to configure secondary DNS.
- **Band type:** The type of band used by the WAN. We advise not to touch this parameter as it is at maximum by default.
- **Upstream:** Set upload limit.
- **Downstream:** Set downside limit.

## WAN Advanced Settings.

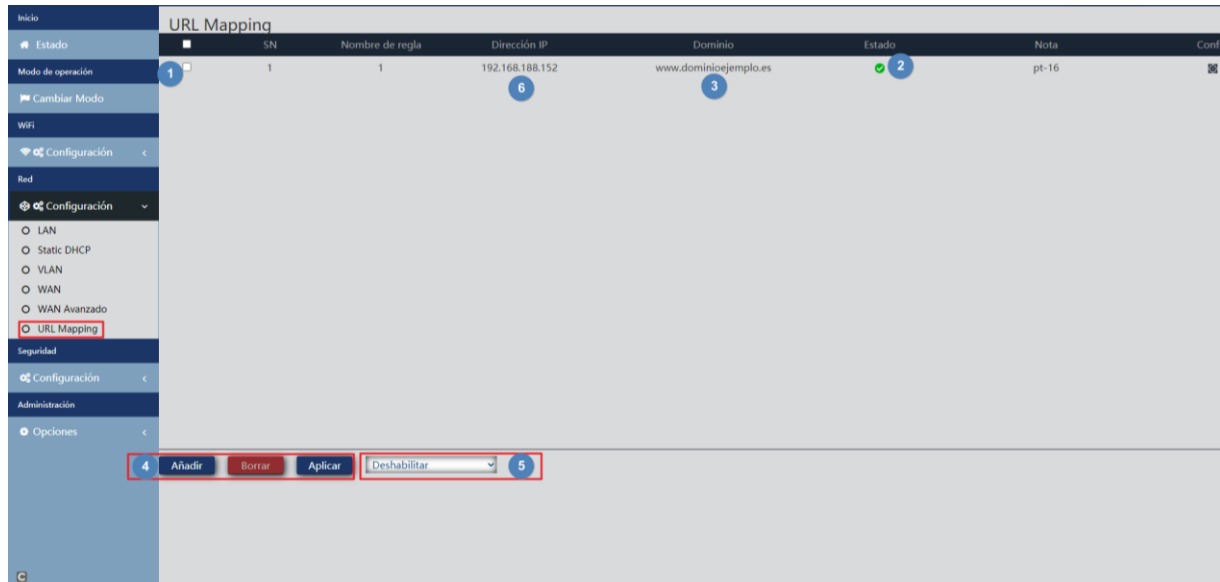
We can configure different advanced parameters that affect the WAN.



- **8080:** Allows us to enable access to the WAN interface by its IP and the port we configure, by default 8080.
- **Clone MAC:** Useful option for those Internet access services that are authenticated based on the MAC address of the user's PC. APs can emulate such MAC and thus offer simultaneous connection to multiple devices
- **Enable ping access on WAN:** Allows us to enable pinging the WAN interface.
- **Enable IPsec pass-through on the VPN connection:** Allows tunnel-type VPN connections to pass through without further specific configuration
- **Enable PPTP pass-through on VPN connection:** Allows tunnel-type VPN connections to pass through without further specific configuration
- **Enable L2TP pass-through on VPN connection:** Allows tunnel-type VPN connections to pass through without further specific configuration
- **Line detection Host name 1 114.114.114.114 Host name 2 114.114.115.115:** Allows you to configure an address to verify that the WAN part has internet output.

## URL Mapping

APs facilitate the connection of servers installed on the LAN, for which even the redirection of domain calls that, received on the WAN interface, are routed to specific IP addresses is supported.



1. List of LAN servers.
2. The status of each of the URL mapping rules.
3. Domain addressing (requests received on the WAN IP and forwarded to the corresponding IPs).
4. Adding and deleting entries. We also have the apply button.
5. Activation of the URL mapping function.
6. LAN IP address of the mapped server.

When you click **add**, a window will appear where we will complete the data that appears in the previous Interface. With the "scan" button we can select the IP and the device to which we redirect.

URL Mapping

Status ☒

Rule Name

IP Address  Scan

Domain

Mark

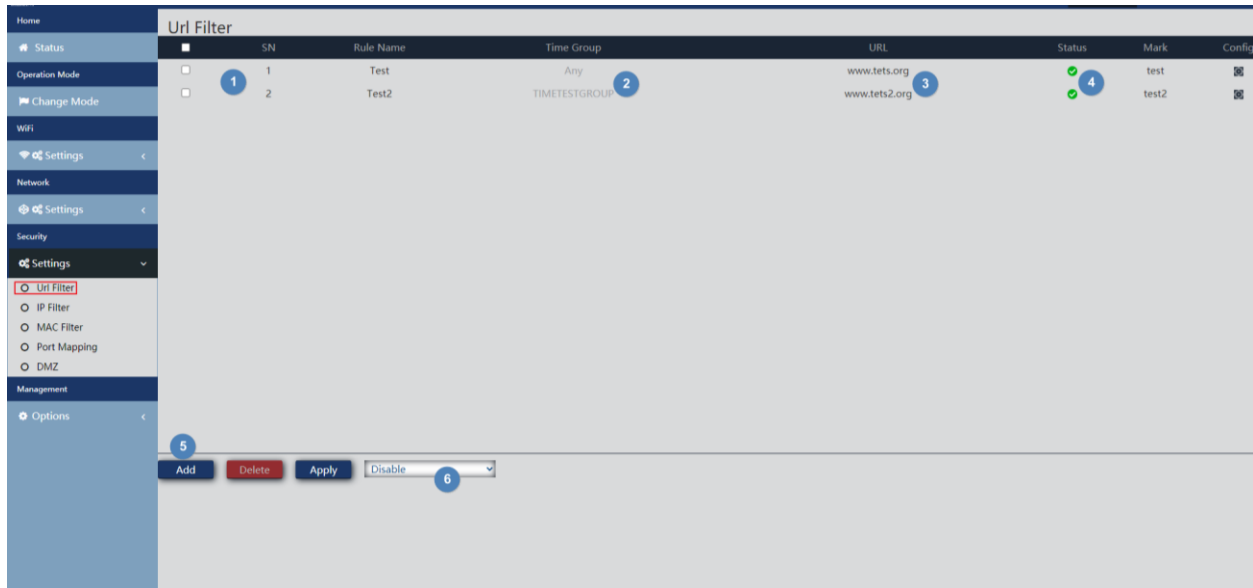
Save

## Security Settings.

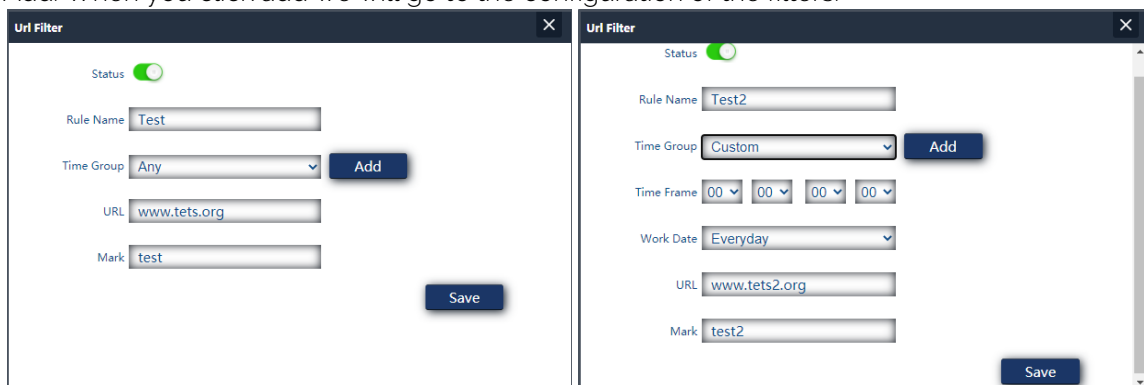
It allows us to configure different security protocols on the computer. To make the changes you must click apply.

### URL Filter.

Allows you to block access to configured Internet addresses.



1. Ip filters defined.
2. The time at which the rule is applied (defined custom or according to predefined "temporary groups" in [Time Group](#) ).
3. Blocked URLs.
4. The activation status of the filter.
5. Add. When you click add we will go to the configuration of the filters.



- o **Status:** We can enable or disable the filter.
- o **Rule Name:** We assign a name to the filter.

- **Time group:** You can assign a period in which the filter is put into operation. We can select one previously defined in Time [Group](#) (pressing add will take us directly to time group) or create a custom one. If we select custom, we will have the following options
    - i. **Time frame:** Hours at which the rule will be put into operation.
    - ii. **Work date:** We assign days of operation of the rule (every day or by selecting some)
  - **URL:** We define the URL over which the rule applies.
  - **Mark:** We put a note that we want.
6. Enabling filters (don't forget **'Apply'**).

Once created they can be modified with the icon .

### IP Filter.

It facilitates a system of rules that allows you to filter traffic to the Internet. Rules can be block or permission, depending on whether you select them (blacklists or whitelists).

Home

Status

Operation Mode

Change Mode

WiFi

Settings

Network

Settings

Security

Settings

- Url Filter
- IP Filter
- MAC Filter
- Port Mapping
- DMZ

Management

Options

IP Filter

	SN	Rule Name	Time Group	IP Address	Port Range	Protocol	Status	Mark	Config
<input type="checkbox"/>	1	Test	Any	Custom	10-11	TCP+UDP		test	
<input type="checkbox"/>	2	Test2	Custom	IPTESTGROUP	1-10	TCP+UDP		test2	

7

AddDeleteApply

Disable8

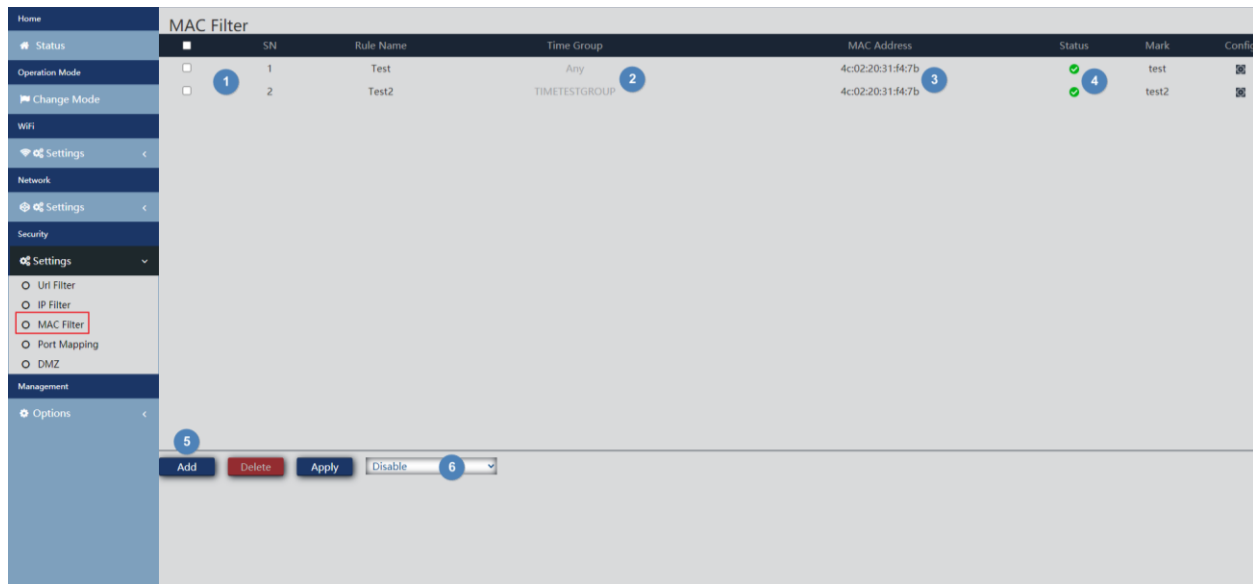
7. Add. When you click add we will go to the configuration of the filters.

- o **Status:** We can enable or disable the filter.
  - o **Rule Name:** We assign a name to the filter.
  - o **Time group:** You can assign a period in which the filter is put into operation. We can select one previously defined in Time [Group](#) (pressing add will take us directly to time group) or create a custom one. If we select custom we will have the following options
    - i. **Time frame:** Hours at which the rule will be put into operation.
    - ii. **Work date:** We assign days of operation of the rule (every day or by selecting some)
  - o **IP Group:** You have to configure the IP group/ports on which the rule will apply. This can be a group previously defined in IP [Group](#) (pressing add will take us directly to IP group). You can also create a custom one.
  - o **IP address:** Enter the range manually or select the device by means of the 'scan' button.
  - o **Port Range:** We enter the range of ports manually.
  - o **Protocol:** We define which protocol will affect TCP/UDP.
  - o **Mark:** We put a note that we want.
8. Enabling whitelist or blacklist (don't forget "Apply").

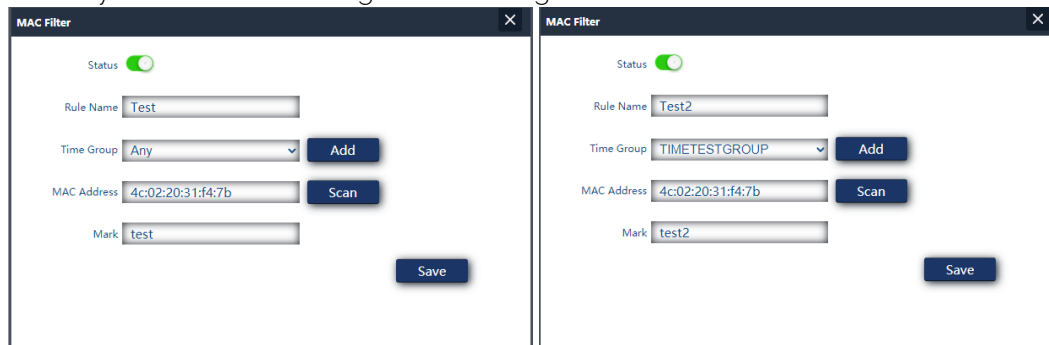
Once created they can be modified with the icon .

## MAC Filter.

Enables the restriction or denial of Internet access to devices based on their MAC address.



1. Mac filters defined.
2. The time at which the rule is applied (defined custom or according to predefined "temporary groups" in [Time Group](#) ).
3. MAC addresses to which the.
4. The activation status of the filter.
5. add. When you click add we will go to the configuration of the filters.



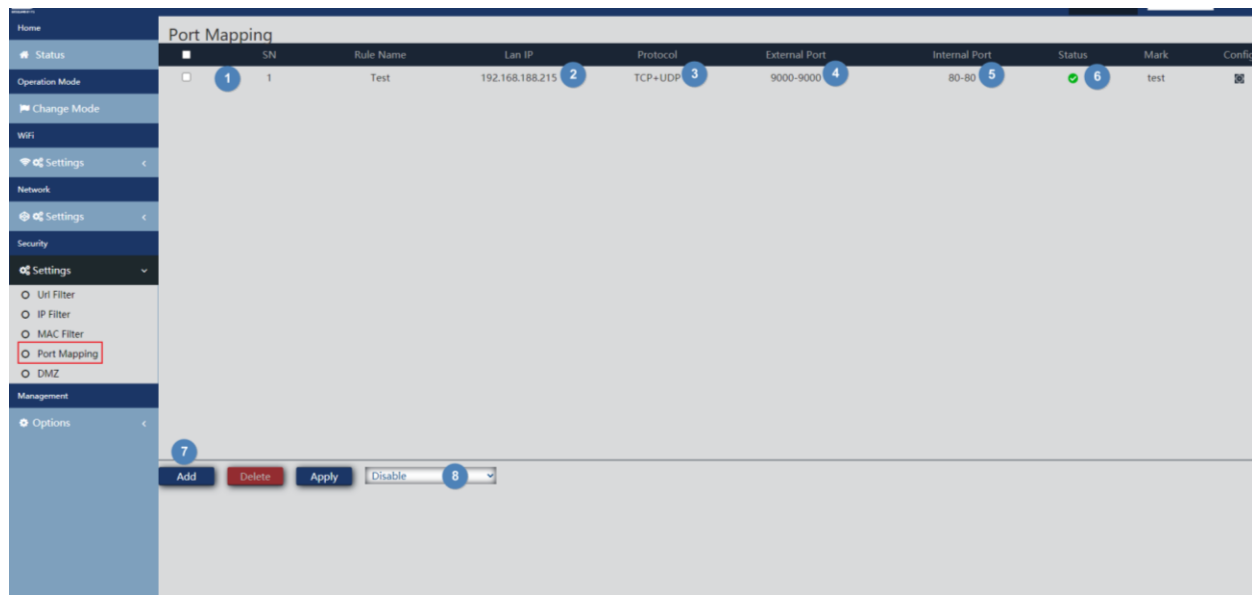
- o **Status:** We can enable or disable the filter.
- o **Rule Name:** We assign a name to the filter.
- o **Time group:** You can assign a period in which the filter is put into operation. We can select one previously defined in [Time Group](#) (pressing add will take us directly to time group) or create a custom one. If we select custom, we will have the following options.
  - i. **Time frame:** Hours at which the rule will be put into operation.
  - ii. **Work date:** We assign days of operation of the rule (every day or by selecting some).

- **MAC Address:** We define the MAC on which the rule applies.
  - **Mark:** We put a note that we want.
6. Enabling whitelist or blacklist (don't forget **'Apply'**).

Once created they can be modified with the icon .

## Port Mapping


It allows to ensure the external publication of services available on the LAN, by mapping external ports of the WAN over LAN resources (IP address + port, internal).



1. Mapping rules defined.
2. The LAN IP to which the rule is directed.
3. The protocol of the port to which the rule applies.
4. The external port to which the rule applies.
5. The internal port to which the rule applies.
6. Rule firing status.

7. Add. When you click add we will go to the configuration of the rule.

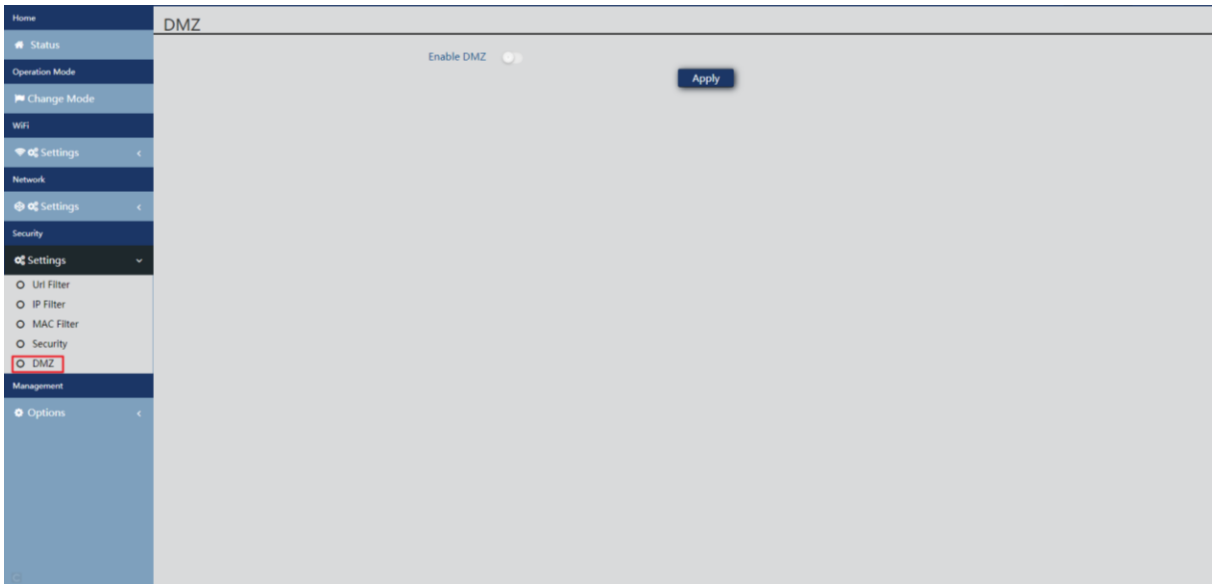
- **Status:** We can enable or disable the rule.
  - **Rule class:** It allows us to select the type of rule to apply the port number automatically.
  - **Rule Name:** We assign a name to the rule.
  - **Protocol:** We indicate on what type of port protocol TVP/UDP applies.
  - **LAN IP:** We define the IP on which the rule applies. We can press '**scan**' to see the currently connected devices and select one.
  - **External Port:** Wan port where the request will enter.
  - **Internal port:** Port of the equipment on our LAN to which we address the request.
  - **Mark:** We put a note that we want.
8. Enabling whitelist or blacklist (don't forget '**Apply**').

Once created they can be modified with the icon .

DMZ.

DMZ (Demilitarized Zone) is a feature that can compromise the security of the internal network and care must be taken to use it. It leaves all ports on the AP open and implies that anyone from the Internet will be able to perform a trace to detect vulnerabilities in the services being used. That is why its use is not recommended. When enabling we will be asked about which IP you want to apply the DMZ protocol since it can only be applied on one private IP at a time.

In the case of not knowing if we have a problem of ports, configuration of an application, that the DDNS fails or what happens, it is a way to rule out failures.



## Management Options.

Configure.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Configuration](#).

Reboot.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Reboot](#).

Modify password.

It's exactly the same as it's dealt with in the AP interface part. Look at [Modify Password](#).

Upgrade.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Upgrade](#).

Time.

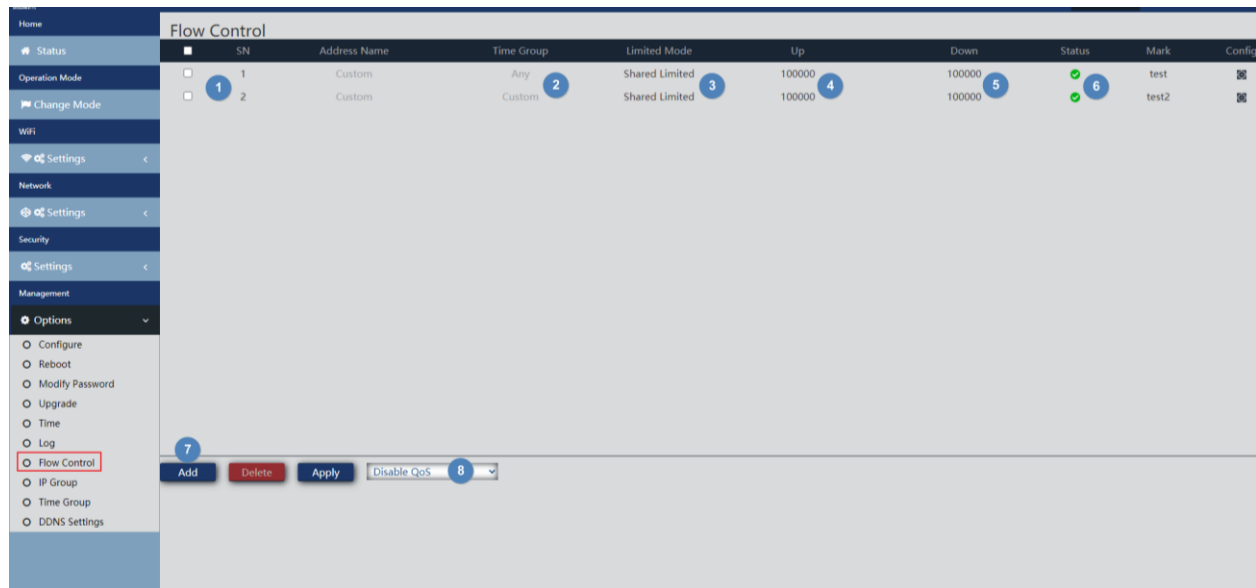
It's exactly the same as it's treated in the AP. Look in [Time part](#).

Log.

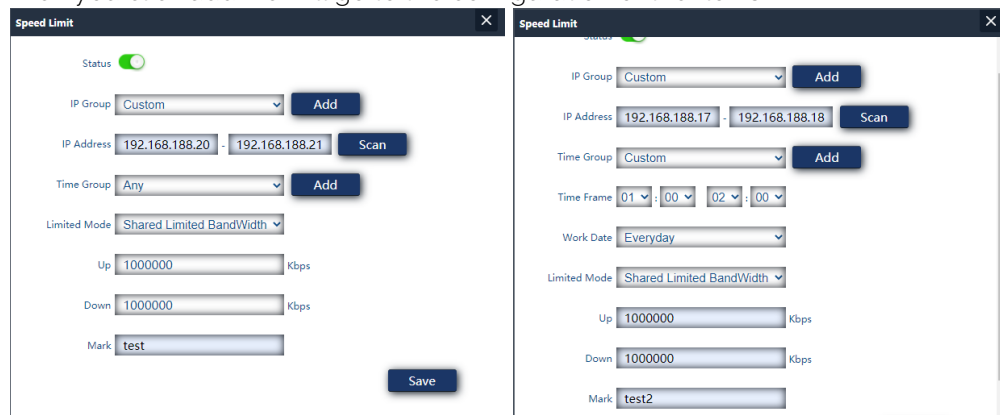
It's exactly the same as it's treated in the AP interface part. Look in [Log](#).

## Flow control.

It allows us to limit the rise and fall of the equipment according to the rule that we configure.



1. Flow control defined.
2. The time at which the rule is applied (defined custom or according to predefined "temporary groups" in [Time Group](#) ).
3. Limited mode selected
4. Flow control activation state.
5. add. When you click add we will go to the configuration of the flows.

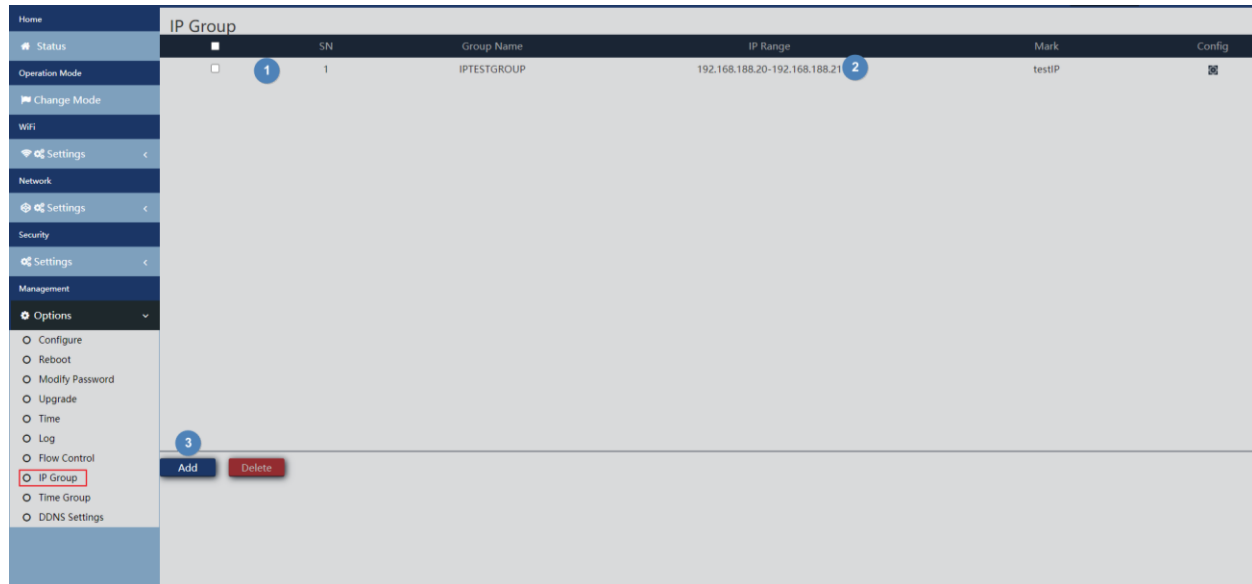


- o **Status:** We can enable or disable the filter.
- o **IP Group:** You have to configure the IP group/ports on which the rule will apply. This can be a group previously defined in IP [Group](#). (pressing add will take us directly to IP group). You can also create a custom one with the following parameters.
- o **IP address:** Enter the range manually or select the device by means of the 'scan' button.

- **Time group:** You can assign a period in which the filter is put into operation. We can select one previously defined in Time [Group](#) (pressing add will take us directly to time group) or create a custom one. If we select custom, we will have the following options
    - i. **Time frame:** Hours at which the rule will be put into operation.
    - ii. **Work date:** We assign days of operation of the rule (every day or by selecting some)
  - **Limited mode:** We can choose the mode of limitation:
    - i. **Shared limited bandwidth:** The limit is distributed among all IPs in the configured range.
    - ii. **Exclusive limited bandwidth:** The limit that has been configured within the range is limited by IP.
  - **Up:** We can configure the upload limit we want in kbps. Example 100000 kbps would be 100Mbps.
  - **Down:** We can configure the drop limit we want in kbps. Example 100000 kbps would be 100Mbps.
  - **Mark:** We put a note that we want.
6. Enabling whitelist or blacklist (don't forget **'Apply'**).

## IP group.

These are groups of one or more IP addresses on the LAN on which security rules will be applied (URL filters, IP filters, etc.) or traffic control (QoS) rules.



1. Defined groups.
2. The IP range of the group that was created.
3. Add. When you click add we will go to the configuration of the IP groups:

IP Group

Group Name

IPTESTGROUP

IP Address

192.168.188.20 - 192.168.188.21

Scan

Mark

testIP

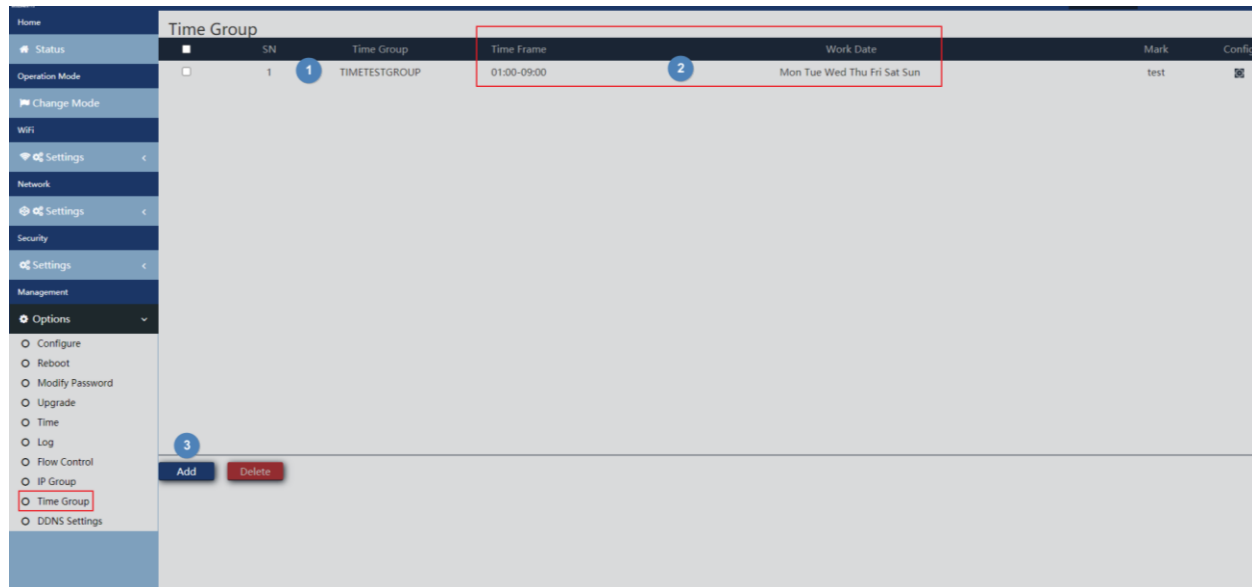
Save

- **Group Name:** We enter the name of the group we want to create.
- **IP address:** Enter the range manually or select the device by means of the 'scan' button.
- **Mark:** We put a note that we want.

## Time group.

Time groups allow you to restrict the application of safety rules and/or flow control to specific time slots, including not only times but even specific days of the week.

Temporary groups are selectable in the configuration of **IP**, **URL**, **QoS** rules from the same form of definition of these rules and, of course, they can be applied in different rules at the same time, depending on the configuration



1. Defined groups.
2. Time range defined for the group.
3. Add. When you click add we will go to the configuration of the IP groups:

- **Time Group:** We enter the name of the group we want to create.
- **Time period:** Enter the period manually or select the device by means of the 'scan' button.
- **Working date:** We can select "Every day" or "Weekly" according to needs.
- **Mark:** We put a note that we want.

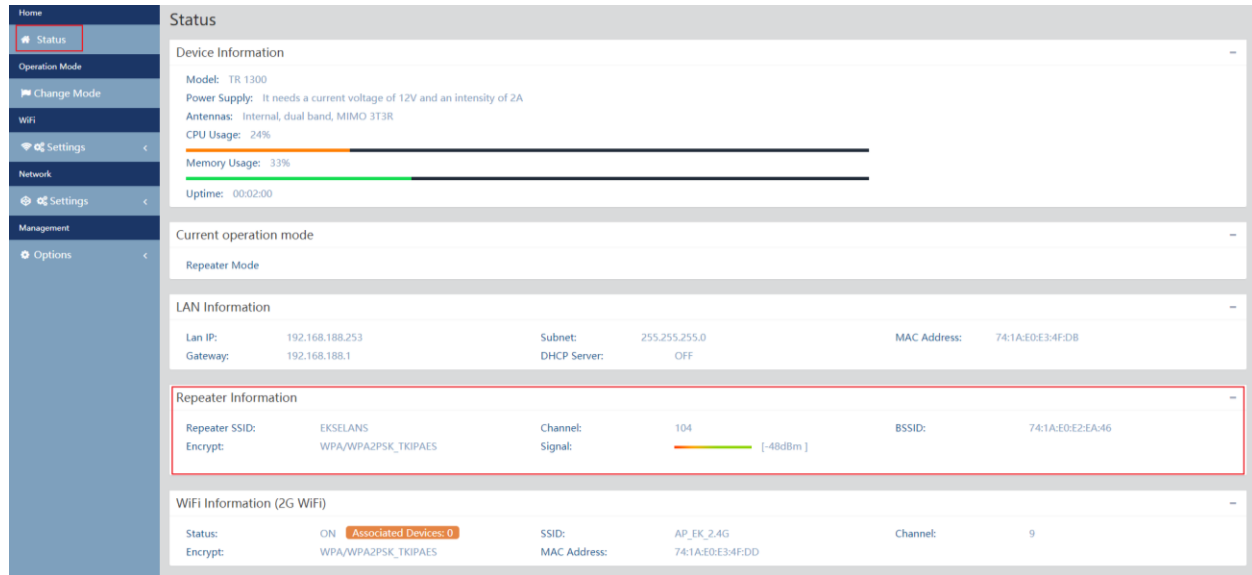
#### DDNS configuration.

Allows you to configure a DDNS server (it is an external service such as "No-IP", "Dynu"). With this service we can emulate a fixed IP of our provider. We must register in these services, which are not linked to EK.

## Interface in Repeater mode.

### Home Status.

It is similar to the AP mode but with the **Repeater** part added, where it shows us the quality of the link:



### Operation Mode Change Mode.

It's exactly the same as it's treated in the interface AP part. Look at [Operation Mode: Change Mode.](#)

### Wi-Fi: Configuration.

#### 2.4G Wi-Fi.

It's exactly the same as how it's treated in the AP. Look at [2.4G Wi-Fi part.](#)

#### 5G Wi-Fi.

It's exactly the same as how it's treated in the AP. Look at [5G Wi-Fi part.](#)

### MAC Access Control.

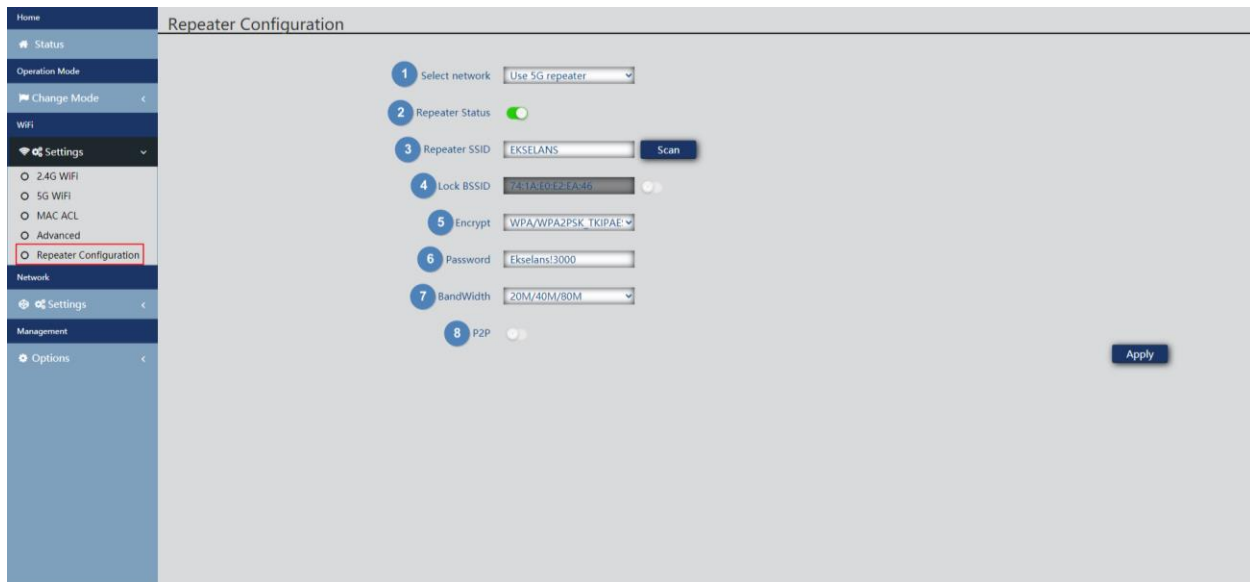
It's exactly the same as it's treated in the AP interface part. Look at [MAC Access Control.](#)

### Advanced Config.

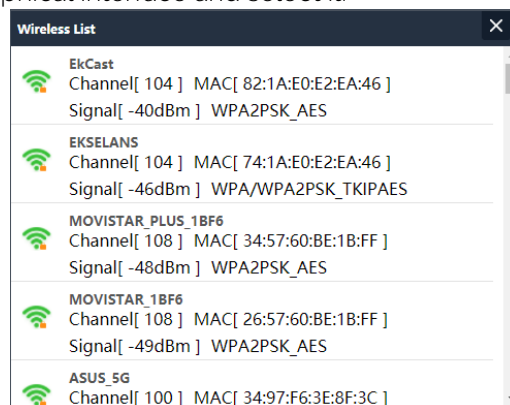
It's exactly the same as it's treated in the AP interface part. Look at [Advanced Config.](#)

## Repeater configuration.

We will be able to reconfigure the repeater part as it suits us.



1. **Select Network:** We must select the network band that we are going to repeat either 2G or 5G.
2. **Repeater Status:** Whether or not we enable the signal to be repeated.
3. **Repeater SSID:** We select the SSID we want to repeat. We can use the SCAN button to search the network thanks to graphical interface and select it.



4. **Lock BSSID:** You can close by MAC the configuration of the repeater. In this way if another issuer is configured with the SSID to repeat, not having the same MAC that we have blocked does not make the link.
5. **Encryption:** Allows us to select the encryption mode or set it free if desired.
6. **Password:** Allows us to configure the password for the selected SSID.
7. **Bandwidth:** The desired bandwidth is configured, depending on the network we choose (2G or 5G) we can select some values or others.
8. **P2P:** Allows you to propagate wds configuration between terminals (It is recommended to disable it).

## Network Settings.

### LAN.

It's exactly the same as it's treated in the AP. Look at [LAN part](#).

### VLAN.

It's exactly the same as it's treated in the AP interface part. Look at [VLAN](#).

## Management Options.

### Configure.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Configuration](#).

### Reboot.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Reboot](#).

### Modify password.

It's exactly the same as it's dealt with in the AP interface part. Look at [Modify Password](#).

### Upgrade.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Upgrade](#).

### Time.

It's exactly the same as it's treated in the AP. Look in [Time part](#).

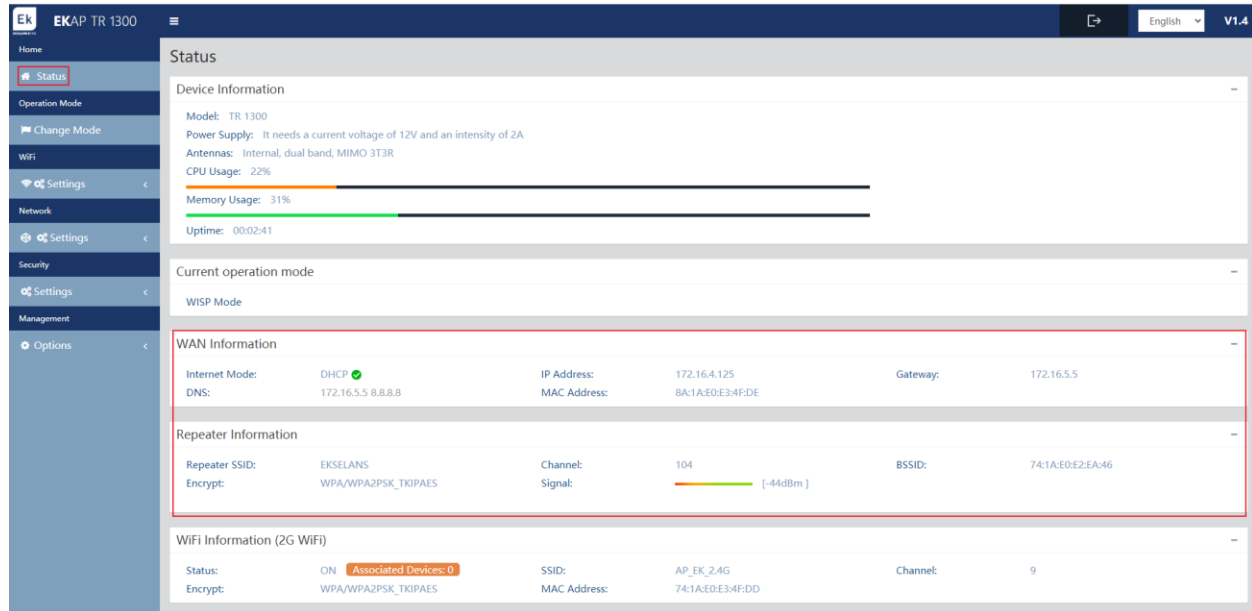
### Log.

It's exactly the same as it's treated in the AP interface part. Look in [Log](#).

## Interface in WISP mode.

### Home: Status.

It is similar to AP mode but with the **Repeater and WAN** part added. This shows the link quality and the WAN IP of the appliance:



### Operation Mode Change Mode.

It's exactly the same as it's treated in the interface AP part. Look at [Operation Mode: Change Mode](#).

### Wi-Fi: Configuration.

#### 2.4G Wi-Fi.

It's exactly the same as how it's treated in the AP. Look at [2.4G Wi-Fi part](#).

#### 5G Wi-Fi.

It's exactly the same as how it's treated in the AP. Look at [5G Wi-Fi part](#).

### MAC Access Control.

It's exactly the same as it's treated in the AP interface part. Look at [MAC Access Control](#).

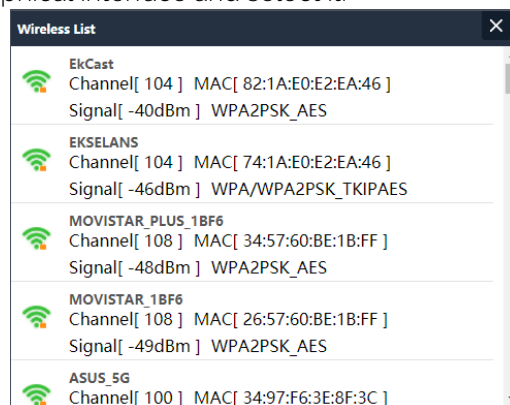
### Advanced Config.

It's exactly the same as it's treated in the AP interface part. Look at [Advanced Config](#).

## Repeater configuration.

We will be able to reconfigure the repeater part as it suits us.

1. **Select Network:** We must select the network band that we are going to repeat either 2G or 5G.
2. **Repeater Status:** Whether or not we enable the signal to be repeated.
3. **Repeater SSID:** We select the SSID we want to repeat. We can use the SCAN button to search the network thanks to graphical interface and select it.



4. **Lock BSSID:** You can close by MAC the configuration of the repeater. In this way if another issuer is configured with the SSID to repeat, not having the same MAC that we have blocked does not make the link.
5. **Encryption:** Allows us to select the encryption mode or set it free if desired.
6. **Password:** Allows us to configure the password for the selected SSID.
7. **Bandwidth:** The desired bandwidth is configured, depending on the network we choose (2G or 5G) we can select some values or others.
8. **P2P:** Allows you to propagate wds configuration between terminals (It is recommended to disable it).

## Network: Configuration.

### LAN.

It's exactly the same as it's treated in the AP. Look at [LAN part](#).

### Static DHCP.

.

### VLAN.

It's exactly the same as it's treated in the AP interface part. Look at [VLAN](#).

### WAN.

It's exactly the same as it's treated in the AP interface part. Look at [WAN](#).

### WAN Advanced.

It's exactly the same as it's treated in the AP interface part. Look at [WAN Advanced Settings](#).

### URL Mapping.

It's exactly the same as it's treated in the AP interface part. Look at [URL Mapping](#).

## Security: Settings.

### Url Filter.

It's exactly the same as it's treated in the AP interface part. Look at [URL Filter](#).

### IP Filter.

It's exactly the same as it's treated in the AP interface part. Look at [IP Filter](#).

### MAC Filter.

It's exactly the same as it's treated in the AP interface part. Look at [MAC Filter](#).

### Port Mapping.

It's exactly the same as it's treated in the AP interface part. Look at [Port Mapping](#).

### DMZ.

It's exactly the same as it's treated in the AP interface part. Look at [DMZ](#).

## Administration: Options.

### Configuration.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Configuration](#).

### Reboot.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Reboot](#).

### Modify password.

It's exactly the same as it's dealt with in the AP interface part. Look at [Modify Password](#).

### Upgrade.

It's exactly the same as how it's dealt with in the AP interface part. Look at [Upgrade](#).

### Time.

It's exactly the same as it's treated in the AP. Look in [Time part](#).

#### Log.

It's exactly the same as it's treated in the AP interface part. Look in [Log](#).

#### Flow Control.

It's exactly the same as it's treated in the AP interface part. Look at [Flow control](#).

#### IP Group.

It's exactly the same as it's treated in the AP interface part. Look at [IP group](#).

#### Time Group.

It's exactly the same as it's treated in the AP interface part. Look at [Time group](#).

#### DDNS Settings.

It's exactly the same as it's treated in the AP interface part. Look at [DDNS configuration](#).

## FAQ.

**I can't access the equipment:** We perform a factory reset to the equipment. We connect by ethernet and verify that we can ping your default IP, the 192.168.188.253. In case of not being able to check if we have well configured the IP of our PC. Go to the [Computer Access](#) section.

**Can the LED be turned off?** It is not possible to turn off the LED.

**The LED shines dimly and I can't connect to the internet:** Perform a factory reset to the computer I have tried to navigate with the default SSID, the AP\_EK\_... if you are unable to call the support phone number 93 583 95 43.

**I configure the Repeater mode and I have no connection with the internet:** Check if the P2P is activated, in case of being activated disable it and fly try the connection.

**I configure the WISP mode and I have no connection with the internet:** Check if the P2P is activated, in case of being activated disable it and fly try the connection.

**Devices connect to WI-FI and disconnect continuously:** Access the computer and verify how intensively they have connected. You can see this value in the window that will open if you click on the **'Associated Devices'** in the Home: Status part, within the Wi-Fi that is connected 2.4Ghz or 5Ghz.

**I do not know if I have the latest version of FW:** Check the latest version that is on our WEBSITE in the part of Software, Wi-Fi, <https://ek.plus/sw/Wi-Fi/>.