



SINGLE-WAN GIGABIT VPN ROUTER
USER INTERFACE MANUAL

Models:

AN-110-RT-2L1W

AN-110-RT-2L1W-WIFI





Federal Communication Commission Interference Statement

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

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

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

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

This device is designed for indoor use only.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Industry Canada Statement

This device complies with Industry Canada's licence-exempt RSSs. Operation is subject to the following two conditions:

1. This device may not cause interference; and
2. This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Caution:

(i) The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) For product available in the USA/Canada market, only channel 1-11 can be operated. Selection of other channels is not possible.



Avertissement:

(i) Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 63cm between the radiator & your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 63 cm de distance entre la source de rayonnement et votre corps.

FCC Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

(i) Les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) Pour les produits disponibles aux États-Unis / Canada du marché, seul le canal 1 à 11 peuvent être exploités. Sélection d'autres canaux n'est pas possible.

CE Warning

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

The device complies with ISED's license-exempt RSSs and Canada ICES-003.

CE Statement

This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator & your body.

All operational modes:

2.4GHz: 802.11b, 802.11g, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40)

5GHz: 802.11a, 802.11n (HT20), 802.11n (HT40), 802.11ac (VHT20), 802.11ac (VHT40), 802.11ac (VHT80)

The frequency and the maximum transmitted power in EU are listed below:

2412-2472MHz: 19.90 dBm

5180-5240MHz: 22.90 dBm

The device is restricted to indoor use only when operating in the 5150 to 5350 MHz frequency range..



AT	BE	BG	HR	CY	CZ	DK
EE	FI	FR	DE	EL	HU	IE
IT	LV	LT	LU	MT	NL	PL
PT	RO	SK	SI	ES	SE	UK

Certifications





About this Manual

This manual provides installers and end users with current information regarding the installation, setup, use, and maintenance of the product. The symbols below identify important information:



Pro Tip - Pro tips provide extra value, utility, or ease of use. Pro tips may also link to extra information that provide a better understanding of the application, technology or use of the feature in question. These items are added for your convenience.



Note - Notes emphasize important information that does not regard the safety of the equipment or user. Notes usually contain ancillary information or a step in the process, that, if missed, causes additional work to overcome.



Caution - The caution symbol indicates information vital to the safety of the product. Failing to follow a caution usually results in permanent damage to the equipment, which is not covered by the warranty.



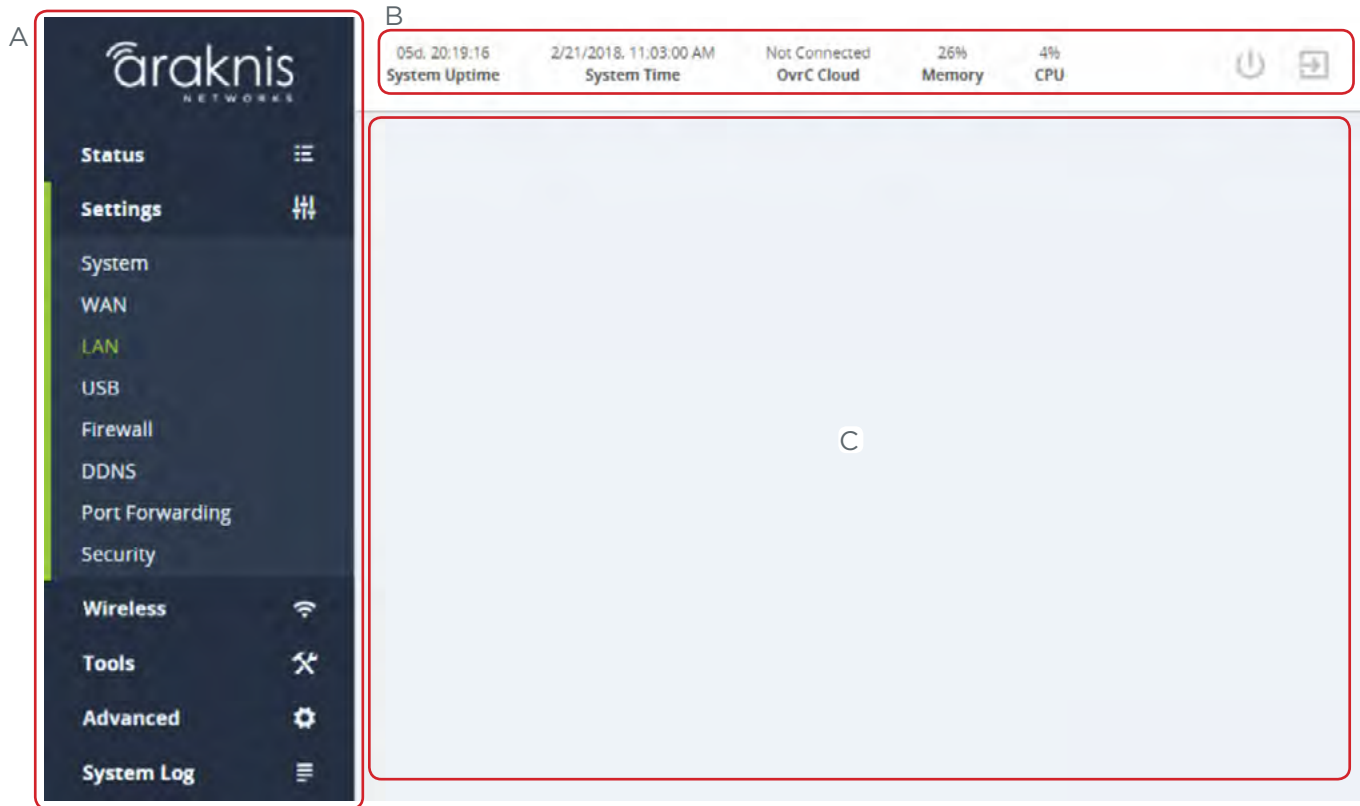
Warning - Warnings are vital to the personal safety of the installer or end user. Not following a warning can result in serious injury or death of the installer or end user, as well as permanent damage to the equipment.



Table of Contents

Federal Communication Commission Interference Statement.....	2
Industry Canada Statement.....	2
FCC Warning.....	3
CE Warning.....	3
Certifications.....	4
About this Manual.....	5
Table of Contents.....	6
Menu Overview.....	7
Status > System.....	8
Status > Clients & Services.....	11
Status > Ports.....	14
Settings > System.....	15
Settings > WAN.....	17
Settings > LAN.....	21
Settings > Firewall.....	24
Settings > DDNS.....	26
Settings > Port Forwarding.....	27
Settings > Security.....	28
Wireless > Status (<i>WI-Fi model only</i>).....	31
Wireless > Settings (<i>WI-Fi model only</i>).....	33
Tools.....	36
Advanced > Static Route.....	38
Advanced > NAT.....	39
Advanced > VLANs.....	40
Advanced > VPN.....	41
Advanced > IPV6.....	43
Advanced > Local DNS.....	46
Advanced > SNMP.....	47
Advanced > QoS.....	49
System Log.....	51
Specifications.....	52

Menu Overview



A - Main Navigation Panel

Use the collapsible Status, Settings, Tools, Advanced, and System Log headings (and their submenus) to configure and maintain the router. The green bar and gray highlight shows which header is active.

B - Top Bar

The top bar displays

- the system uptime (in days, hours minutes, and seconds),
- the system time,
- the connection status to the OvrC server, and
- the memory and CPU used.

To the right are two icons that you can click to restart and to log out, respectively.

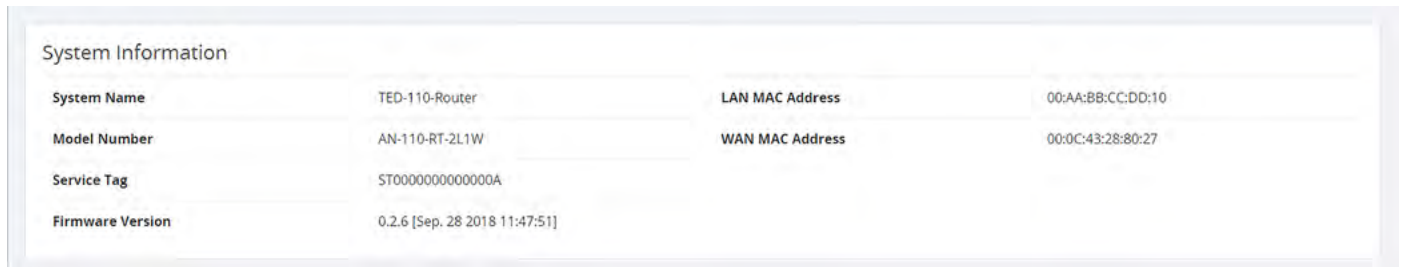
C - Main Window

This displays the currently selected window, as indicated by the green lettering in the navigation panel.

Status > System

The System Status screen provides a real-time summary of router system information, and is the first screen that appears when you log in to the router web interface. Use the screen to verify settings and operation of your device.

System Information Section



System Information			
System Name	TED-110-Router	LAN MAC Address	00:AA:BB:CC:DD:10
Model Number	AN-110-RT-2L1W	WAN MAC Address	00:0C:43:28:80:27
Service Tag	ST0000000000000A		
Firmware Version	0.2.6 [Sep. 28 2018 11:47:51]		

System Name: The user-assigned name for the device. This serves as the DHCP hostname of the device (shown when scanning the network). Use this to differentiate similar devices on your network.

Model Number: This is the part number for the router (as shown on our website).

Service Tag: The internal tracking number used to track every Araknis Networks product sold. This is required to claim the device on OvrC.

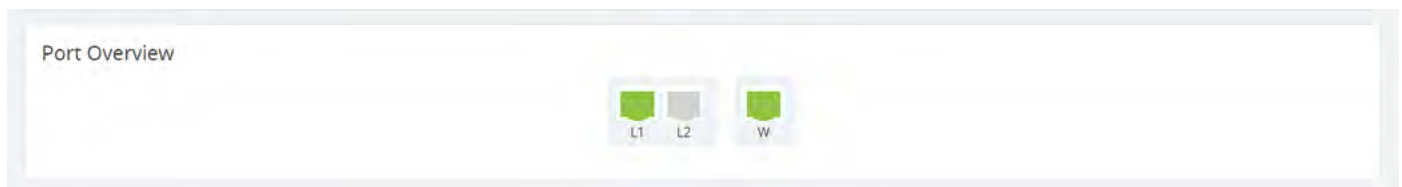
Firmware Version: The version installed on the router. Keep this current using OvrC.

WAN MAC Address: The unique Media Access Control (MAC) address for the WAN port.

LAN MAC Address: MAC address of the router. The MAC address is used to configure OvrC access.

Port Overview Section

This gives an at-a-glance status for each port on the router.



Each port is color-coded based on its negotiated speed:

- **Gray:** Not connected to a device, or the connected device has not negotiated a speed.
- **Orange:** 10/100Mbps connection is active.
- **Green:** 1Gbps connection is active.
- **Red:** Port has been disabled by the user in the web interface settings.

Port Status Section

This provides detailed information for each port on its own line. These can be configured under **Settings > LAN > LAN Settings**.

Interface	Name	Speed	Duplex
WAN	WAN1	1Gbps	Full
LAN1	LAN1	1Gbps	Full
LAN2	LAN2	N/C	N/C

Interface: Designates the physical port on the router.

Name: Name used to identify each port.

Speed: User-selected or device-negotiated port speed.

Duplex: Displays the duplex mode of the port.

WAN Status Section

This displays current information about the WAN interface status. It updates in real time.

Name	WAN1
IP Address	10.102.158.72
Subnet Mask	255.255.0.0
Default Gateway	10.102.0.1
DNS 1	10.102.105.165
DNS 2	10.102.105.166

Release Renew

1 Gb/s

Two key buttons are at the bottom.

Release Button: Click to release the current WAN IP address back to the DHCP pool and receive a new one.

Renew Button: Click to renew the current WAN DHCP connection. The WAN IP address may or may not change.

 **Note** - The Release and Renew buttons control the network IP address.

Interface: Each WAN has its own table.

IP Address: WAN IP address of the connection.

Subnet Mask: WAN subnet mask.

Default Gateway: WAN gateway IP address.

DNS 1: WAN primary domain name server.

DNS 2: WAN secondary domain name server.



At the very bottom, the WAN's current speed is displayed. The color code is as follows:

- **Gray:** Not connected to a device, or the connected device has not negotiated a speed.
- **Orange:** 10/100Mbps connection is active.
- **Green:** 1Gbps connection is active.
- **Red:** Port has been disabled by the user in the web interface settings.

Status > Clients & Services

This section describes the router firewall services, VPN services, attached clients, and port forwarding settings that are currently in use. This is where you can locate devices are (via IP/DHCP reservation) and determine which services could be affecting system performance.

Despite the appearance, this table is information only; you cannot adjust settings here. To adjust the settings, go to **Settings > Firewall**.

Firewall Status

SPI (Stateful Packet Inspection): See whether the SPI firewall setting is on or off.

DoS (Denial of Service): See whether the DoS firewall setting is on or off.

Block WAN Request: See whether the Block WAN Request firewall setting is on or off.

Remote Management: See whether the Remote Management firewall setting is on or off.

VPN Tunnel Status Section

A virtual private network (VPN) provides a connection between different networks through a secure tunnel over the Internet. Data sent through the VPN tunnel is encrypted for privacy even when connected to a public or shared network that isn't secure. VPNs are commonly used to send data between networks in different geographical locations that have no dedicated physical connection.

The router can support a maximum of five OpenVPN, as well as five PPTP tunnels. Both types can be active simultaneously.

	Used	Available
OpenVPN	0	5
PPTP	0	5

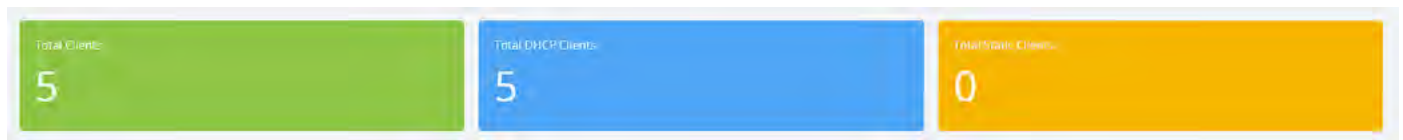
This router features a built-in OpenVPN server for secure, easily configured access to the network (via the internet) from devices with an OpenVPN client application. OpenVPN communicates using encrypted SSL/TLS channels between networks that the hide traffic from other devices on the internet.

The router must be configured for each OpenVPN account to be used. Client applications are available for PC and Mac computers and iOS and Android mobile devices.

We recommend that you do not use PPTP. The technology is old and does not use encryption.

Clients Overview Section

This shows the number of attached devices, as well as how many are static vs. DHCP.



DHCP Status Section

This ARP table tracks every device connected to your network, whether it has a DHCP address or a static IP address. In addition, the table tracks whether the device is online or offline.

Network	Range	DHCP IPs Used	DHCP IPs Available	Total DHCP Pool
192.168.1.1	192.168.1.100 - 192.168.1.199	5	95	100

Client Table Section

Client Host Name	IP Address	MAC Address	Manufacturer	ⓘ	ⓘ
E5570-1472-Butterfield	192.168.1.101 ⌚	88:08:CF:3A:26:5A	Intel Corporate	⊞	🗑️
Wattbox	192.168.1.105 ⌚	D4:6A:91:02:F0:0D	Snap AV	⊞	🗑️
new-host0	192.168.1.108 ⌚	D4:6A:91:15:E8:3D	Snap AV	⊞	🗑️
AN-210-SW-8-POE	192.168.1.110 ⌚	D4:6A:91:72:42:BC	Snap AV	⊞	🗑️
AN-500-AP-I-AC	192.168.1.100 ⌚	D4:6A:91:73:BD:4D	Snap AV	⊞	🗑️

Cancel Apply

The client table section uses an ARP table to show all clients, their IP addresses (both DHCP and static), and their MAC addresses. The 110 models can support up to 150 client devices.

Click to sort the table on any column. The Show dropdown in the top right filters the list.

The color bar at the left end of each line shows whether that client is up (green) or down (gray).

For DHCP addresses, click on the clock icon to show the remaining lease time.

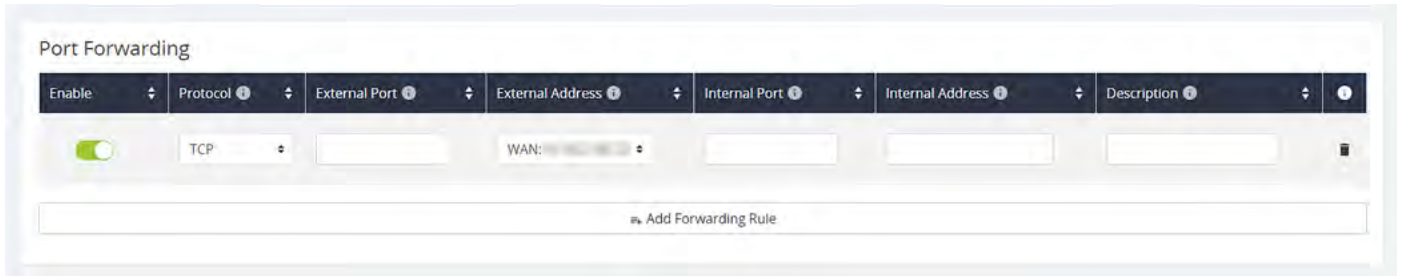
To reserve a DHCP address, click on the + icon to the left of the trash can icon.

Clicking the trash can removes that device's DHCP assignment. You'll need to reboot the device to have it request a new IP address from the router.



Port Forwarding Section

This lists all of the port forwarding rules in place. See **Settings > Port Forwarding** for information on setting these rules.



Status > Ports

Port Overview Section

This gives an at-a-glance status for each port on the router.



Each port is color-coded based on its negotiated speed:

- **Gray:** Not connected to a device, or the connected device has not negotiated a speed.
- **Orange:** 10/100Mbps connection is active.
- **Green:** 1Gbps connection is active.
- **Red:** Port has been disabled by the user in the web interface settings.

Port Status Section

These can be configured under **Settings > LAN**.

The screenshot shows a 'Port Status' section with a table containing the following data:

Interface	Name	Speed	Duplex
WAN	WAN1	1Gbps	Full
LAN1	LAN1	1Gbps	Full
LAN2	LAN2	N/C	N/C

Interface: Each physical port has its own row.

Name: Name used to identify each port.

Speed: User-selected or device-negotiated port speed.

Duplex: Displays the duplex mode of the port.

VLAN ID: The ID number of the VLAN.

Sent: The quantity of data sent through the port since the last time it was powered on.

Received: The quantity of data received by the port since the last time it was powered on.

Errors: The number of data transmission errors since the last time it was powered on.

Settings > System

System Settings Section

Here you can adjust the router's name and IP address.

The screenshot shows two panels. The left panel, titled "System Settings", contains fields for "System Name" (TED-110-Router), "System IP Address" (192.168.1.1), "System Subnet Mask" (255.255.255.0), and a toggle for "System LED's" which is turned on. The right panel, titled "Time Settings", includes a toggle for "Set local time automatically (NTP)" which is on, a "Time Zone" dropdown set to "(GMT-05:00) Eastern Time (US & Canada)", an "NTP Server" dropdown set to "time.nist.gov", a toggle for "Enable Daylight Savings Time" which is on, and "Start Date" and "End Date" fields. The start date is set to March 2nd, Sunday at 02:00, and the end date is set to November 1st, Sunday at 02:00.

Names can be up to 63 characters long, and can contain letters, numbers, hyphens, underscores, and periods. It cannot contain spaces.

The IP can be provided in either IPv4 or IPv6.

- If IPv4, this links to the Gateway IP Address (Settings -> LAN) of the default card
- If IPv6, this links to the IPv6 Address (Advanced -> IPv6)

The System Subnet Mask is not editable on this page. It is calculated from the router's IP address.

Also, if the LED lights bother you, you can switch them off here (except for the power light).

Time Settings

The screenshot shows the "Time Settings" panel. It features a toggle for "Set local time automatically (NTP)" which is on, a "Time Zone" dropdown set to "(GMT-05:00) Eastern Time (US & Canada)", an "NTP Server" dropdown set to "time.nist.gov", a toggle for "Enable Daylight Savings Time" which is on, and "Start Date" and "End Date" fields. The start date is set to March 2nd, Sunday at 02:00, and the end date is set to November 1st, Sunday at 02:00.

NTP: By default, the router checks the time automatically, using the NIST (National Institute of Standards and Technology) servers to synchronize to Coordinated Universal Time. This provides an accurate and

integrated approach to setting system time. Using NTP as an option requires Internet access. If you do not wish to use this service, deselect the checkbox and see **Manual** settings, below.


Set your time zone. North American time zones range from Hawaii (GMT-10:00) in the west to Newfoundland (GMT-03:30) in the east.

Change your NTP server if desired.

Manual: With manual sync, your router uses its internal clock. We do not recommend this setting because any electronic system's internal clock can drift. However, this choice is your only option if your network is not connected to the Internet.

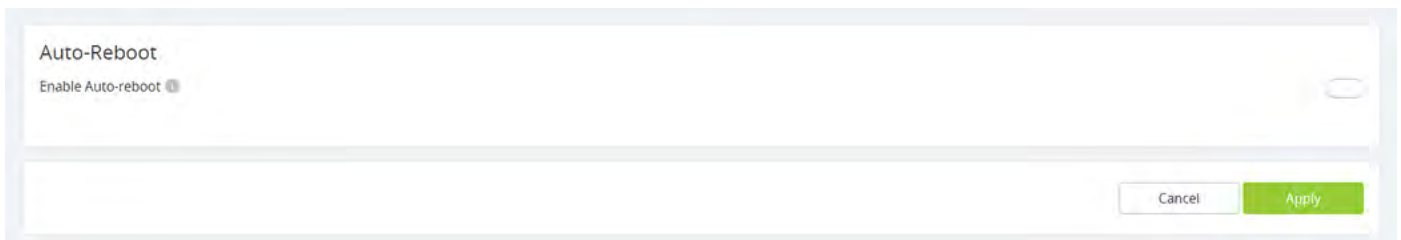
Set your desired time. As soon as you click apply, the new time settings are applied.

DST: By default, Daylight Saving Time is enabled. It works with both NTP and manual time settings. The Start Time and End Time boxes set the month, week, day, and hour (in 24-hour time) that daylight saving time starts and ends.

 **Note** - You are not setting the exact day and date with this tool. Instead, you are selecting (for example) the second Sunday in March.

If your location does not observe daylight saving time, click deselect the checkbox. Places that do not observe daylight saving time include Arizona (outside of Navajo territory), Hawaii, Saskatchewan, and a number of local exceptions across Canada. For Arizona and Hawaii, disable DST. For Saskatchewan, disable DST and set your system to Central Time. For other exceptions, check local regulations.

Auto-Reboot Section



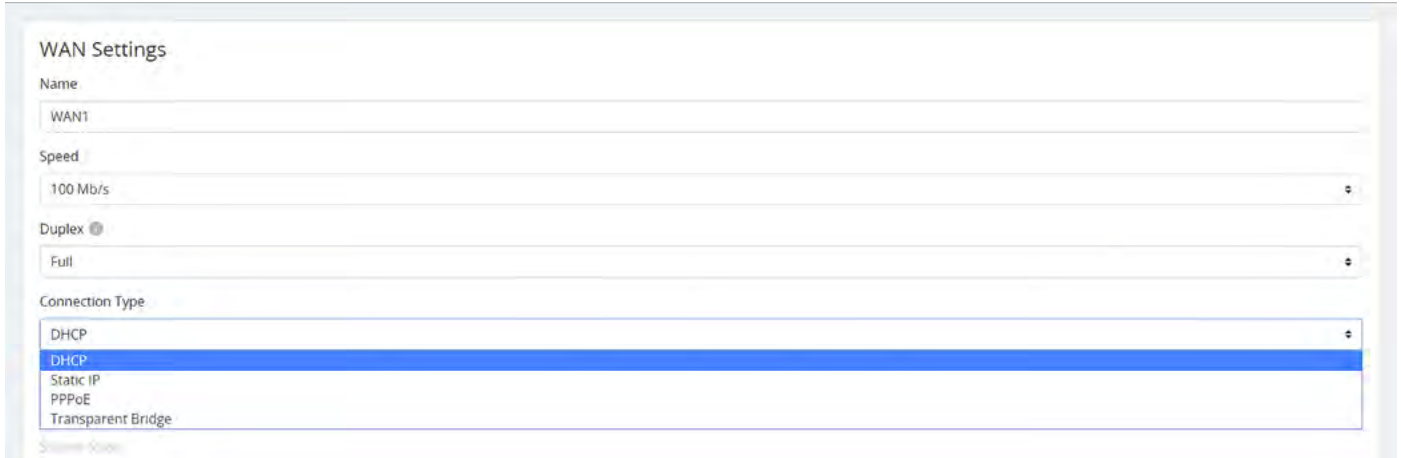
For best network performance, set your router to reboot on a regular basis (preferably when no one is likely to be using it). When enabled, select either weekly or monthly, then select the day(s) of the week, or the day of the month, as appropriate. Finally, choose the time of day.

For best performance with multiple auto-rebooting devices, reboot the network devices in this order: modem, router, switch, access points.

Settings > WAN

WAN Settings Section

Here you set the WAN port's name and connection speed.



The screenshot shows the WAN Settings configuration page. The 'Name' field is set to 'WAN1'. The 'Speed' dropdown is set to '100 Mb/s'. The 'Duplex' dropdown is set to 'Full'. The 'Connection Type' dropdown menu is open, showing options: DHCP (highlighted in blue), Static IP, PPPoE, and Transparent Bridge. Below the dropdown, there is a 'Show More' link.

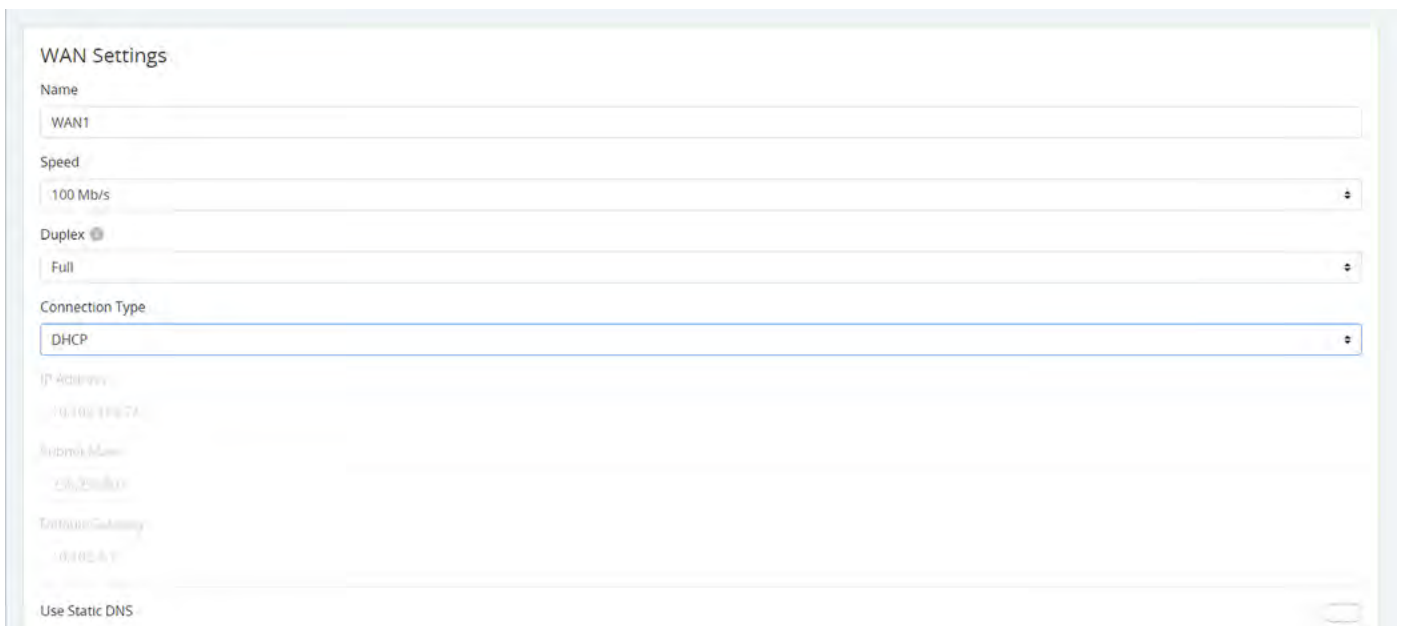
The top shows the WAN being edited.

Select the WAN port's speed and, if the speed is not set to Auto, their duplex setting.

You can also set the type of WAN connection you want to use. Each selection displays different customization options in the center of this dialog, as shown here.

... With DHCP Selected

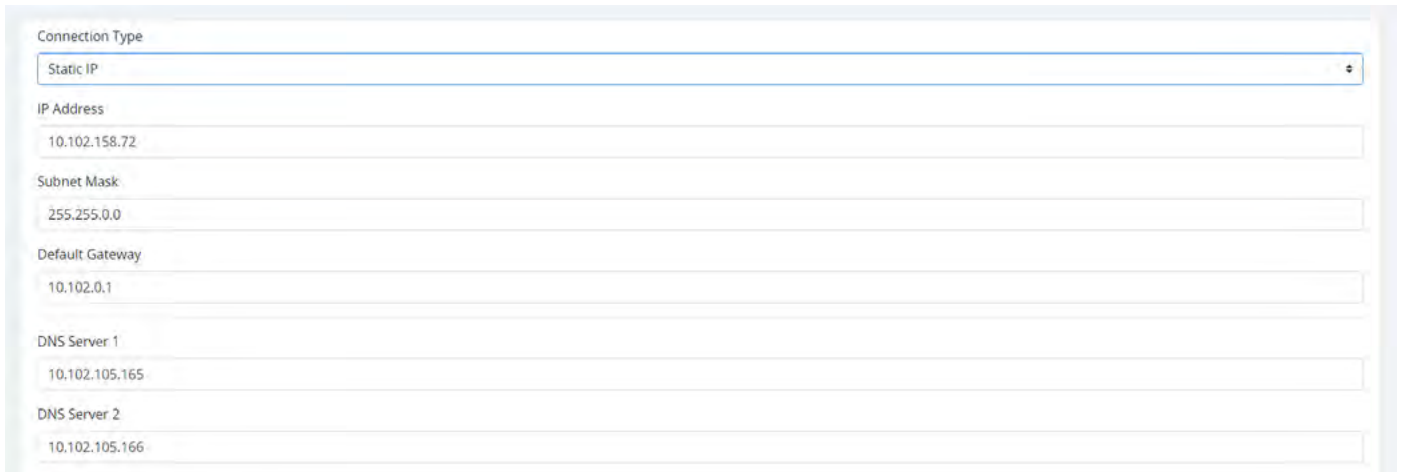
This sets the WAN port to use DHCP (automatically negotiating IP settings with your ISP).



The screenshot shows the WAN Settings configuration page with 'DHCP' selected in the 'Connection Type' dropdown. Below the dropdown, the following fields are visible: 'IP Address' (192.168.1.1), 'Subnet Mask' (255.255.255.0), and 'Gateway' (192.168.1.1). There is a checkbox for 'Use Static DNS' at the bottom.

... With Static IP Selected

This sets an unchanging IP address for the WAN. Using this is dependent on your ISP and service plan.

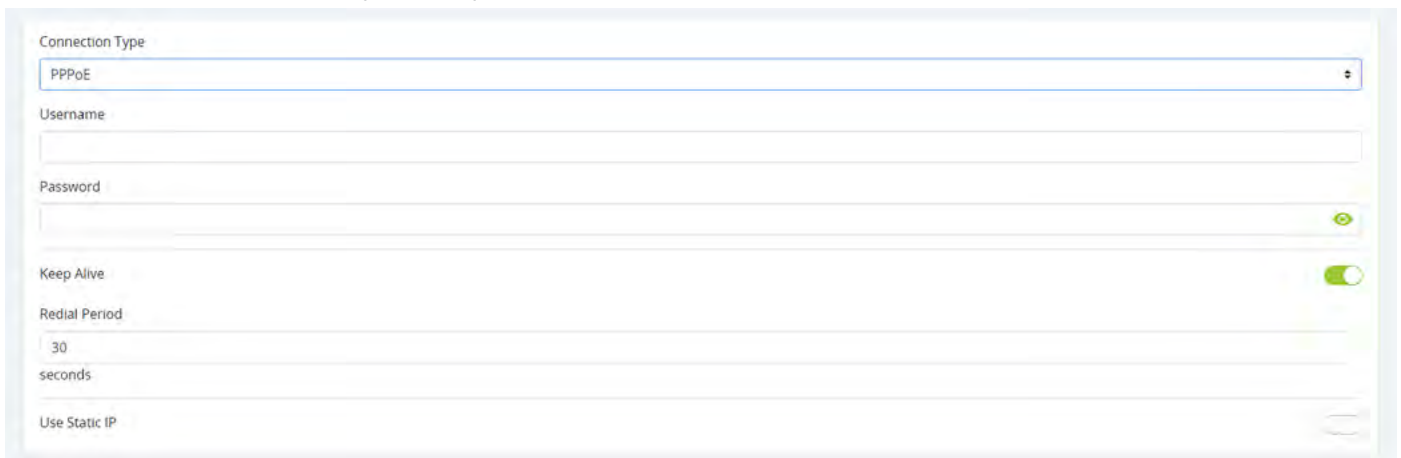


The screenshot shows the WAN configuration interface with the following fields:

- Connection Type: Static IP
- IP Address: 10.102.158.72
- Subnet Mask: 255.255.0.0
- Default Gateway: 10.102.0.1
- DNS Server 1: 10.102.105.165
- DNS Server 2: 10.102.105.166

... With PPPoE Selected

Use this for DSL and other peer-to-peer connections.

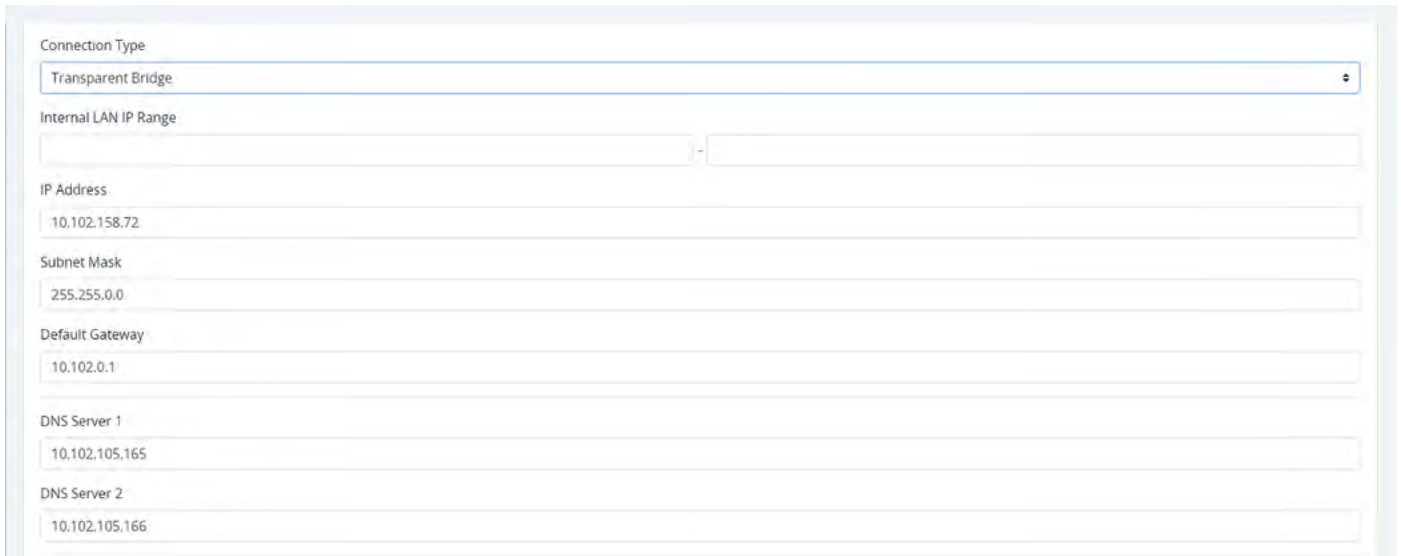


The screenshot shows the WAN configuration interface with the following fields:

- Connection Type: PPPoE
- Username: (empty)
- Password: (empty)
- Keep Alive: (checked)
- Redial Period: 30 seconds
- Use Static IP: (unchecked)

... With Transparent Bridge Selected

This disables all routing functions on your router. Use this if there is an ISP-provided router that must sit on the network.



The screenshot shows the WAN configuration page with 'Transparent Bridge' selected in the 'Connection Type' dropdown. Below this, several input fields are visible: 'Internal LAN IP Range' (empty), 'IP Address' (10.102.158.72), 'Subnet Mask' (255.255.0.0), 'Default Gateway' (10.102.0.1), 'DNS Server 1' (10.102.105.165), and 'DNS Server 2' (10.102.105.166).

... And at the Bottom:

At the bottom, you can set the MTU (maximum transmission unit) either automatically or manually. For most purposes, leave Auto MTU selected and active so that the router can negotiate with the ISP.


The WAN's negotiated (or fixed) speed appears at the bottom of the section. If it shows in green, the WAN is operational. If the WAN is not operational, this shows as gray.



The screenshot shows the 'Auto MTU' section with a checked checkbox and a value of '1500'. At the bottom of the section, a green bar indicates the WAN speed is '15Mbps'.

Release Button: Click to release the current WAN IP address back to the DHCP pool and clear any WAN related IP settings.

Renew Button: Click to renew the current WAN DHCP connection. The WAN IP address may or may not change.

 **Pro Tip:** The Renew and Release buttons only take effect when DHCP is the connection type.

Multi-WAN Section

Network Service Detection regularly checks to ensure that the network connection is active, using a ping test and/or a Domain Resolution test. If it detects that the network is inactive, it performs the action selected in the dropdown.

Multi-WAN

Network Service Detection

Retry Count

Time Between Retries
seconds

Action

When Network Service Detection is enabled, you can opt to use any or all of the three detection methods listed to ensure your router is connected to the internet.

Detection Methods

Ping Default Gateway

Ping Remote IP(s)

IP	<input type="checkbox"/>
<input type="text" value="8.8.8.8"/>	<input type="checkbox"/>
<input type="text" value="4.2.2.2"/>	<input type="checkbox"/>
<input type="text" value="Add IP Destination"/>	

Resolve Domain Name(s)

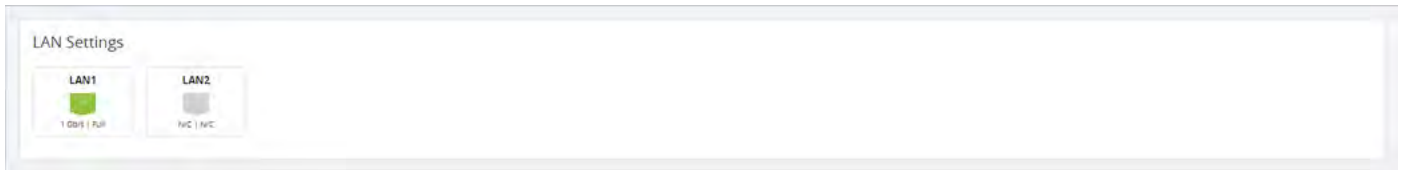
URL	<input type="checkbox"/>
<input type="text" value="www.google.com"/>	<input type="checkbox"/>
<input type="text" value="Add URL"/>	

Ping Default Gateway refers to the default of of WAN 1 (if more than one WAN is available).

Alternatively, you can add up to ten IPs (entered as IPv4 addresses) or three URLs to check.

Settings > LAN

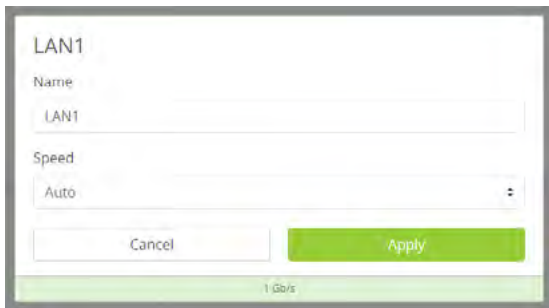
LAN Settings Section



Names can be up to 63 characters long, and can contain letters, numbers, hyphens, underscores, commas, periods, and the following special characters: ! @ # \$ % ^ & * ? +. It cannot contain spaces.

This shows the LANs available, their speed (color coded), and their duplex settings. Each port is color-coded based on its negotiated speed:

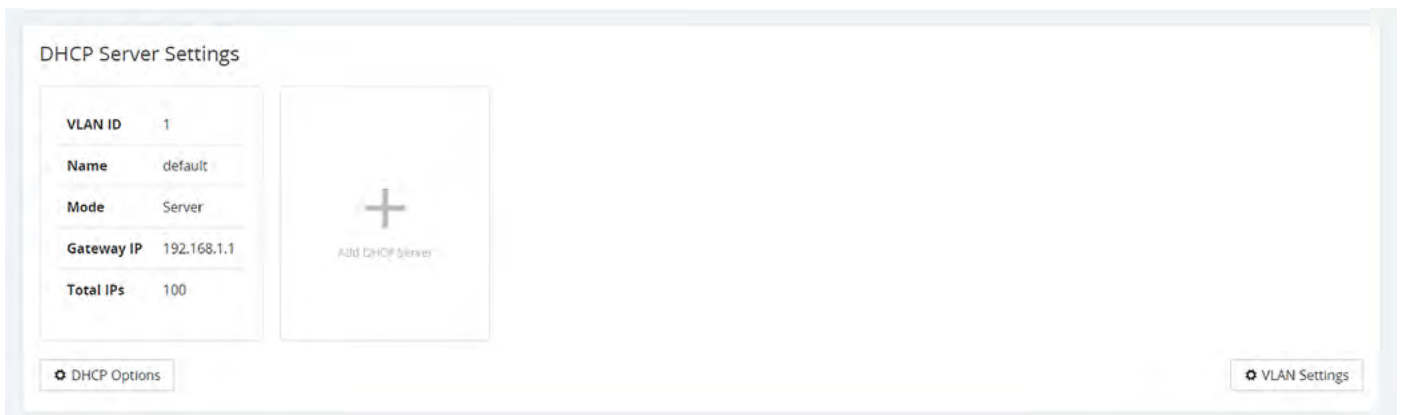
- **Gray:** Not connected to a device, or the connected device has not negotiated a speed.
- **Orange:** 10/100Mbps connection is active.
- **Green:** 1Gbps connection is active.
- **Red:** Port has been disabled by the user in the web interface settings.



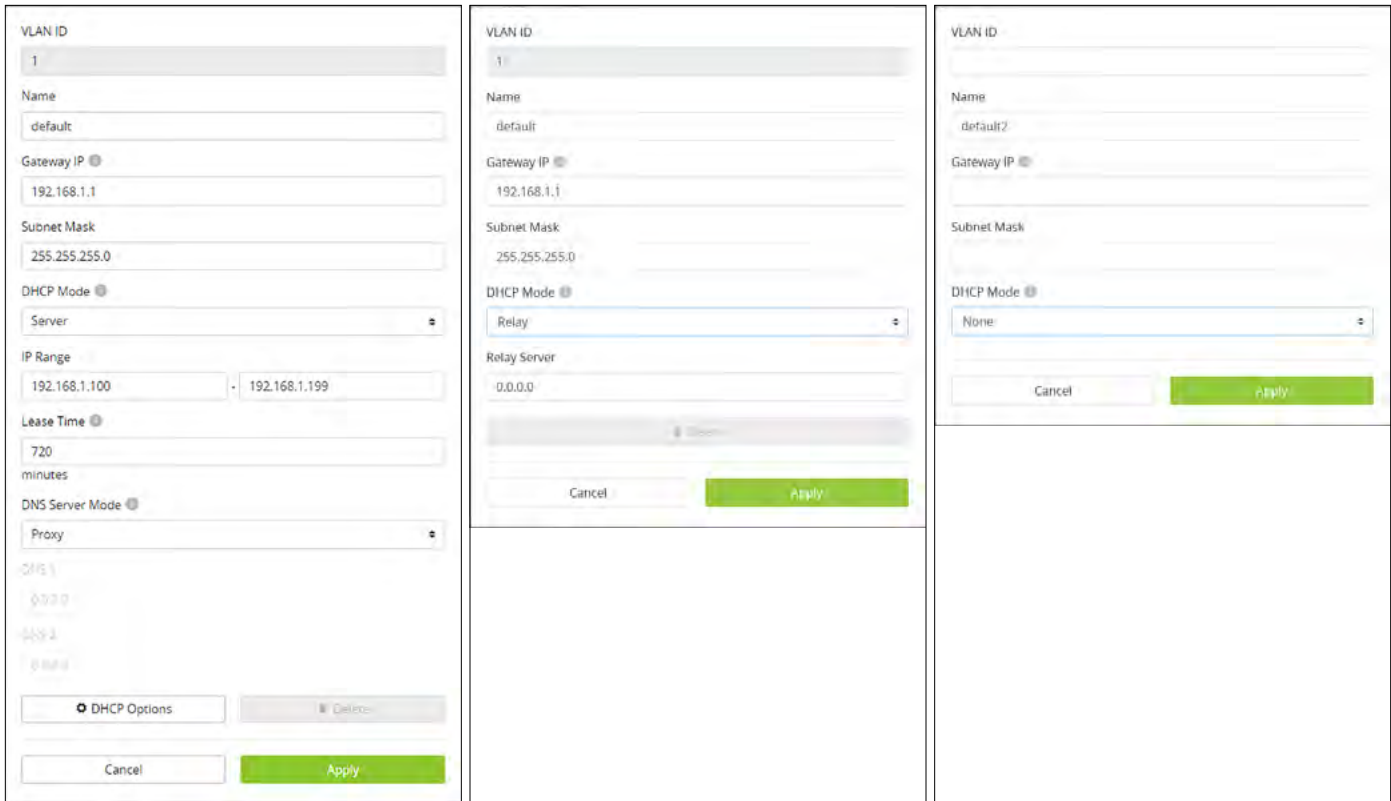
Click on a port to open a dialog where you can change the LAN's name, speed settings, and duplex setting (if the port is not set to auto). This also shows the actual speed at bottom, color coded as normal.

DHCP Server Settings Section

This shows the current information about the router's configured subnets. Depending on how your system is set up, there may be several of these. Click on a card to edit that subnet's settings (including several options not shown in the summary). Add a new subnet by clicking the **+ Add DHCP Server** card.



VLAN Settings Button: This takes you directly to the **Advanced > VLANs** page.

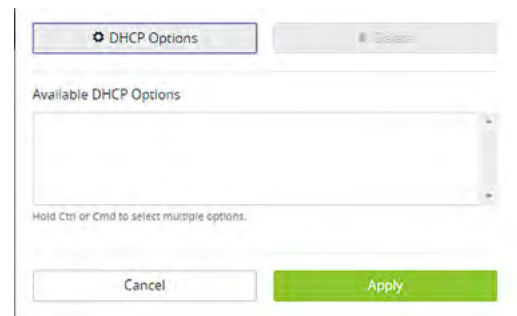


Click on an existing subnet card, or adding a new DHCP Server, opens a dialog for you to set VLAN parameters. The options change (as shown above) based on whether you set the DHCP mode to None, Relay (which forwards DHCP requests to a separate device that serves as that network’s DHCP server), or Server.

The VLAN ID ranges from 1–4095; duplicating an entry increments the previous entry. Note that setting the VLAN ID also adjusts the Gateway IP and IP Range fields (and vice versa).

The Gateway IP for the default card is the IP at which the router’s UI is accessible.

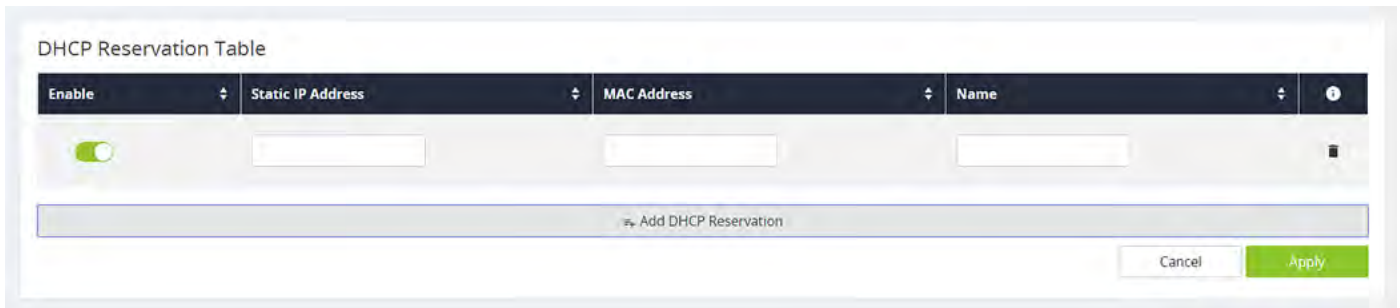
DHCP Options Button: This opens a dialog for adding DHCP rules to your router. Any options that were set up are available globally and can be included in a DHCP server card. You can use the Shift and Command keys to select multiple DHCP Options at once.



Note – This is a feature that most generic network setups do not need. These rules should be set up by an IT administrator.

DHCP Reservation Table Section

This shows a list of all DHCP addresses reserved by your system.



Click the **Add DHCP Reservation** button to a device. The IP address must be in IPv4 format.

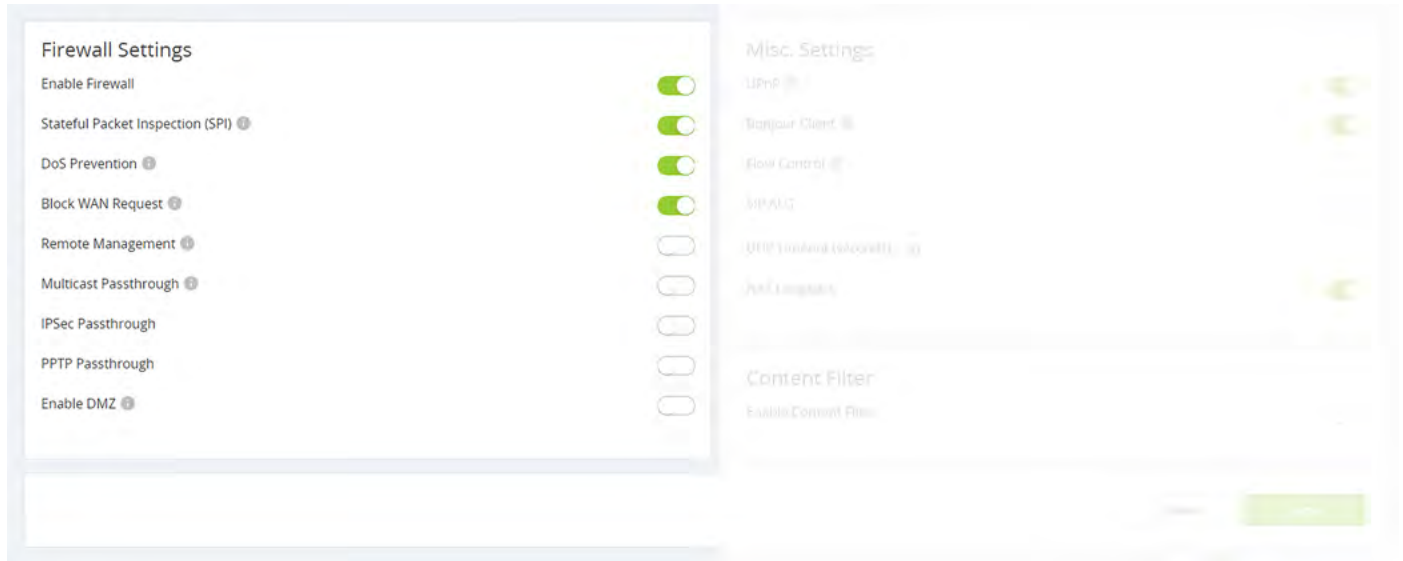
The color bar at the left end of each line shows whether that client is up (green) or down (gray). For DHCP addresses, click on the clock icon to show the remaining lease time. To reserve a DHCP address, click on the + icon to the left of the trash can icon.

Clicking the trash can removes that device's DHCP reservation. You'll need to reboot the device to have it request a new IP address from the router.

Settings > Firewall

This covers the router's built-in firewall capabilities. Each of these provides added security to your system.

Firewall Settings Section



When the firewall is enabled, you can activate any or all of:

- **Stateful Packet Inspection (SPI)** to check incoming and outgoing data for anomalies
- **DoS Prevention** to thwart denial of service attacks
- **Block WAN Request** to keep external connections from accessing your network

Remote Management: This allows you to access the router from offsite. However, we suggest you leave this disabled and use OvrC instead. See OvrC.com for details.

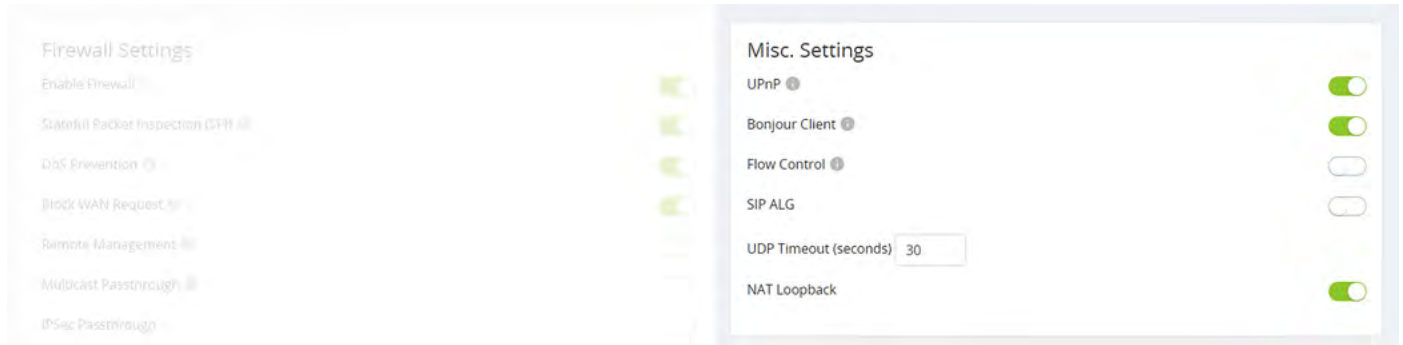
Multicast Passthrough: This enables multicast traffic to pass from WAN to LAN. Typically used in the event a multicast source is on the WAN side of the network.

IPSec Passthrough: This allows IPsec VPN traffic to pass from WAN to LAN. Typically used in Double NAT topologies wherein there is an IPsec tunnel established upstream to the WAN side of this router.

PPTP Passthrough: This allows PPTP VPN traffic to pass from WAN to LAN. Typically used in Double NAT topologies wherein there is a PPTP tunnel established upstream to the WAN side of this router.

Enable DMZ: Some ISPs do not support bridging to bypass any NAT or firewall rules in place. In such cases, DMZ allows access to the network. You are required to enter the DMZ address in IPv4 format.

Misc. Settings Section



UPnP: This enables Universal Plug and Play, a protocol that permits the network to discover and operate devices and applications seamlessly.

Bonjour Client: Bonjour is Apple's implementation of Zero Configuration networking, which allows users to search, locate and set up Apple Access Points.

Flow Control: This feature implements IEEE 802 protocols around managing congestion on the network. It is normally not needed; please contact technical support if you are considering enabling this feature.

SIP ALG: This enables or disables the Application Layer Gateway, a feature that inspects and modifies VOIP traffic for intended optimization depending on system compatibility. Please consult your VOIP hardware and service provider for whether this feature should be enabled.

UDP Timeout: For VOIP systems, this feature enlarges the udp session timeout to ensure persistent connectivity of VOIP devices. Serves as Consistent NAT.

NAT Loopback: NAT Loopback is needed for using remote access mechanisms like DDNS while being on the network itself.

This is used primarily with cameras/NVRs to use a common schema for accessing cameras whether remote or local to the network.

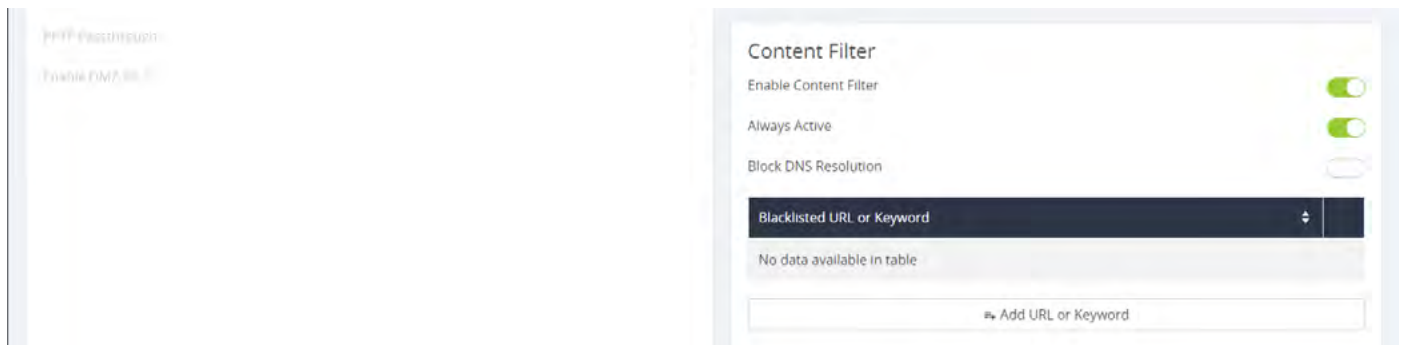
Content Filter Section

The Content Filter feature is designed to block selected URLs or websites with selected offensive terms.

When enabled, the filter can be active 24/7, or you can set times and days for the filter to be in operation.

Block DNS Resolution blocks access to HTTPS sites.

Use the button at the bottom to add a new term or URL to the blacklist.





Settings > DDNS

WAN DDNS Settings

Enable

Service
AraknisDNS.com

Host Name
 Register AraknisDNS.com

WAN IP Address

Cancel Apply

WAN DDNS Section

Dynamic DNS allows you to access the router web interface and other network devices from the Internet using a standard web URL instead of the WAN IP address.

Select which DNS service you want to use, then enter your desired URL into the host name text box. Press the **Register** button to implement it. If that specific URL has already been used, the system typically adds a unique ID (often two to four digits) to your domain. If you do not like this assignment, try another domain or DNS service.

Example: If you choose the domain myhome, your system's URL is myhome.AraknisDNS.com. If someone has already claimed the myhome URL, then your system's URL could be something like myhome13.AraknisDNS.com.

Settings > Port Forwarding

The External Address field displays the WAN IP for the system.

Network ports direct traffic between software applications running on network devices. Port numbers are always associated with a host IP address and a protocol type, usually TCP, UDP, or both (TCP/UDP).

Network HTTP traffic defaults to TCP port 80. When an address is entered in the web browser, the request is automatically sent to port 80 unless a different port is appended to the address. For example, if you access a device at IP address 192.168.1.20, the request actually processes as if you entered 192.168.1.20:80.

When software from LAN devices need access to and from the internet, additional ports may be forwarded to the device to allow communication through the router firewall. Common uses for port forwarding include:

- Remote access for surveillance cameras and recorders
- Computer games and server applications
- Remote storage devices
- Remote access for network device user interfaces (WAPs, managed switches, power monitoring devices)

Note - Many popular programs and protocols are set to use specific port numbers by default. For instance, HTTPS services typically use port 443, and SMTP mail services typically use port 25.

Port Forwarding Section

Port Forwarding

Enable	Protocol	External Port	External Address	Internal Port	Internal Address	Description
<input checked="" type="checkbox"/>	TCP		WAN: [IP]			

[Add Forwarding Rule](#)

Port Triggering Section

Use port triggering to enable ports only when needed by watching internal ports for activity.

Port Triggering

Enable Port Triggering

Enable	Trigger Ports	Forwarded Ports	Description
<input checked="" type="checkbox"/>			

[Add Port Trigger](#)

[Cancel](#) [Apply](#)

Settings > Security

User Accounts Section

Here you can create new accounts to access the router. We recommend that you do not give anyone access to the default account.

⚡ Caution - To protect your system, it is vital that you change the default credentials on the admin account. The default username is *araknis* and the default password is *araknis*. Please change the account name (to something other than *admin*) and also create a unique password. It's best if neither the account name nor password can be found in the dictionary.

Username	Password	Confirm Password
araknis	<input type="password"/>	<input type="password"/>
newUser	<input type="password"/>	<input type="password"/>

[Add User](#)

Access Management Section

Enabling HTTPS encrypts all user access communication with your router. When enabled, you must specify a port to use. By default, this feature uses port 443; we strongly recommend you use a different port for HTTPS communication.

Access Management

Enable HTTPS

Port:

MAC Based Access Management

MAC Address List

MAC Address
No data available in table

[Add MAC Address](#)

Before you enable access management, first change the admin username and password from their default values; access management cannot be enabled until these are changed.

☰ Note - If you enable access management, and then change the default admin credentials, the credential changes and HTTPS enablement activate simultaneously. If you are remote, this could cause you to lose connection with your router.

Access management has no impact on DDNS.



Access management can work even if there is a port forward rule back to the router's IP. As long as the access management port isn't the same as the external port in the remote management section, both can work on the system concurrently.

Example: You enable access management on port 7000, and port forwarding to the routers IP address at port 6001. You can then remotely access the router at either <https://example.araknisdns.com:7000> or <https://example.araknisdns.com:6001>

You **must** port forward the external port to the internal port specified for the HTTPs setting on the security page for this to work in the way you've written it.

You can also limit access to your router to include only select devices (up to 16) by enabling **MAC Based Access Management**. Click the **Add MAC Address** button to their MAC addresses here.

Similarly, you can enable **IP Based Access Management** to restrict access to your router to include only devices at certain IP addresses within your network.

Note that IP and MAC methods are mutually exclusive.

Whitelist & Blacklist Section

The whitelist and blacklist are tools that allow you to permit or block access of network devices to your router (gateway) and thus the internet. Specify the network devices that you wish to permit or block using either their IP or MAC addresses.

The screenshot displays two side-by-side configuration panels for security settings. The left panel is titled 'Whitelist' and the right panel is titled 'Blacklist'. Both panels have an 'Enable' toggle switch that is turned on (green). Each panel features a dropdown menu for 'IP/Mac Address' with a search icon and a refresh icon. Below this is a text input field containing the example address '192.168.0.1 OR A8:86:DD:B1:4D:7F' and a trash icon. A button labeled 'Add IP or MAC Address' is positioned below the input field. Each panel also has an 'Always Active' toggle switch that is turned off. Below this are 'From' and 'To' time selection fields, both set to '12:00'. At the bottom of each panel is a day-of-the-week selector with buttons for S, M, T, W, T, F, S. At the bottom right of the entire interface are 'Cancel' and 'Apply' buttons.

When using the whitelist, all devices except for your entries are blocked.

When using the blacklist, all devices except for your entries are permitted.

You can also set the blacklist and whitelist to be always active or to operate on a schedule. The whitelist and blacklist cannot have overlapping schedules.

Wireless > Status (WI-Fi model only)

Provides a detailed look at wireless settings and performance for radio status and settings, wireless network configuration and connected client status.

Radio Interfaces Section

This provides key data on the router’s wireless configuration. It cannot be edited; it is for informational purposes only.

Radio Interfaces		
	2.4 GHz	5 GHz
Interface Status	Enabled	Enabled
Operation Mode	Access Point	Access Point
Wireless Mode	B/G/N	A/N/AC
Channel Bandwidth	20 MHz	80 MHz
Channel Selection	Auto	Auto
Operation Channel	8	48
Channel Frequency	2.447 GHz	5.240 GHz
SSIDs Used	1/8	1/8


Wireless Networks Section

This lists all the wireless networks you have set up on your router.

Wireless Networks	
SSID	1
Name	araknis_initial
Interface	Both
VLAN	1

Wireless Clients Section

This lists all devices currently attached to one of your wireless networks.

SSID	Device Name	MAC	RSSI(dBm)	TX	RX	BAN
araknis_initial	iPhone	38:89:2C:C1:E8:BF	-87	2.5 KB	768 B	

Wireless > Settings (WI-Fi model only)

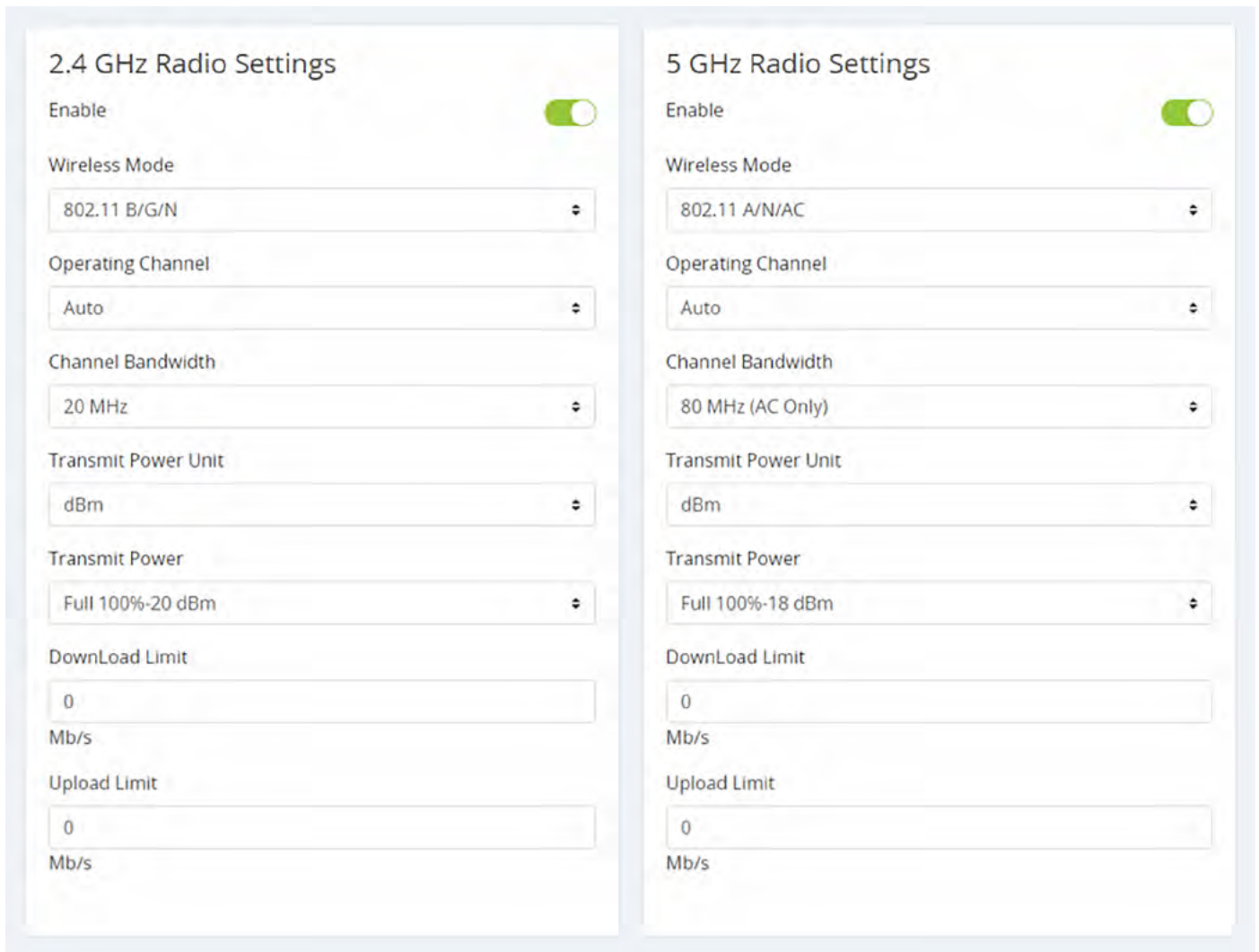
Global Settings Section

The band steering feature encourages dual-band client devices to stay on the 5 GHz band. This frees up resources on the 2.4 GHz band for single-band clients.



Radio Settings Sections

Here you can customize how your Wi-Fi works, or disable select bandwidths.



Wireless Mode: We recommend you leave this at 802.11 B/G/N.

Operating Channel: Select the desired Wi-Fi channel. Use a different channel than other Wireless Access

Devices on the network. On the 2.4GHz radio, there are only three non-overlapping channels: 1, 6 and 11. Select a channel as far away from close-numbered channels as possible.

Channel Bandwidth: Select the desired channel bandwidth. Smaller values allow greater range and larger values provide greater throughput. The combination setting allows the Wireless Access Device to decide.

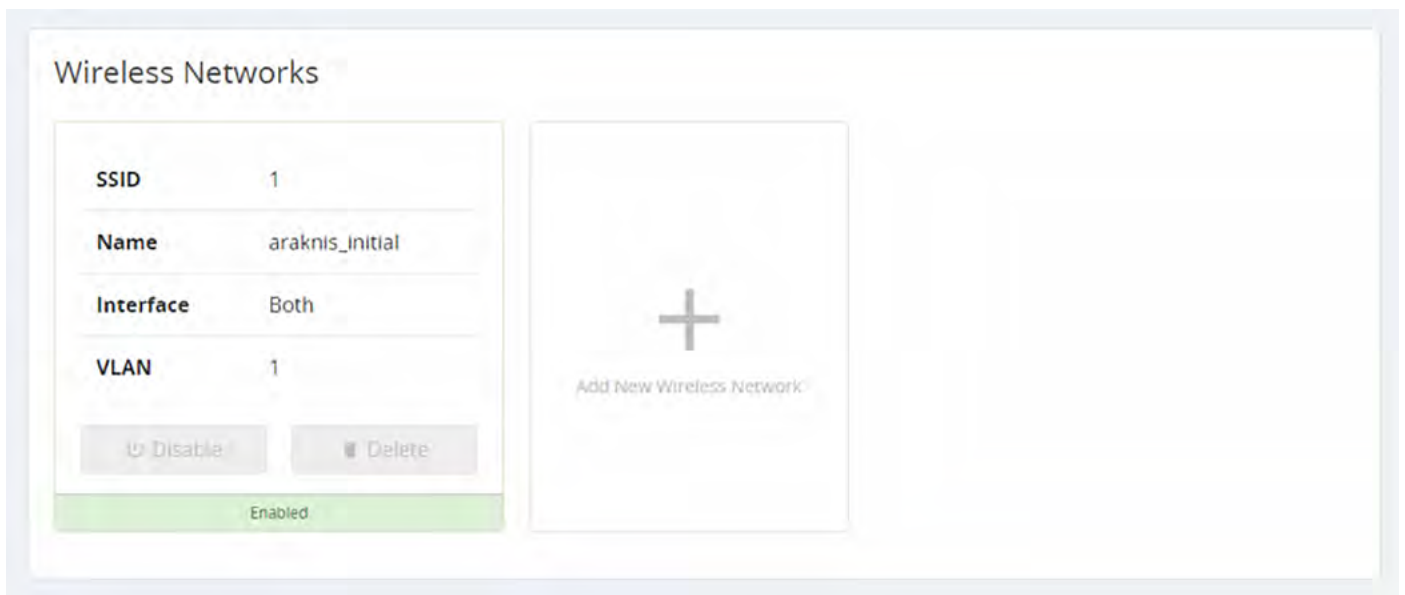
Transmit Power Unit: Select the preferred unit of measure.

Transmit Power: Use the dropdown to set the radio power. Higher power improves performance but can cause interference with other wireless access devices in close range on the same channel. Also, a higher coverage range corresponds with lower throughput (i.e., to achieve the highest transmit power, the connection must run at the lowest data rate). Set this value as low as possible (for adequate coverage) to get the maximum wireless speed / data throughput.

Download Limit and Upload Limit: These place speed caps on those activities so they don't hog all available bandwidth and slow your network.


Wireless Networks Section

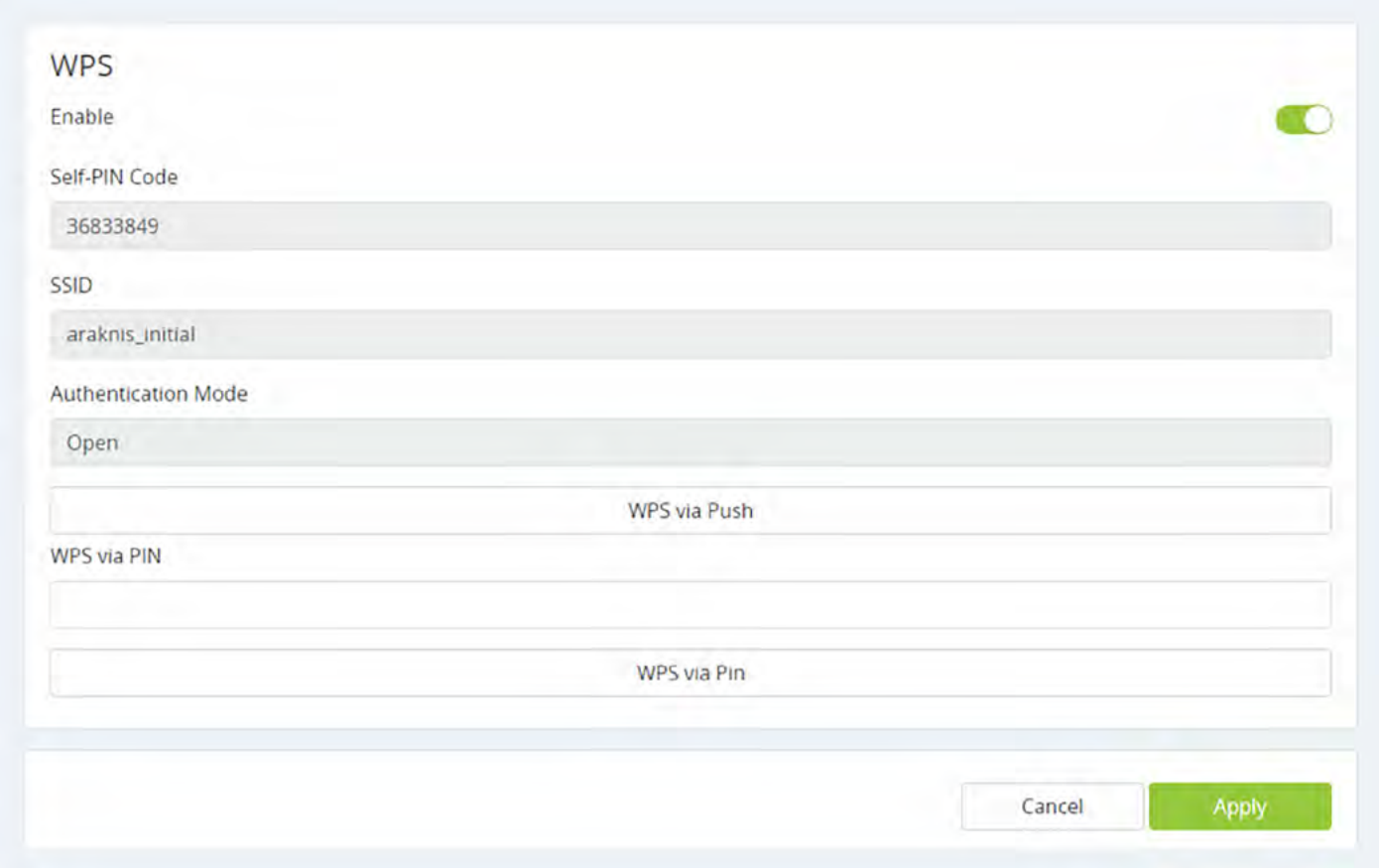
This lists all wireless networks on your system. Press the **+ Add New Wireless Network** button to create a new one (for example, a guest network).



WPS Section

WPS (Wi-Fi Protected Setup) allows setup of WPS-equipped Wi-Fi devices. Instead of sharing the SSID and security credentials with a client, WPS connects clients using a push button or PIN entry method.

 **Note** - We do not recommend using this. Leaving it enabled can lead to unauthorized access via an exploit.



WPS

Enable

Self-PIN Code
36833849

SSID
araknis_initial

Authentication Mode
Open

WPS via Push

WPS via PIN

WPS via Pin

Cancel Apply

WPS via Push

This requires WPS to be enabled, as well as a client device equipped with a WPS Push Button.

Power on the WPS-enabled client device to be connected.

Press the WPS button on the client device, then click the WPS via Push button in the WAP interface.

The device connects. Test connectivity to the device to ensure Wi-Fi operation.

WPS via PIN

This requires WPS to be enabled, as well as a client device equipped with WPS via PIN.

Power on the WPS enabled client device to be connected.

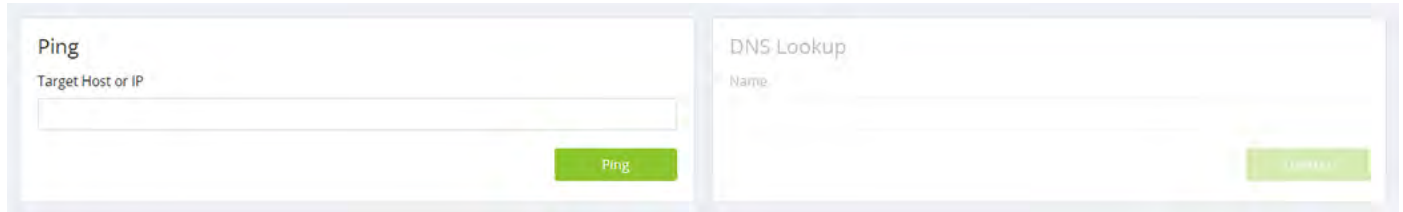
In the interface above, enter the WPS PIN from the client device in the WPS via PIN field, then click Apply.

The device connect. Test connectivity to the device to ensure Wi-Fi operation.

Tools

Ping Section

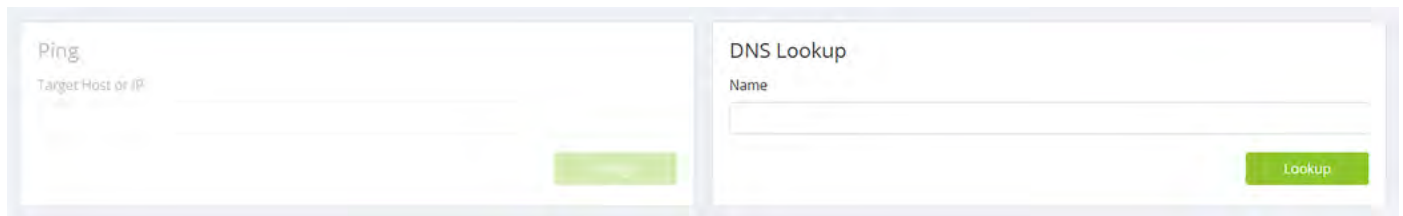
Enter an IP address here and click the Ping button to see if the target device responds. If it does, the system displays a measure of how long it took the device to respond.



The screenshot shows two adjacent panels. The left panel is titled "Ping" and contains a text input field labeled "Target Host or IP" and a green "Ping" button. The right panel is titled "DNS Lookup" and contains a text input field labeled "Name" and a green "Lookup" button.

DNS Lookup Section

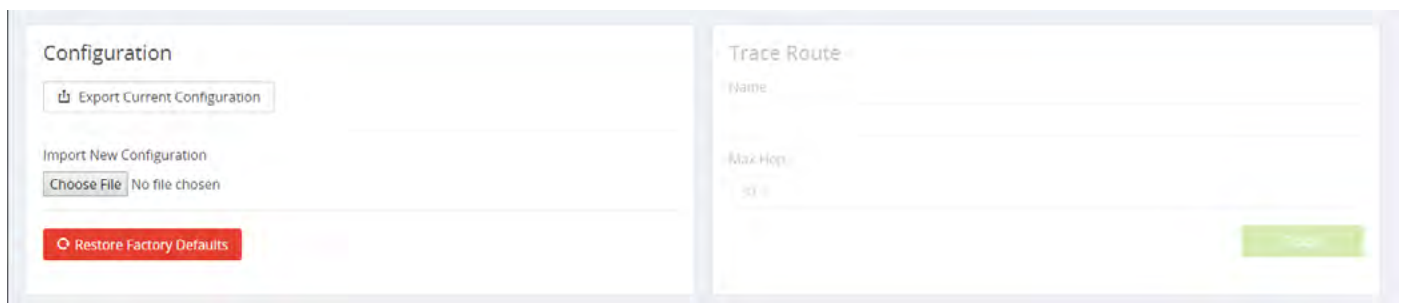
This tool provides a mechanism to resolve a domain name to an IP address. Enter the URL and press the **Lookup** button.



The screenshot shows the "DNS Lookup" section, which includes a text input field labeled "Name" and a green "Lookup" button.

Configuration Section

Here you can export your router's configuration (we highly recommend this before each you update the firmware), import a new configuration file, or restore the router to its factory default settings.



The screenshot shows two adjacent panels. The left panel is titled "Configuration" and contains three main sections: "Export Current Configuration" with a button, "Import New Configuration" with a "Choose File" button and "No file chosen" text, and "Restore Factory Defaults" with a red button. The right panel is titled "Trace Route" and contains a text input field labeled "Name", a "Max Hop" input field, and a "Start" button.

Trace Route Section

This displays all relays between your router and the target URL, as well as the delays encountered by the data packet sent.

The screenshot shows the 'Trace Route' configuration section. On the left, under 'Configuration', there are buttons for 'Export Current Configuration', 'Import New Configuration' (with a 'Choose File' button and 'No file chosen' text), and 'Restore Factory Defaults'. On the right, the 'Trace Route' section has a 'Name' input field, a 'Max Hop' input field with the value '30', and a green 'Trace' button.

The screenshot shows the 'Trace Route' result page. The 'Name' field contains '30.0.0.4'. A red 'Stop' button is visible. The 'Result' section displays a text box with the following output:

```
tracert to 30.0.0.4 (30.0.0.4), 30 hops max, 38 byte packets
 1 10.102.0.1 0.900 ms 0.580 ms 0.700 ms
 2 172.24.8.1 11.420 ms 12.300 ms 11.720 ms
 3 69.20.61.2 12.040 ms 12.460 ms 12.360 ms
 4 69.20.3.22 13.060 ms 12.740 ms 12.460 ms
 5 69.20.2.98 13.460 ms 69.20.2.114 12.600 ms 12.560 ms
 6 69.20.2.172 13.180 ms 69.20.2.160 13.020 ms 69.20.2.164 12.900
ms
 7 10.25.2.95 13.320 ms 12.760 ms 10.25.2.79 13.220 ms
 8 62.115.32.121 13.020 ms !N **
 9 **
```

Enter the IP address of a device or web page. Click the **Start** button.

The system displays the path of communication to that device or website. Click **Stop** if the test is taking too long.

Firmware Settings Section

This gives all pertinent data about the router's current firmware. You can update the firmware at the bottom of this area. Allow 30 seconds for the upload of firmware to take effect, and 10 minutes for a firmware update to complete.

When possible, we recommend updating firmware using OvrC.

The screenshot shows the 'Firmware Settings' page. It displays the following information:

- Active: Partition 1
- Version: 0.2.6
- Build Date: Sep. 28 2018 11:47:51
- Image Name: IMG-[0.2.6]
- Image Size: 44.62 MB

At the bottom, there is an 'Update Firmware' section with a 'Choose File' button and 'No file chosen' text, and a red 'Update' button.

Advanced > Static Route

Static routing is used to create routes to other subnets using a fixed routing table.

Static routes are commonly used to allow traffic between subnets on different routers. For example, in a large office network, there is a subnet configured for the first floor inside of Router 1 with the IP address 192.168.1.0. Computers on the third floor are connected to Router 2 using subnet 192.168.30.0, and they need to communicate with the 192.168.1.0 subnet. A static route is configured in each router to the port connecting them.

Routing Table Section

The routing table displays default routing information for the router. Use this information to troubleshoot and set up static routes.

Destination	Netmask	Gateway	Interface
Default	0.0.0.0	10.102.0.1	WAN
10.102.0.0	255.255.0.0	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN
239.0.0.0	255.0.0.0	0.0.0.0	LAN

Static Route Table Section

Use this to add entries to the table above.

Subnet	Subnet Mask	Gateway	Interface
<input type="text"/>	<input type="text"/>	<input type="text"/>	LAN
+ Add Static Route			
			<input type="button" value="Cancel"/> <input type="button" value="Apply"/>

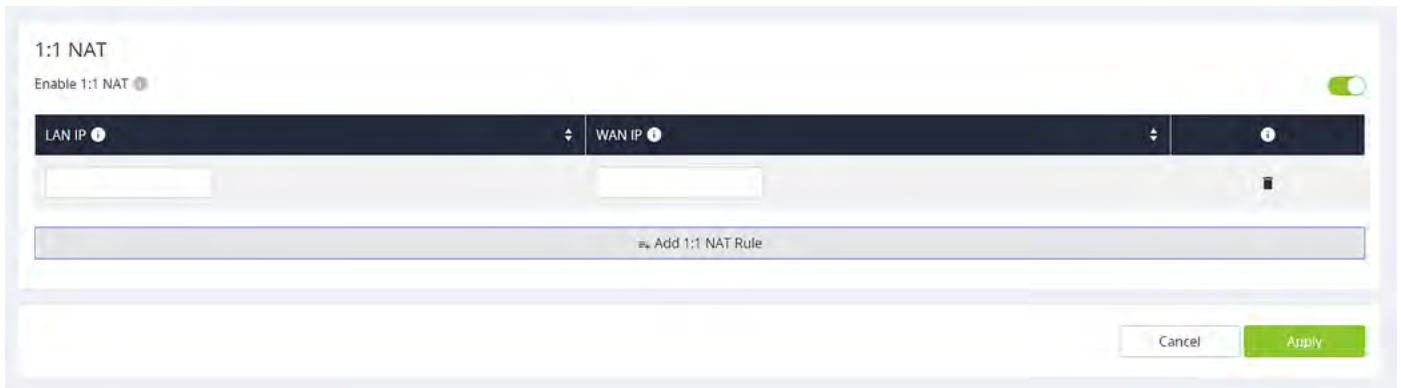
- **Subnet:** Subnet used on the interface specified below.
- **Subnet Mask:** Subnet mask of the interface specified below.
- **Gateway:** Gateway IP address of the interface specified below. The asterisk symbol (*) indicates a wild card.
- **Interface:** References the LAN or WAN entry from the routing table. If your system has more than one LAN and/or WAN, the dropdown also specifies the number.

Advanced > NAT

This configures devices on the LAN so that they appear to have a specific public (WAN) IP address. You must enable this to use and edit NAT entries.

1:1 NAT Section

This shows all NAT entries in tabular format.



The screenshot displays the '1:1 NAT' configuration page. At the top left, the title '1:1 NAT' is shown. Below it, there is a toggle switch labeled 'Enable 1:1 NAT' which is currently turned on. The main area contains a table with two columns: 'LAN IP' and 'WAN IP'. Each column has a dropdown arrow and a help icon. Below the table, there is a button labeled 'Add 1:1 NAT Rule'. At the bottom right of the page, there are two buttons: 'Cancel' and 'Apply'.

To create a new entry, click the Add 1:1 NAT Rule button.

- **LAN IP:** Enter a single IP address or a range to be represented by the specified WAN IP address.
- **WAN IP:** Enter the desired public IP address for use.

Click the Trashcan to delete an existing line from the table

Advanced > VLANs

Virtual Local Area Networks (VLANs) are used to segment traffic on the LAN. Proper setup and use of VLANs can increase the reliability and security of the network.

VLANs Section

To create a new VLAN, click the **+ Add VLAN** button, and enter the parameters below. Each VLAN can have a customized number, except for the default VLAN, which is always set to 1.

VLAN ID	Description	Inter VLAN Routing	Device Management	LAN1	LAN2
1	Default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Untagged	Untagged
		<input type="checkbox"/>	<input type="checkbox"/>	Excluded	Excluded

+ Add VLAN

Cancel Apply

- **Description:** A cue for you to help identify the VLAN's purpose.
- **Inter VLAN Routing:** Select whether routing between VLANs is enabled or disabled. This allows communication between those client devices residing on those VLANs.
- **Device Management:** This permits devices on this LAN access to the gateway (this router).
- **LAN#:** Configure the LAN ports on the router for the VLAN. A port may be configured as one of one following options:
 - **Untagged:** The port is a member of the specified VLAN. VLAN frames handled through this port are not tagged with a VLAN ID.
 - **Tagged:** The port is a member of the specified VLAN. VLAN frames handled through the port are tagged with a VLAN ID.
 - **Excluded:** The port is not a member of the specified VLAN. This is the default setting.

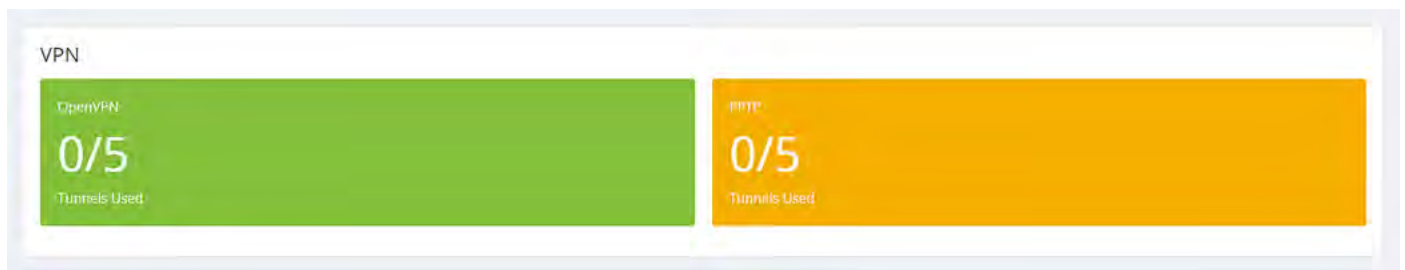
Click the trashcan to delete an existing VLAN. The default VLAN cannot be deleted.

Advanced > VPN

A Virtual Private Network (VPN) provides a connection between different networks through a secure tunnel over the Internet. Data sent through the VPN tunnel is encrypted for privacy even when connected to a public or shared network that isn't secure. VPNs are commonly used to send data between networks in different geographical locations without requiring a dedicated physical connection between the networks. VPNs may be configured via the OpenVPN or PPTP standard.

VPN Section

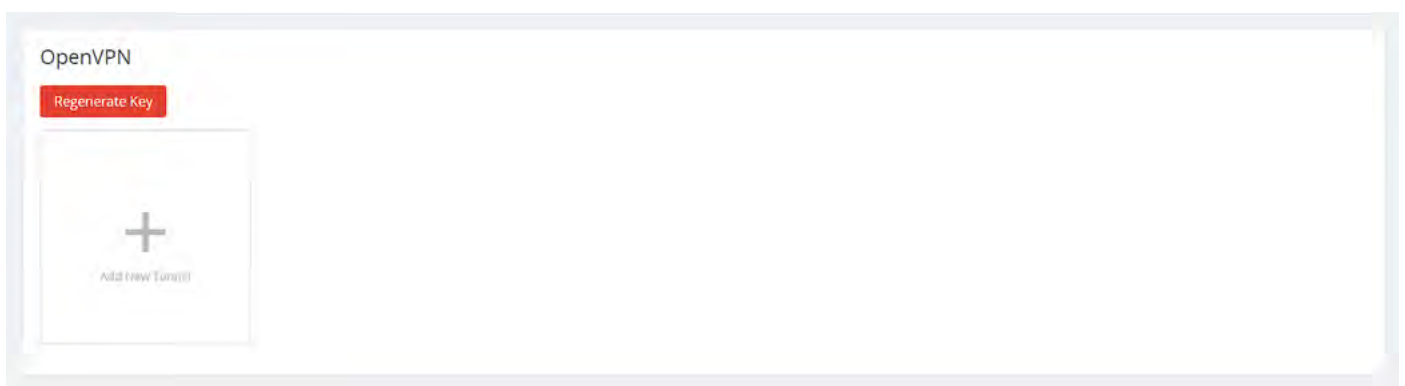
The router can support a maximum of five OpenVPN, as well as five PPTP tunnels. Both types can be active simultaneously.



Open VPN Section

The AN-110 family of routers feature a built-in OpenVPN server for secure, easily configured access to the network from the Internet using devices with an OpenVPN client application. Use OpenVPN to access local network devices like shared drives and home network servers as if you were on the local network.

OpenVPN communicates using encrypted SSL/TLS channels between networks that hide traffic from other devices on the Internet. The OpenVPN server runs on the router to control access to the tunnels, and users connect using a client application installed on their computer.



Click the Add New Tunnel and enter the name of the VPN as well as the server IP address, which is typically the same as your WAN IP address for the router. If a DDNS connection is active, use the first DDNS entry. Only change this field if a different DDNS service or static IP is being configured on the WAN side.

The remote IP address is the remote IP address of the device connecting to the account. It is not user configurable.

VPN users are provided with a configuration file generated by the OpenVPN server. This file is used as a

key for the client application to communicate with the server and open a connection. The router must be configured for each OpenVPN account that will be used.

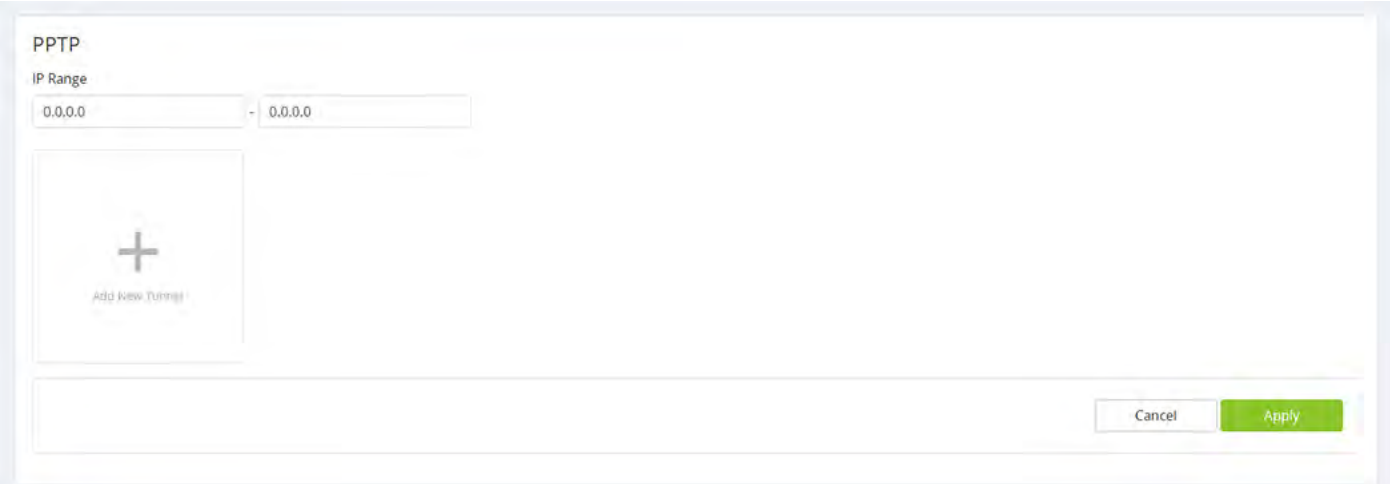
Client applications are available for PC and Mac computers and iOS and Android mobile devices.

Click the Regenerate a Key button to create a new cryptographic key for your VPN. Your users must then download the new config file to continue to use the established tunnel.

PPTP Section

Point-to-Point Tunneling Protocol uses an older methodology to establish any given tunnel. As it does not require encryption or authentication, PPTP is easy to implement, but also not very secure.

At the top, set the IP range for which PPTP is valid.



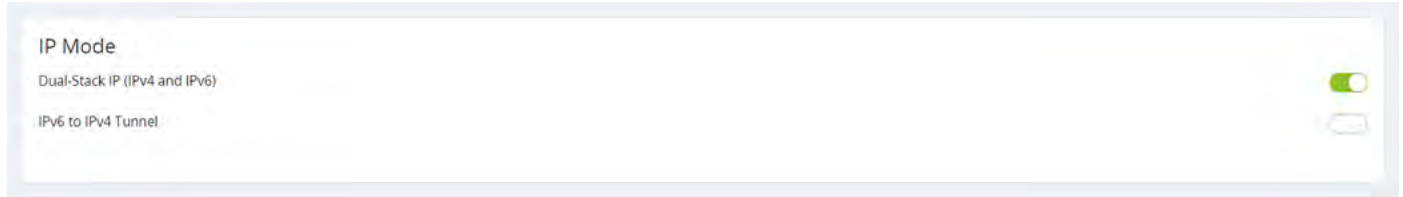
The screenshot shows a web-based configuration interface for PPTP. At the top left, the title 'PPTP' is displayed. Below the title, there is a section labeled 'IP Range' with two input fields separated by a hyphen, both containing the value '0.0.0.0'. Below the IP range section is a large, light-colored button with a plus sign and the text '+ Add New Tunnel'. At the bottom right of the form, there are two buttons: 'Cancel' and 'Apply'.

Click the **+ Add New Tunnel** button to create a new PPTP tunnel. Enter the tunnel name, and a username and password for that user.

Advanced > IPV6

IP Mode Section

This section defines how the router handles IPv6 addresses sent to the system.

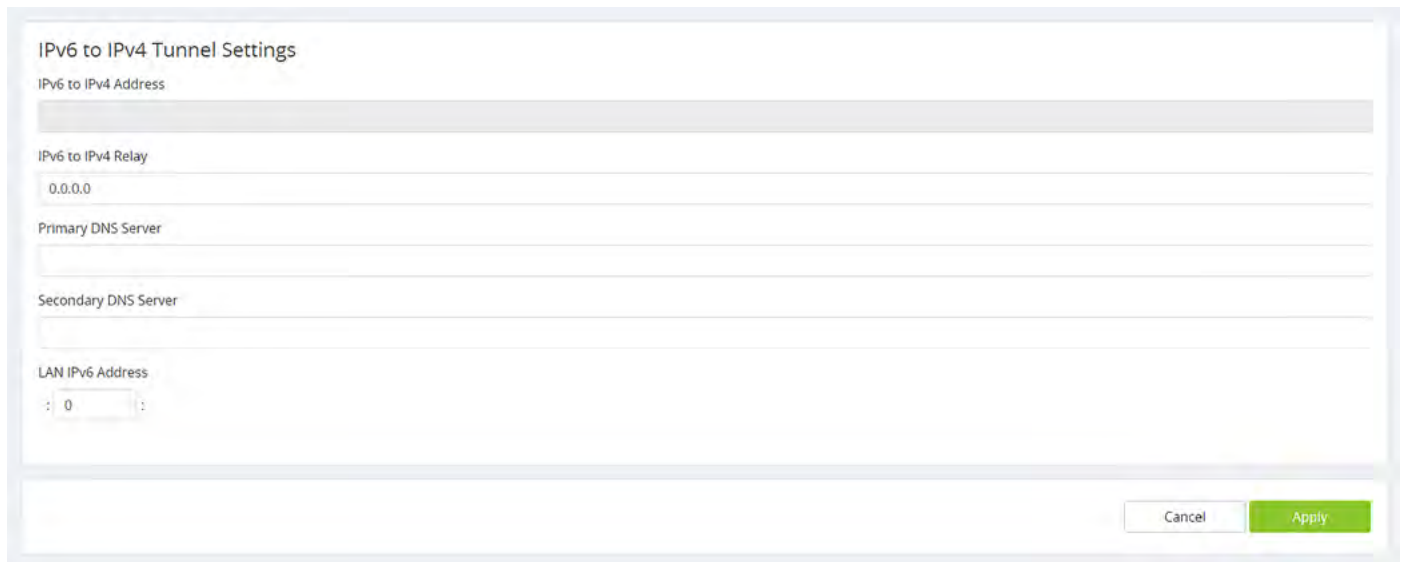


Dual-stack is fine (and recommended) for most applications. The router recognizes both address styles and parses out whichever address is unnecessary.

IPv6 to IPv4 tunnel creates a tunnel for transferring IPv6 addresses across an IPv4 backbone.



IPv6 to IPv4 Tunnel Settings Section



IPv6 to IPv4 Address is the address offered by the IPv6-to-IPv4 relay server at the location specified.

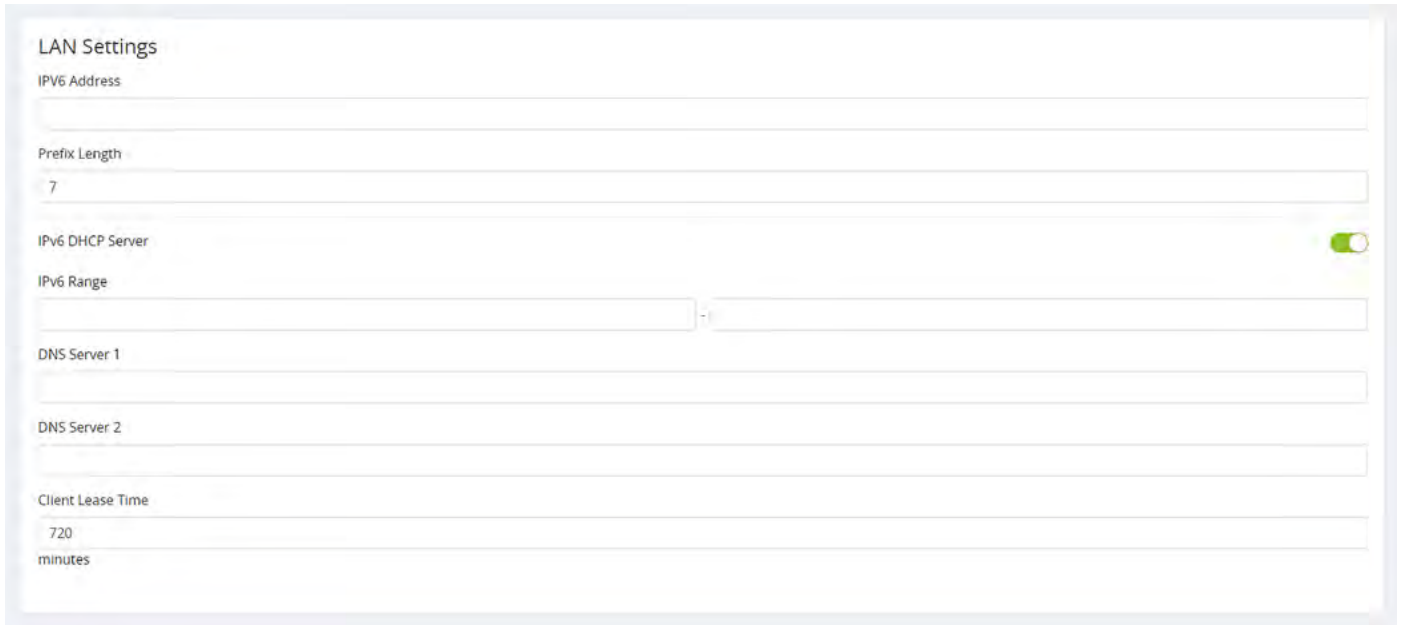
192.168.99.1 (the default) uses the router as the relay server. If a different address is entered, it must point to an External IPv6 Server. In addition, this external address ignores the IPv6 Address Field and DNS 1 and DNS 2 fields

IPv6 to IPv4 Relay is the location of the IPv6 subnet.

Primary and Secondary DNS Servers handle DNS resolution for IPv6 requests, and must be in IPv6 format.

LAN IPv6 Address is the IPv6 address location at which the LAN gateway exists.

LAN Settings Section



The screenshot shows the LAN Settings configuration page. It contains the following fields and controls:

- IPv6 Address:** An empty text input field.
- Prefix Length:** A text input field containing the value '7'.
- IPv6 DHCP Server:** A toggle switch that is currently turned on (green).
- IPv6 Range:** Two text input fields separated by a hyphen, both currently empty.
- DNS Server 1:** An empty text input field.
- DNS Server 2:** An empty text input field.
- Client Lease Time:** A text input field containing '720' and a label 'minutes' below it.

IPv6 Address: Enter the LAN IPv6 Address.

Prefix Length: Set the IPv6 equivalent to the IPv4 subnet mask. This is done by specifying the number of bits rather than using IP notation.

IPv6 DHCP Server: Enable or disable the IPv6 DHCP Server.

Range Start and End: Enter a starting and an ending IPv6 address for the DHCP server address range.

DNS 1 and DNS 2: Enter the primary and secondary IPv6 DNS address.

Client Lease Time: Number of minutes that a DHCP lease lasts.

WAN Settings Section

The exact appearance of this section changes with the option selected.

... With DHCP Selected

When DHCP is selected, your only option is whether to use a static DNS. To do so, click the checkbox and enter the server addresses in IPv6 format.

... With Static IP Selected

WAN IP Address is the IPv6 address that acts as the root of the IPv6 WAN.

Prefix Length acts as the IPv6 subnet mask for the LAN side of the network.

Default Gateway Address is the IPv6 address of the router.

Finally, add the IPv6 addresses for your preferred DNS servers.



... With PPPoE Selected

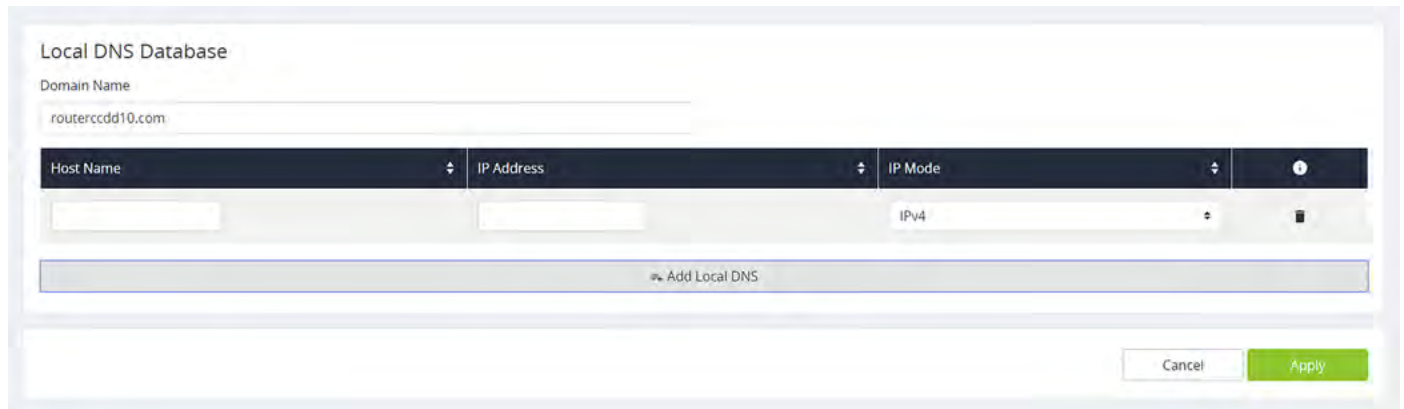
When used with IPv6 on the WAN side, PPPoE is similar to IPv4 in that the WAN connection is authenticated using encapsulated Point-to-Point Protocol (PPP) frames.

The screenshot shows the 'WAN Settings' configuration page. The 'WAN IP Mode' dropdown menu is set to 'PPPoE'. Below this, there are input fields for 'Username', 'Password', and 'Service Name'. The 'Keep Alive' toggle switch is turned on, and the 'Redial Period' is set to '30 seconds'.

Please consult your ISP for specific settings for configuring your WAN IPv6 service using PPPoE.

Advanced > Local DNS

This creates a local DNS server on the router for speedier results and forwarding. Use this expressly for devices in the local network (for example, to create a URL like `backporchcamera.myhome.com`).



The screenshot shows the 'Local DNS Database' configuration page. At the top, there is a 'Domain Name' text box containing 'routerccdd10.com'. Below this is a table with columns for 'Host Name', 'IP Address', and 'IP Mode'. The 'IP Mode' column has a dropdown menu currently set to 'IPv4'. At the bottom of the table is a '+ Add Local DNS' button. Below the table are 'Cancel' and 'Apply' buttons.

In the Domain Name text box at the top, enter the URL for for the device that will serve as the local DNS for your network.

Click the **+ Add Local DNS** button to add an entry. Enter the host device's name—the text you want to appear before your URL—its IP address, and select its IP mode.

For example, if your domain is myhome.com, enter backporchcamera in the device name text box. The router autofills the rest of the URL.

Be sure to complete these steps for each device with a local DNS entry:

- Reserve an IP address for each device being configured, or set each device to have a static IP address. (Using a DHCP address can cause the domain name to point to a different device if the address is reissued after setup.)
- Set the DNS server setting in each device to the same IP address as the router (default: 192.168.1.1).

Advanced > SNMP

Simple Network Management Protocol is used by network administrators to monitor the performance and settings of network devices. Configure SNMP to communicate with management devices in place on the network.

SNMP Settings Section

The screenshot shows two adjacent configuration panels. The left panel, titled 'SNMP Settings', contains the following fields: 'System Name' (routerCCDD10), 'System Contact', 'System Location', 'Enable SNMPv1/v2' (checked), 'Get Community Name' (public), 'Set Community Name' (private), 'Trap Community Name' (public), and 'Send SNMP Trap to' (empty). The right panel, titled 'SNMPv3 Settings', contains 'Enable SNMPv3' (unchecked), a table with one row (IP: 192.168.1.1, User: admin), and 'Trap Receiver IP Address' (empty). At the bottom right are 'Cancel' and 'Apply' buttons.

System Name and Contact: Use these to record the SNMP server manager’s contact person and the server’s physical location. Each of these parameters can be up to 64 characters. These identifiers are arbitrary and do not affect the server’s function, but they are useful to have.

You can enable SNMPv1/v2 and/or SNMPv3. We do not recommend you enable them both; SNMPv3 protocols are not backwards compatible with SNMPv1/v2. Please consult the corresponding client devices on the network to understand which version to use.

If you enable v1/v2, complete the following entries. Keep in mind that communities should be managed on a network wide-basis and require managers and agents on the network to have coordinated settings to work effectively.

Get Community Name: The name of the read-only community on the network

Set Community Name: The name of the read-write community on the network.

Trap Community Name: The name of the notifications community on the network.

Send SNMP Trap to: The IPv4 address to send all the Trap Community messages from all capable SNMP devices on the network.

SNMPv3 Settings Section

SNMP3 adds the ability to set up users with a more robust authentication scheme.

The screenshot shows the 'SNMPv3 Settings' configuration page. On the left, there are fields for 'System Name' (routerCCDD10), 'System Contact', 'System Location', 'Enable SNMPv3' (checked), 'Get Community Name' (public), 'Set Community Name' (private), 'Trap Community Name' (public), and 'Send SNMP Trap to' (192.168.1.1). The right pane has a toggle for 'Enable SNMPv3' (checked) and a table with columns: Enable, Username, Authentication Method, Encryption Method, Group Privilege, and an info icon. Below the table is an 'Add User' button. Further down are fields for 'Trap Receiver IP Address' and 'Trap Receiver User' (set to 'No User'). At the bottom right are 'Cancel' and 'Apply' buttons.

The user table lists all users currently enabled.

Trap Receiver IP Address: The IPv4 address to send all the Trap Community messages from all capable SNMP devices on the network.

Trap Receiver User: Beyond relaying where the traps end up going on the network. Can also limit which user as authenticated on the SNMP network can even have access to these traps (notifications).

When you click **Add User**, the following dialog appears:

The 'Add User' dialog box contains a table with the following structure:

Enable	Username	Authentication Method	Authentication Password	Encryption Method	Encryption Password	Group Privilege	
<input checked="" type="checkbox"/>	<input type="text"/>	None	<input type="text"/>	None	<input type="text"/>	Read Only	

Below the table is an 'Add User' button. At the bottom right are 'Cancel' and 'Apply' buttons.

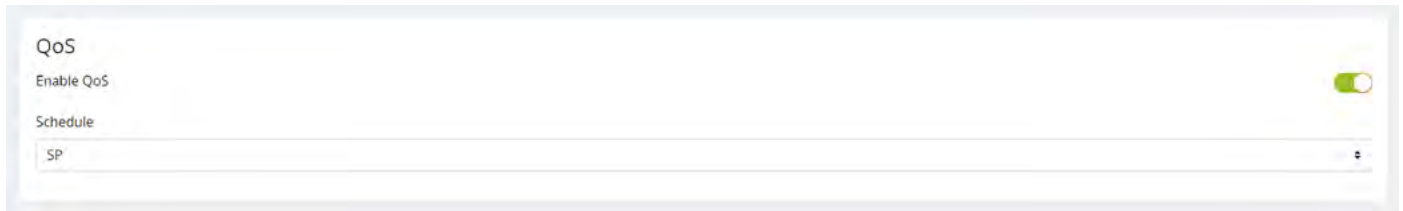
Enter the appropriate information to add a new user. To delete a user, click the trashcan icon by their entry.

Advanced > QoS

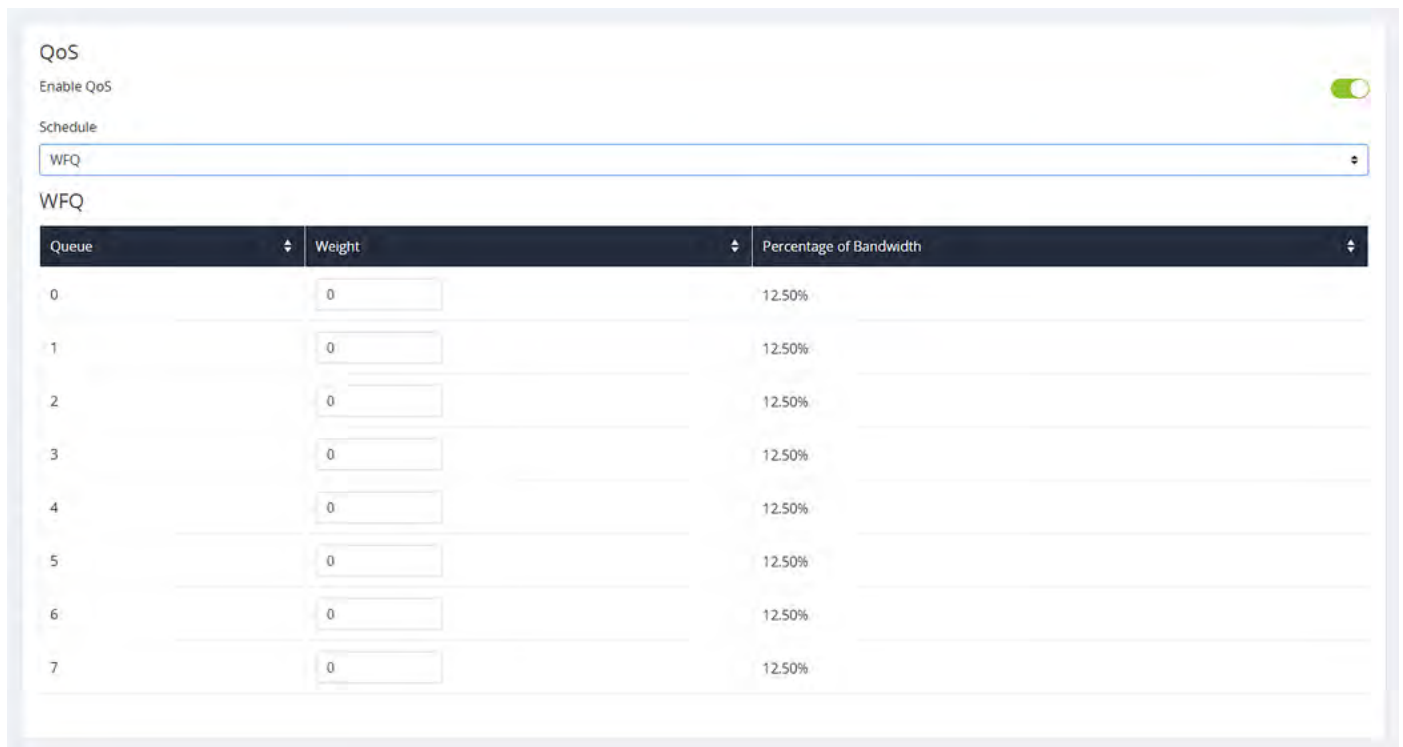
This section is for advanced users only.

QoS, or quality of service, is a protocol that tries to optimize traffic across the network. This is an advanced feature that rarely needs to be implemented except in large congested networks that require prioritization of network services. In essence, QoS tags data packets and then gives them priority based on policy. This lets you transmit key data preferentially.

DSCP is used at the Layer 3 (Network) IP level and as such should be used on a managed network. Consult the manufacturers of all participating network devices to ensure proper configuration.



At the top, select either SP (strict priority) or WFQ (weighted fair queueing). The WFQ table below only appears if you select WFQ in the dropdown.



When WFQ is selected, you must assign the weight. Weight is a relative comparison of how important the data is. The router then adjusts the bandwidth assigned to each queue level according to these numbers.

Note that Queue runs from 0 (minimal) to 7 (very high). Weight runs from 0 (minimal) to 15 (very high).

CoS to DCSP Mapping Section

This section allows mapping of CoS values to DSCP values and ranges, as well as an associated queue. Consider each row as the mapping between these reference buckets.

CoS refers to class of service, which monitors the types of traffic on a network, and assigns priority based on that.

If you are an advanced user, click the DSCP legend to reference the policy classifications for implementing DSCP (differentiated services code point) on your network.

CoS to DSCP Mapping

CoS	Name	DSCP	DSCP Range	Queue
(Lowest) 0	Background	0	0 - 7	0
1	Best Effort	8	8 - 15	1
2	Excellent Effort	16	16 - 23	2
3	Essential Application	24	24 - 31	3
4	Video Application	32	32 - 39	4
5	Voice Application	40	40 - 47	5
6	Internetwork Control	48	48 - 55	6
(Highest) 7	Network Control	56	56 - 63	7

DSCP Legend



System Log

System Log Section

Here you see recorded activities and status changes.

Specifications

Interfaces

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
WAN - RJ45 10/100/1000 Base-T	1	1
LAN - RJ45 10/100/1000 Base-T	2	2
LAN/WAN - Combo RJ45/SFP 10/100/1000Base-T	0	0
USB	1 (USB2.0) - Not Available at Launch	1 (USB2.0) - Not Available at Launch
Wireless Interface	N/A	802.11a/b/g/n/ac
Embedded Antennas	N/A	Yes

Performance

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
LAN - LAN Throughput	1 Gbps	1 Gbps
WAN - LAN Throughput (Unidirectional)	1 Gbps	1 Gbps
WAN - LAN Throughput (Bidirectional)	500 Mbps	500 Mbps

Wireless Performance

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
Antenna Type	N/A	Omni-directional
Transmit Power	N/A	Pls see the MCS table
Receiver Sensitivity	N/A	Pls see the MCS table
802.11 WAVE 2 AC	N/A	2x2:2 MU-MIMO
PHY Data Rate	N/A	Up to 300Mbps @ 2.4GHz Up to 867Mbps @ 5GHz
Operating Frequencies	N/A	2.4 GHz & 5 GHz
Channel Bonding	N/A	Yes (20 MHz, 40 MHz, and 80MHz)
Max TX Power	N/A	18dBm @ 2.4GHz 18dBm @ 5GHz

L2 Features

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
VLANs	Yes - 802.1Q	Yes - 802.1Q
RJ45 Auto-sensing	Yes	Yes
RJ45 Auto-negotiation	Yes	Yes

L3 Features

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
WAN/LTE Link Failover	Not Available at Launch	Not Available at Launch
Static Routing	Yes	Yes
Inter-VLAN Routing	Yes	Yes
DHCP Server	Yes	Yes
DHCP Client	Yes	Yes
DHCP Relay	Yes	Yes
DNS Relay	Yes	Yes
DDNS	Yes	Yes
1:1 NAT	Yes	Yes
PAT (Port Address Translation)	Yes	Yes
Port Trigger	Yes	Yes
DMZ Host	Yes	Yes
IPv6	Yes	Yes

Wireless Features

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
Auto Channel Selection	N/A	Yes
Operation Modes	N/A	Access Point
Multiple SSIDs	N/A	Yes - up to 8 per Radio
Wireless Security	N/A	WPA2-PSK (AES + TKIP) WPA-Enterprise
Hide SSID	N/A	Yes
Guest Network	N/A	Yes

Security

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
Stateful Firewall	Yes	Yes
Stateful Packet Inspection (SPI)	Yes	Yes
DoS Prevention	Yes	Yes
Ping of Death	Yes	Yes
SYN Flood	Yes	Yes
IP Spoofing	Yes	Yes
Port Forwarding	Yes	Yes
Content Filtering (URL & Keyword)	Yes	Yes
UPnP	Yes	Yes
Bonjour	Bonjour Client at Launch	Bonjour Client at Launch



VPN Features

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
PPTP Server	Yes	Yes
PPPoE	Yes	Yes
OpenVPN	Yes	Yes

Management

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
Web Management	Yes	Yes
SNMP v1,2c,3	Yes	Yes
OvrC Pro Embedded	Yes	Yes
Download/Upload Config File	Yes	Yes
System Log	Yes	Yes
HTTP & HTTPs	Yes	Yes
System Time	NTP/Manually	NTP/Manually
Cloud Management	Yes	Yes

Environmental & Physical

Features	AN-110-RT-2L1W	AN-110-RT-2L1W-WIFI
Product Dimensions (W x H x D) in inches	6.75 x 1.25 x 6.75	6.75 x 1.25 x 6.75
External Power Supply	12V 2A DC	12V 2A DC
Temperature Range	Operating Temp. 0°C to 40°C (32°F to 104°F)	Operating Temp. 0°C to 40°C (32°F to 104°F)
	Storage Temp. 0°C to 70°C (32°F to 158°F)	Storage Temp. 0°C to 70°C (32°F to 158°F)
Humidity	Operating Humidity 10% to 85% Non-Condensing	Operating Humidity 10% to 85% Non-Condensing
	Storage Humidity 5% to 90% Non-Condensing	Storage Humidity 5% to 90% Non-Condensing
Certifications	CE, FCC, UL, UPnP	CE, FCC, UL, UPnP