araknis NETWORKS

DUAL-WAN GIGABIT VPN ROUTER

USER INTERFACE MANUAL

Models:

AN-310-RT-4L2W

Manual Version

181213-1132

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 transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage 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 30cm between the radiator & your body.

Industry Canada Statement

This device complies with ISED's licence-exempt RSSs. 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.

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

UL Statement

All models have been evaluated by UL.

This device is intended for indoor use only. It should not be connected to an Ethernet network with outside plant routing.

The user must use the class I optical transceivers which conform to U.S. code of federal regulation, 21 CFR 1040.

© 2018 Araknis Networks®

This equipment is only to be connected to PoE networks without routing to outside plants.

CE Warning

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

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

© 2018 Araknis Networks®

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.

© 2018 Araknis Networks®

Table of Contents

© 2018 Araknis Networks®

LAN Ports on the 310

The AN-310 router has limited support for communications between the LAN 1–3 port grouping, and the LAN 4 port. As a result, we recommend you use LAN 4 as a non-overlapping network

This document provides guidance for the best practices for specific installation scenarios.

What Is Limited?

These limitations include:

- Multicast to support any auto-discovery protocols like SDDP (Control 4), AirPlay, Sonos, etc.
- QoS to support services like VoIP systems

Use Case: Router-on-a-Stick Topolgy

Our recommended procedure is to attach one dedicated switch to the router to handle traffic. Thus the connections run from the modem to the router, and then to the master switch. From there the cables run to other switches, WAPs, and host devices.

In this use case, use the LAN 4 port, which supports higher WAN-LAN throughput than the others:

- LAN 4: WAN-LAN 1Gbps unidirectional, 2Gbps bidirectional (1Gbps up, 1Gbps down, even simultaneously)
- LAN 1–3: WAN-LAN 1Gbps unidirectional, 1.2Gbps bidirectional (600Mbps up, 600Mbps down simultaneously)

Use Case: Router Using Multiple Ports

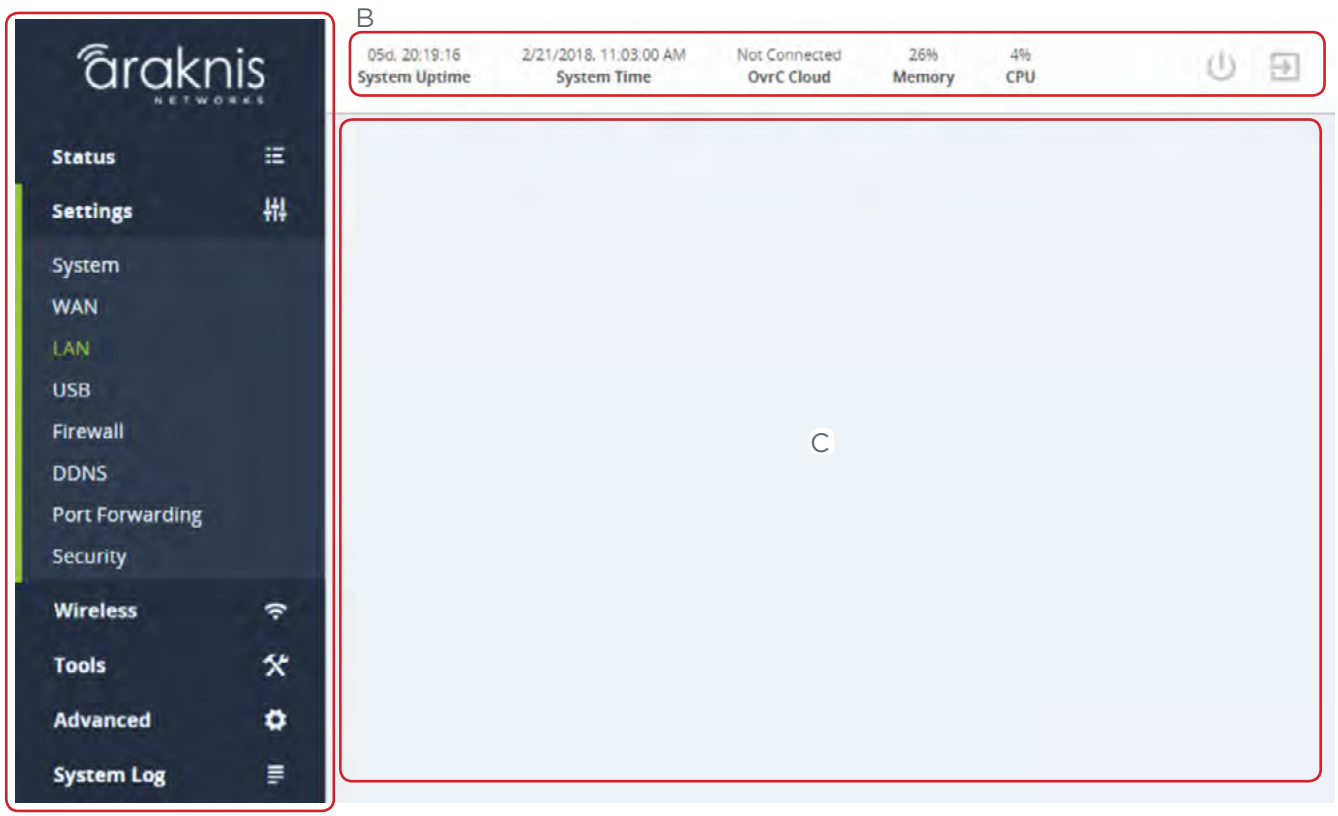
If you are using the router as a switch as well, then we recommend the following:

- Use LAN 1–3 for your networking needs. These three ports communicate together well and your network will function as expeted.
- Use LAN 4 only if you have a secondary non-overlapping network that you have set up using VLAN or subnet. Examples include a surveillance subnet or a separate network or the guest house.

These limitations are imposed by the firmware, and may be resolved via a firmware update at a later time.

© 2018 Araknis Networks®

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

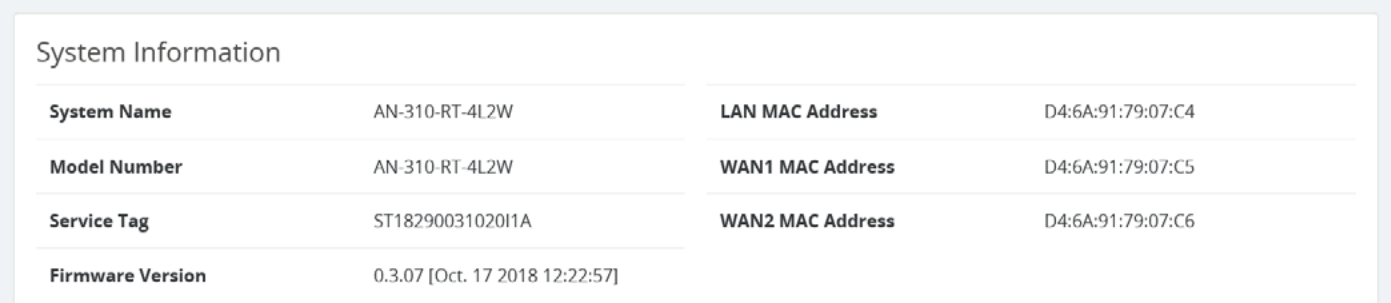
This displays the currently selected window, as indicated by the green lettering in the navigation panel.

© 2018 Araknis Networks®

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 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 each 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.

© 2018 Araknis Networks®

Port Status Section

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

Port Status

Interface	Name	Speed	Duplex
WAN1	WAN1	N/C	N/C
WAN2	WAN2	N/C	N/C
LAN1	LAN1	1Gbps	Full
LAN2	LAN2	N/C	N/C
LAN3	LAN3	N/C	N/C
LAN4	LAN4	N/C	N/C

Interface: Designates the physical port on the router.

Name: Name used to identify each port.

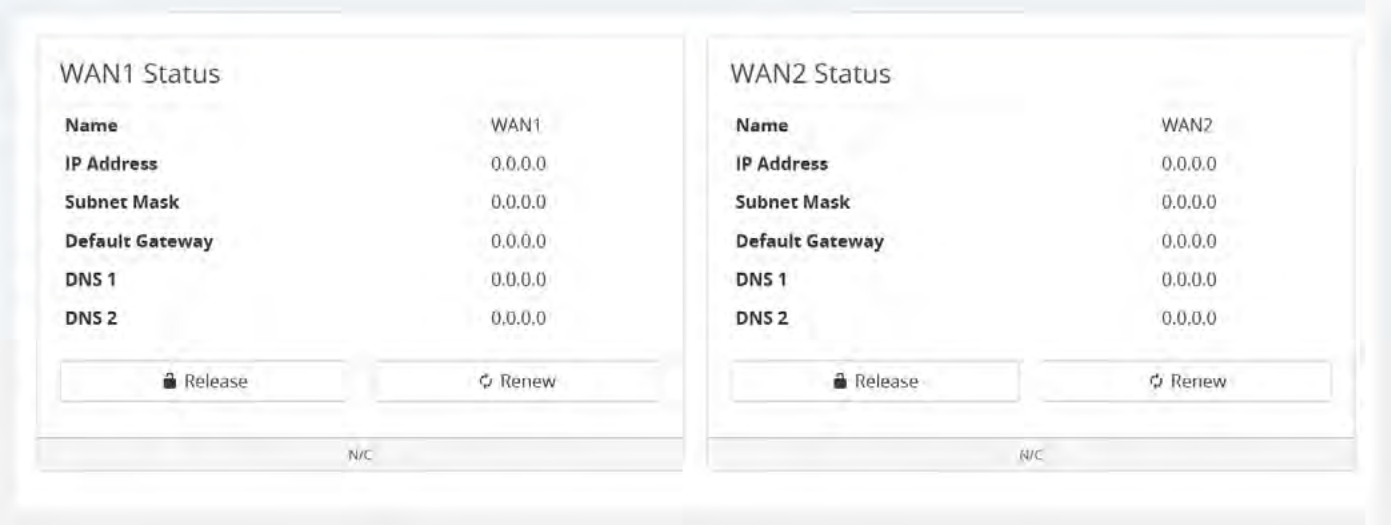
Speed: User-selected or device-negotiated port speed.

Duplex: Displays the duplex mode of the port.

WAN Status Section

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

Note – WAN2 is not yet operational. It will be made operational in a future firmware release.



Two key buttons are at the bottom of each WAN card.

© 2018 Araknis Networks®

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.

© 2018 Araknis Networks®

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 twenty OpenVPN, as well as twenty PPTP tunnels. Both types can be active simultaneously.

This router features a built-in OpenVPN server for secure, easily configured access to the network (via

© 2018 Araknis Networks®

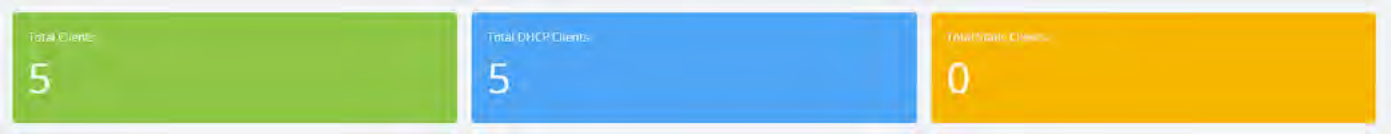
the internet) from devices with an OpenVPN client application. OpenVPN communicates using encrypted SSL/TLS channels between networks that the hide traffic from other devices on the internet.

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

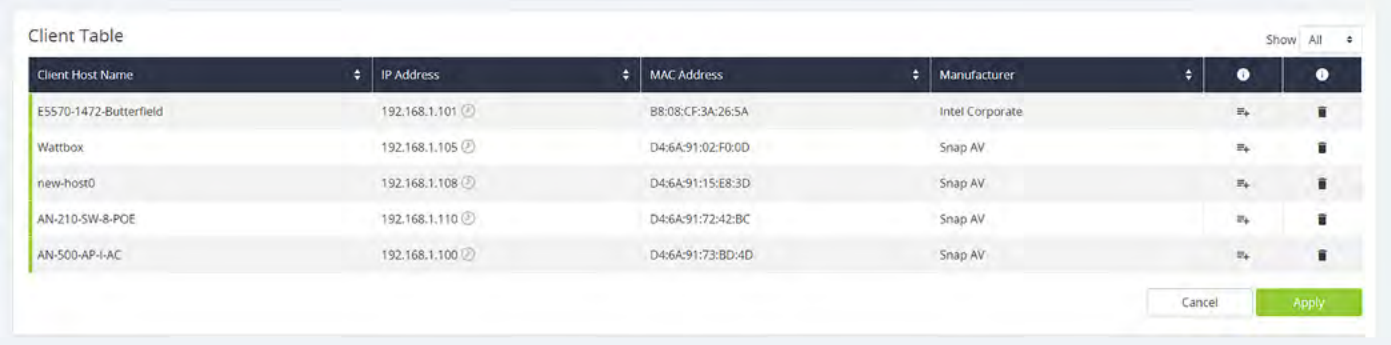
This shows the number of attached devices, as well as how many are static vs. DHCP.



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.

Client Table Section



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 500 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.

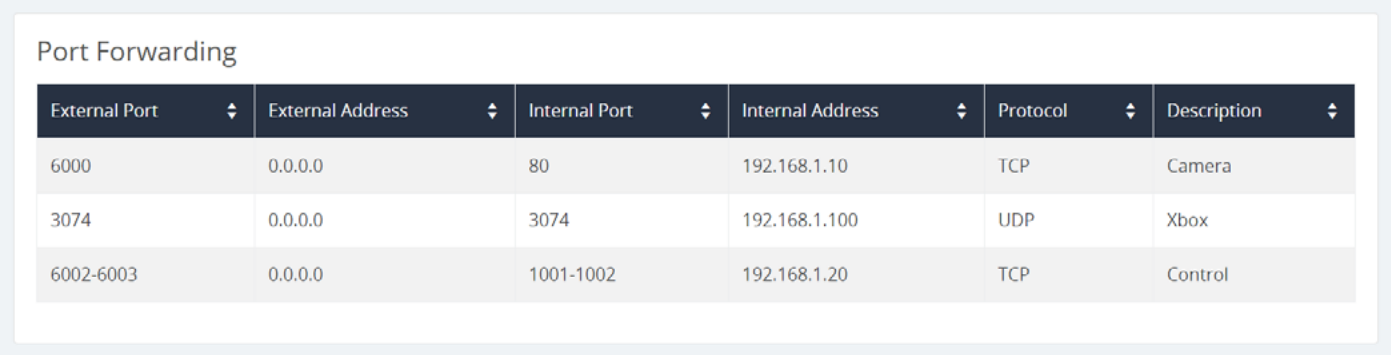
To reserve a DHCP address, click on the **+** icon to the left of the trash can icon.

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.

© 2018 Araknis Networks®

Port Forwarding Section

This lists all of the port forwarding rules in place.



See **Settings > Port Forwarding** for information on how to change these rules.

© 2018 Araknis Networks®

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**.

Port Status

Interface	Name	Speed	Duplex	VLAN ID	Sent	Received	Errors
WAN1	WAN1	N/C	N/C	N/A	-	-	-
WAN2	WAN2	N/C	N/C	N/A	-	-	-
LAN1	LAN1	1Gbps	Full	1	1.0 MB	5.7 MB	0
LAN2	LAN2	N/C	N/C	1	-	-	-
LAN3	LAN3	N/C	N/C	1	-	-	-
LAN4	LAN4	N/C	N/C	1	-	-	-

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.

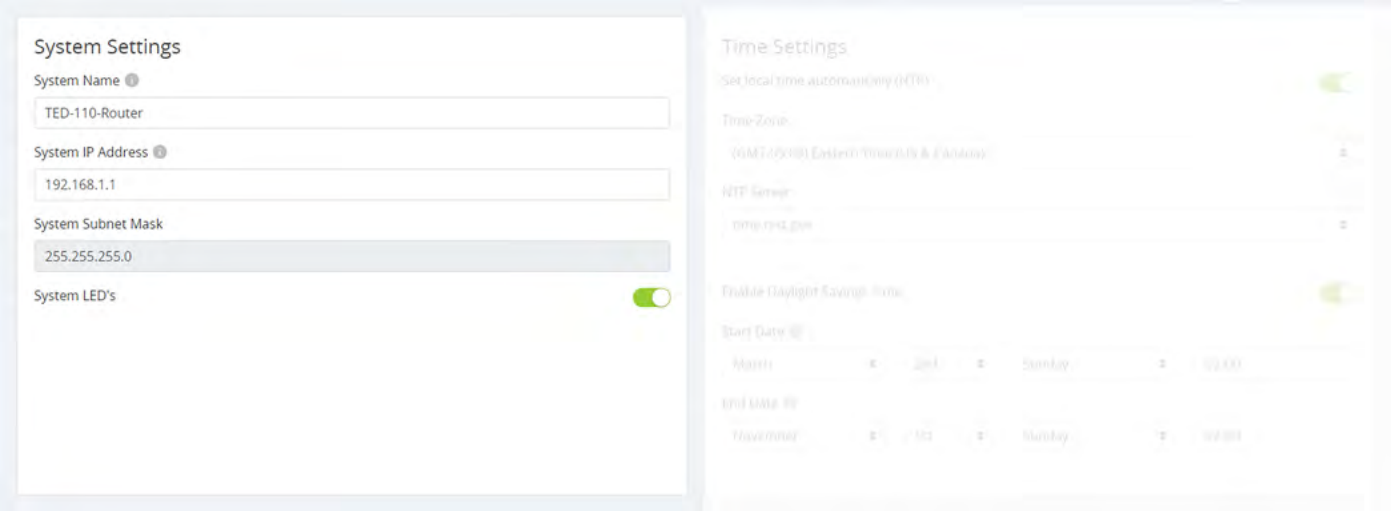
Errors: The number of data transmission errors since the last time it was powered on.

© 2018 Araknis Networks®

Settings > System

System Settings Section

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



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

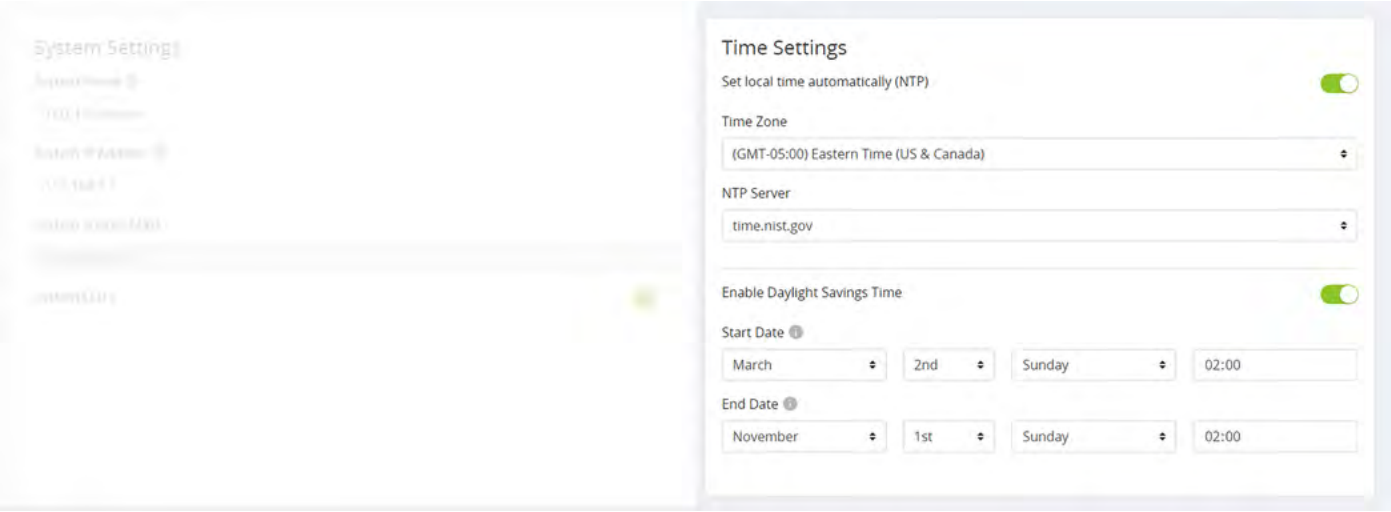
The IP can be provided in either IPv4 or IPv6.

- 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



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

© 2018 Araknis Networks®

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.

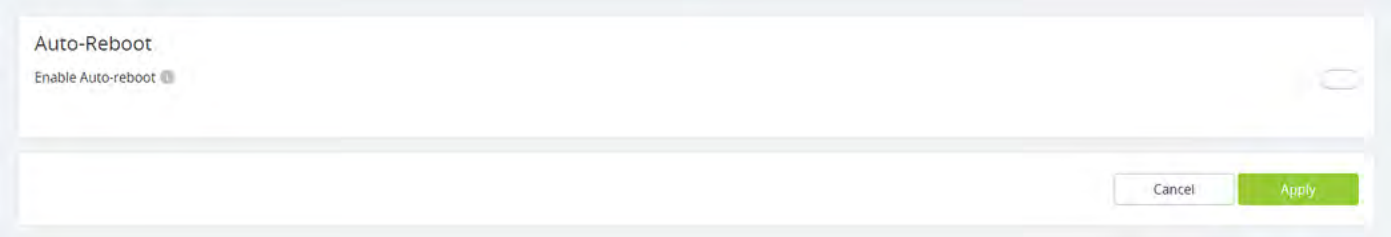
Set your desired time. As soon as you click apply, the new time settings are applied.

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, 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.

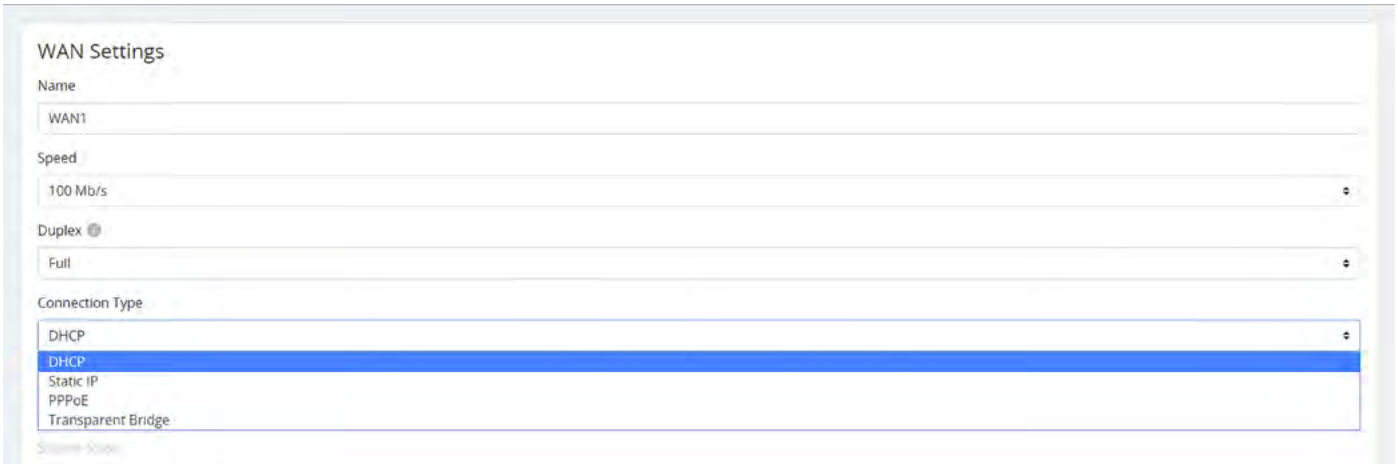
© 2018 Araknis Networks®

Settings > WAN

Note – WAN2 is not yet operational. It will be made operational in a future firmware release.

WAN Settings Section

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



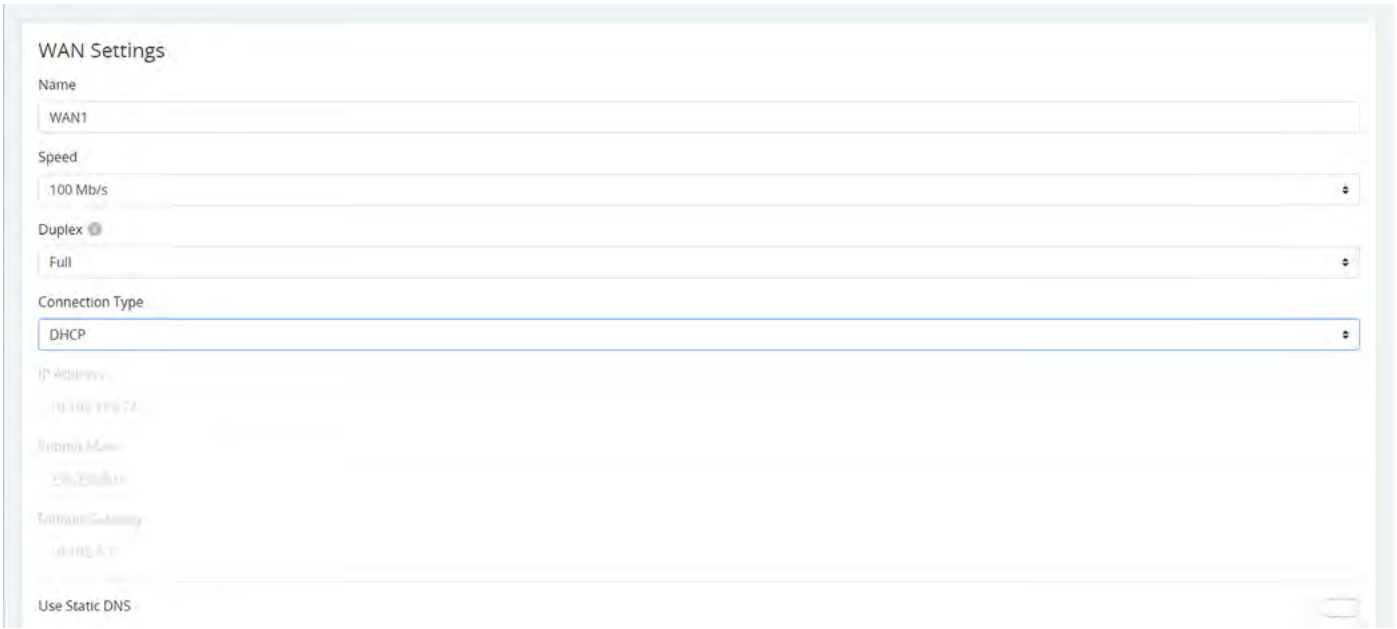
The top shows the WAN being edited.

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

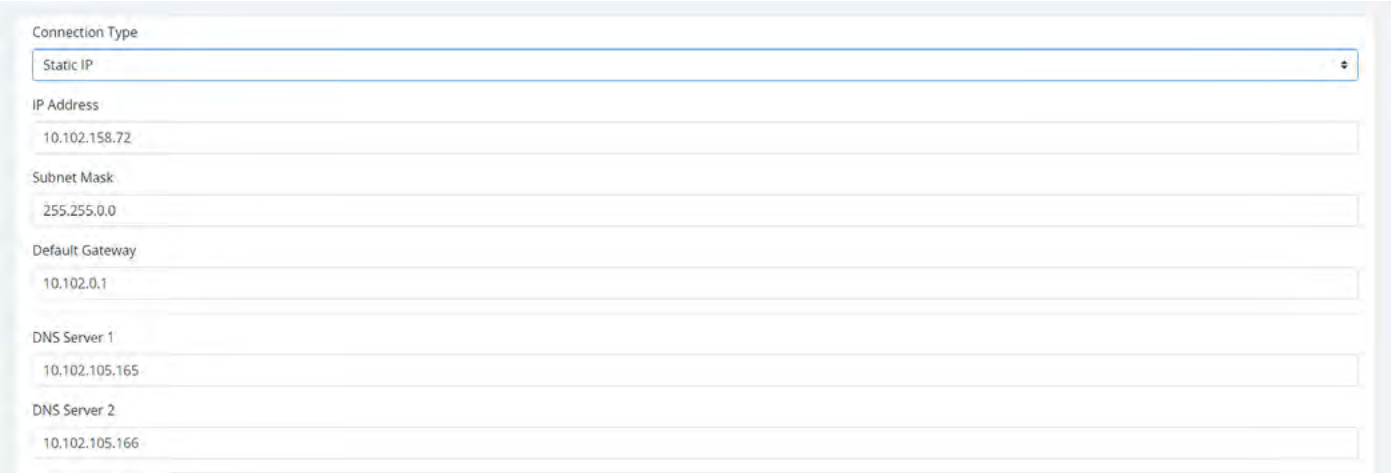
This sets the WAN port to use DHCP (automatically negotiating IP settings with your ISP).



© 2018 Araknis Networks®

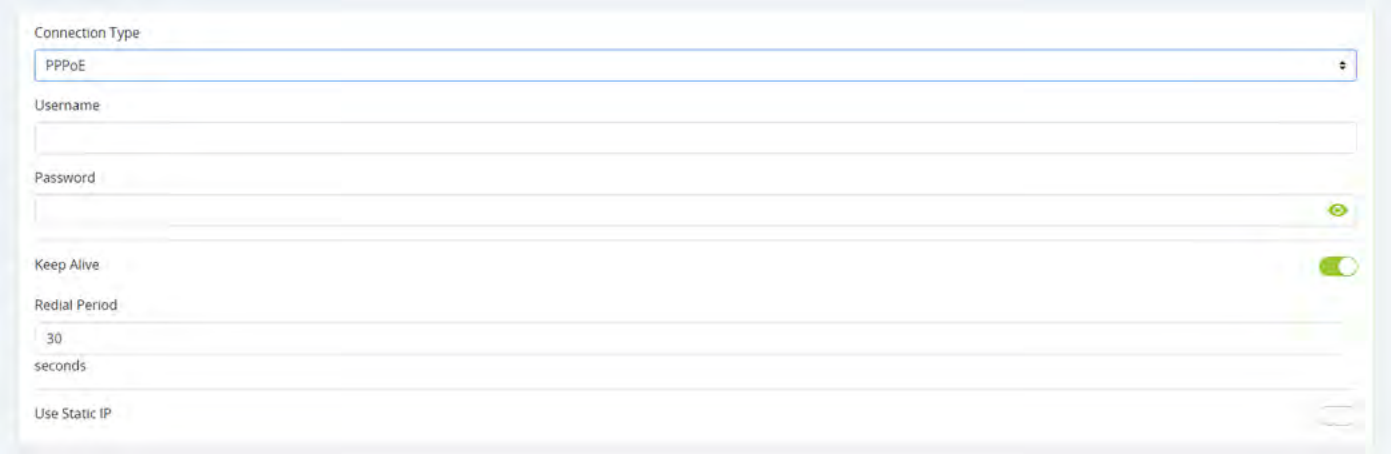
... With Static IP Selected

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



... With PPPoE Selected

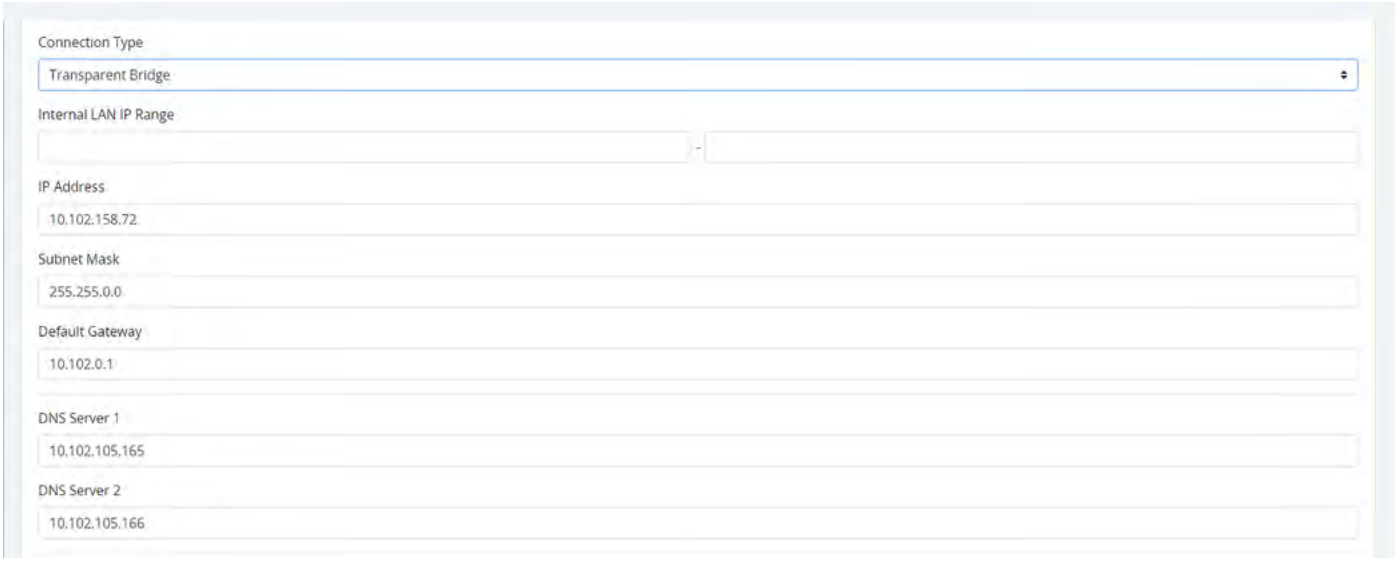
Use this for DSL and other peer-to-peer connections.



© 2018 Araknis Networks®

... With Transparent Bridge Selected

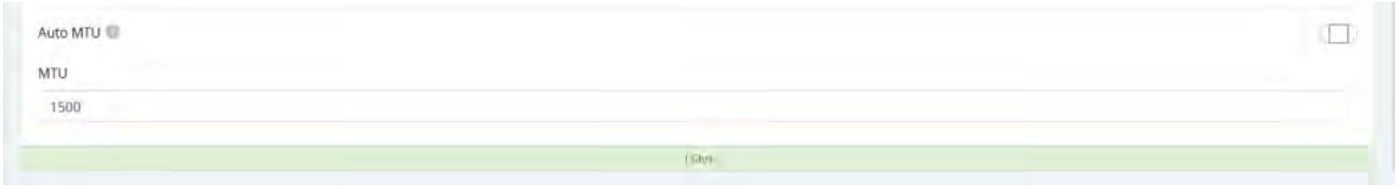
This disables all routing functions or your router. Use this if there is an ISP-provided router that must sit on the network.



... 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.



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

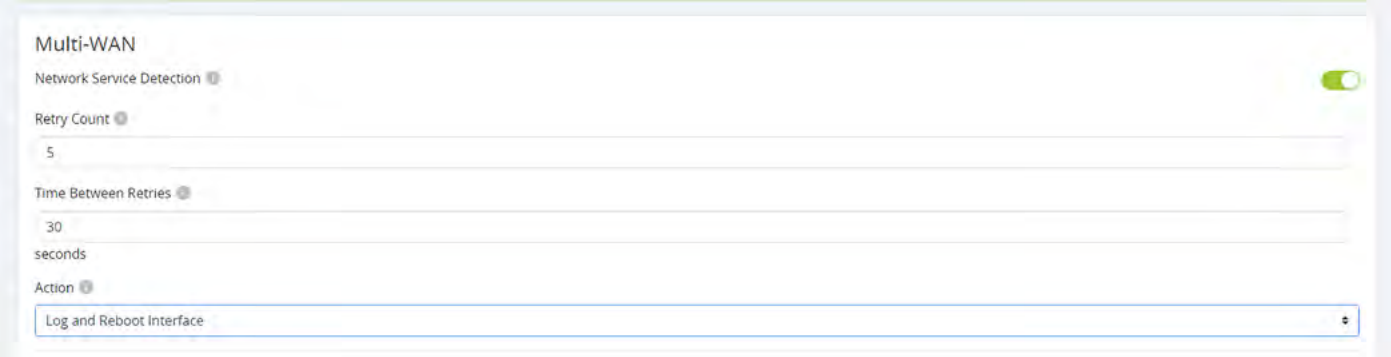
Renew Button: Click to renew the current WAN DHCP connection. The WAN IP address may or may not change.

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

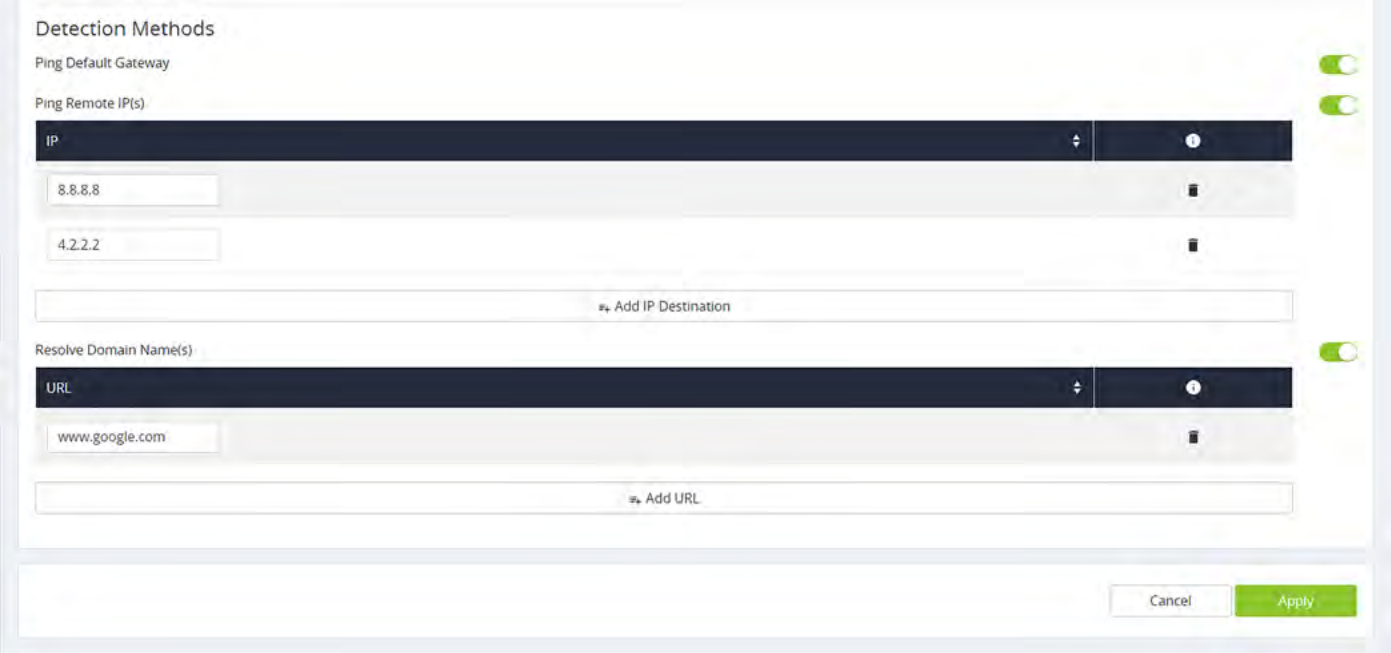
© 2018 Araknis Networks®

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.



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.



Ping Default Gateway refers to the default 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.

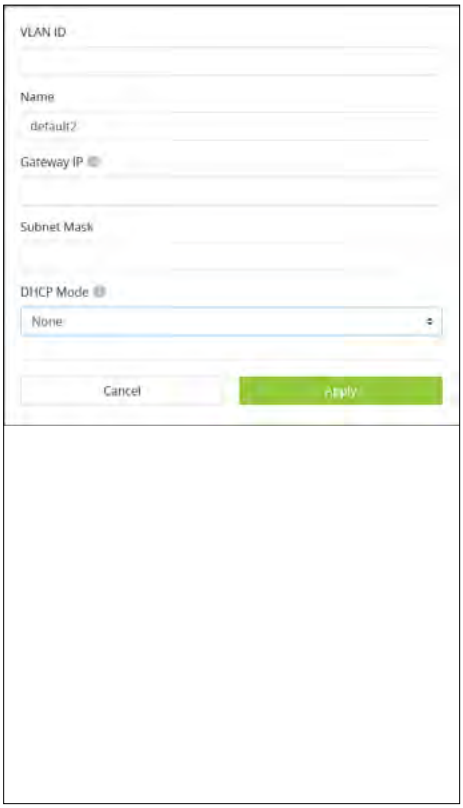
© 2018 Araknis Networks®

Settings > LAN

> **Note –** LAN4 does not communicate with LAN1–3. If you are using the router-on-a stick topology, use LAN4 to connect your router to your master switch. If you are using multuiple ports on the router, use LAN1–3; reserve LAN4 for uses that do not communicate with other LAN ports.

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.

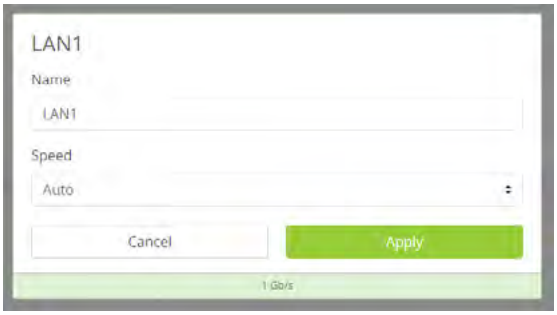


This shows the LANs available, their speed (color coded), and their duplex settings. Each port is color-coded based on its negotiated speed:

- **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.

© 2018 Araknis Networks®

- **Red:** Port has been disabled by the user in the web interface settings.

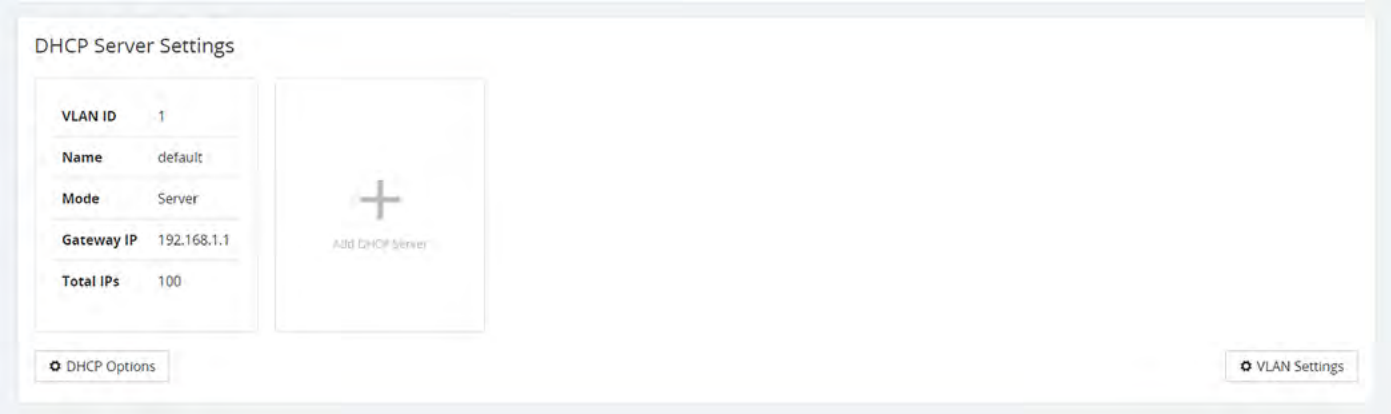


Click on a port to open a dialog where you can change the LAN's name, speed settings, and duplex setting (if the port is not set to auto). This also shows the actual speed at bottom, color coded as normal.

© 2018 Araknis Networks®

DHCP Server Settings Section

This section helps you to create subnets, assign them to VLANs, and configure the DHCP server for that subnet (if needed). Each subnet is represented by a card, sorted by VLAN ID number, with summary information. Click on a card to edit that subnet's settings (including several options not shown).



Add a new subnet by clicking the **+ Add DHCP Server c**ard.

Clicking on a card 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.

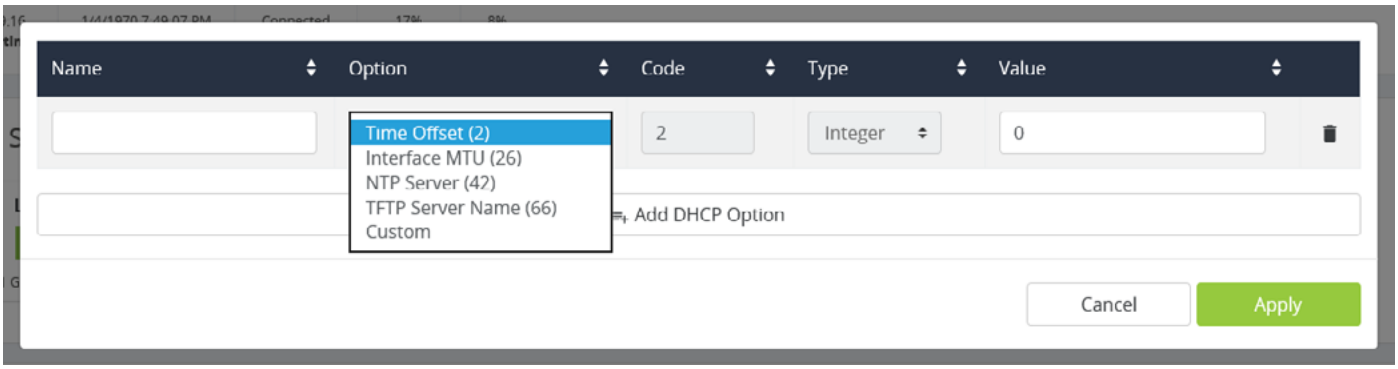
The VLAN ID ranges from 1–4095; duplicating an entry increments the previous entry. Note that setting the VLAN ID also adjusts the Gateway IP and IP Range fields (and vice versa).

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

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

DHCP Options Button

This opens a dialog to configure global DHCP options.



These options are set globally and can be assigned to individual DHCP servers. The purpose of custom

© 2018 Araknis Networks®

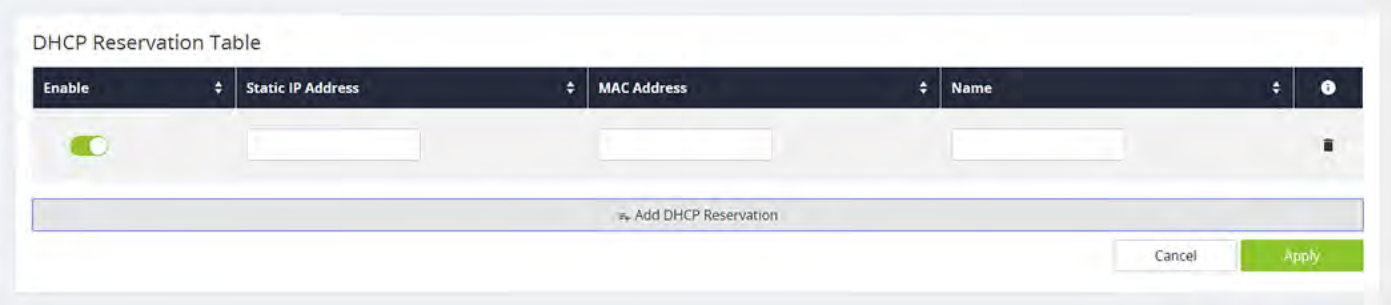
DHCP options is primarily driven by VoIP, as certain manufacturers requires certain DHCP options for their system to work. Ths dialog comes pre-populated with common DHCP options.

VLAN Settings Button

This takes you directly to the **Advanced > VLANs page**.

DHCP Reservation Table Section

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



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

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.

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.

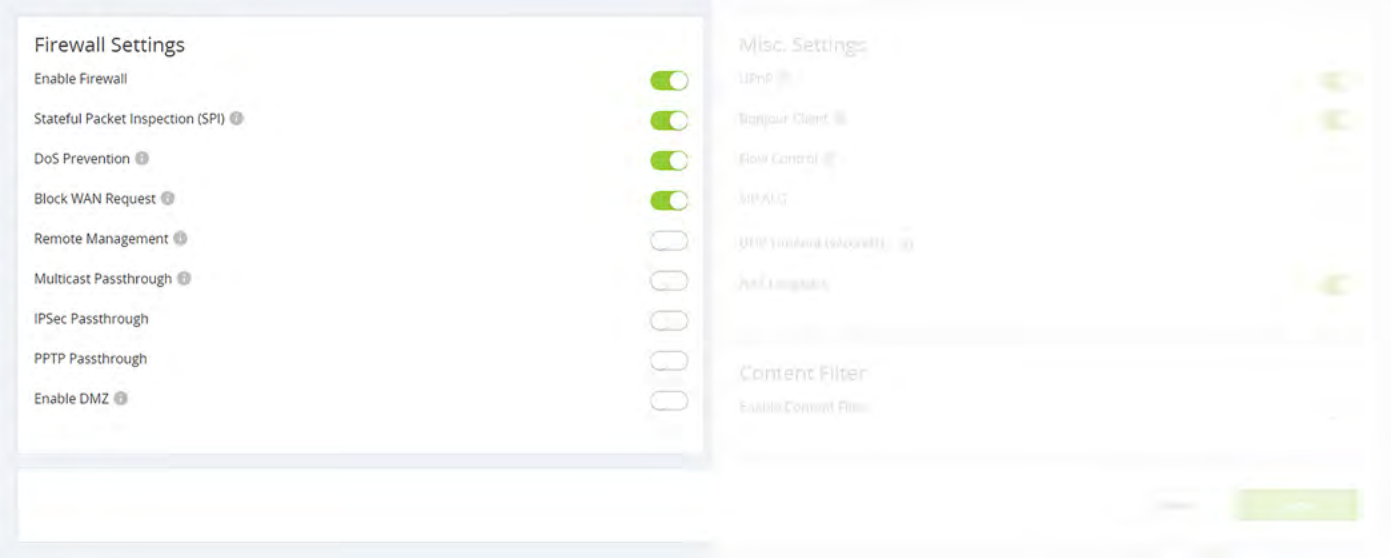
Clicking the trash can removes that device's DHCP reservation. You'll need to reboot the device to have it request a new IP address from the router.

© 2018 Araknis Networks®

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.

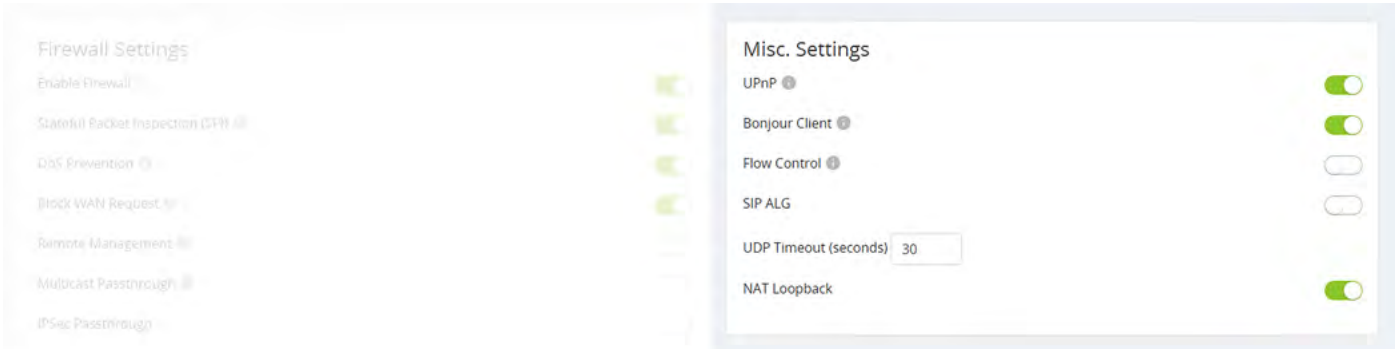
IPSec Passthrough: This allows IPsec VPN traffic to pass from WAN to LAN. Typically used in Double NAT topologies wherein there is an IPsec tunnel established upstream to the WAN side of this router.

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.

© 2018 Araknis Networks®

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.

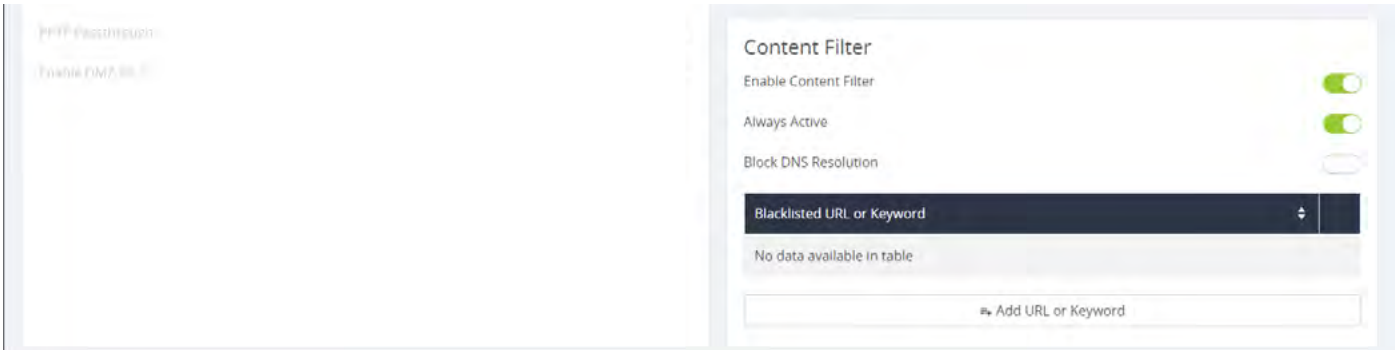
Content Filter Section

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.

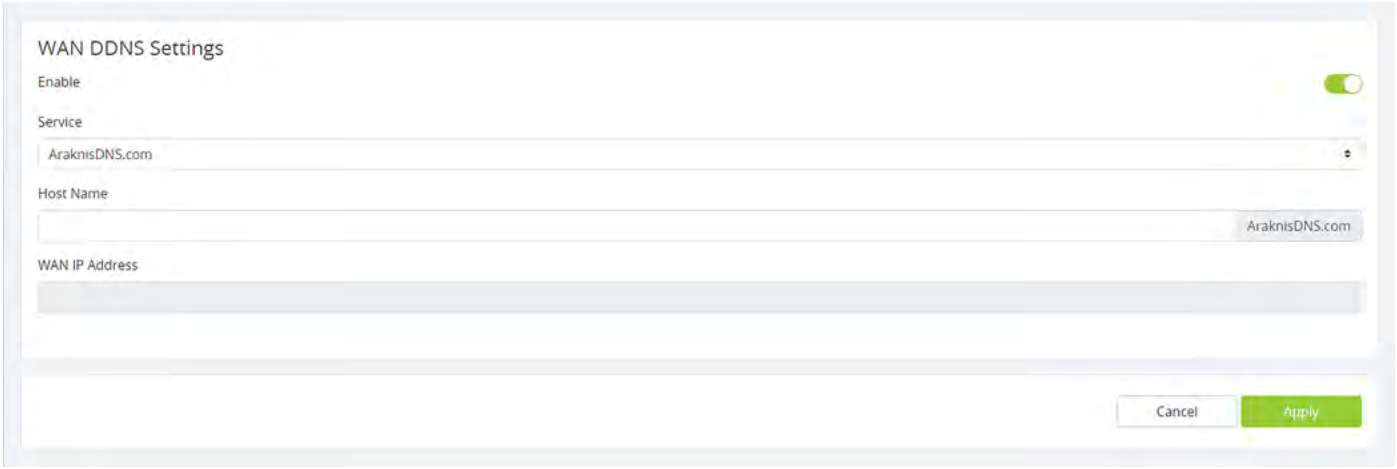
Block DNS Resolution blocks access to HTTPS sites.

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



© 2018 Araknis Networks®

Settings > DDNS



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.

> **Note –** A future firmware upgrade will activate WAN2, at which point you can choose DDNS separately for each WAN.

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.

© 2018 Araknis Networks®

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.

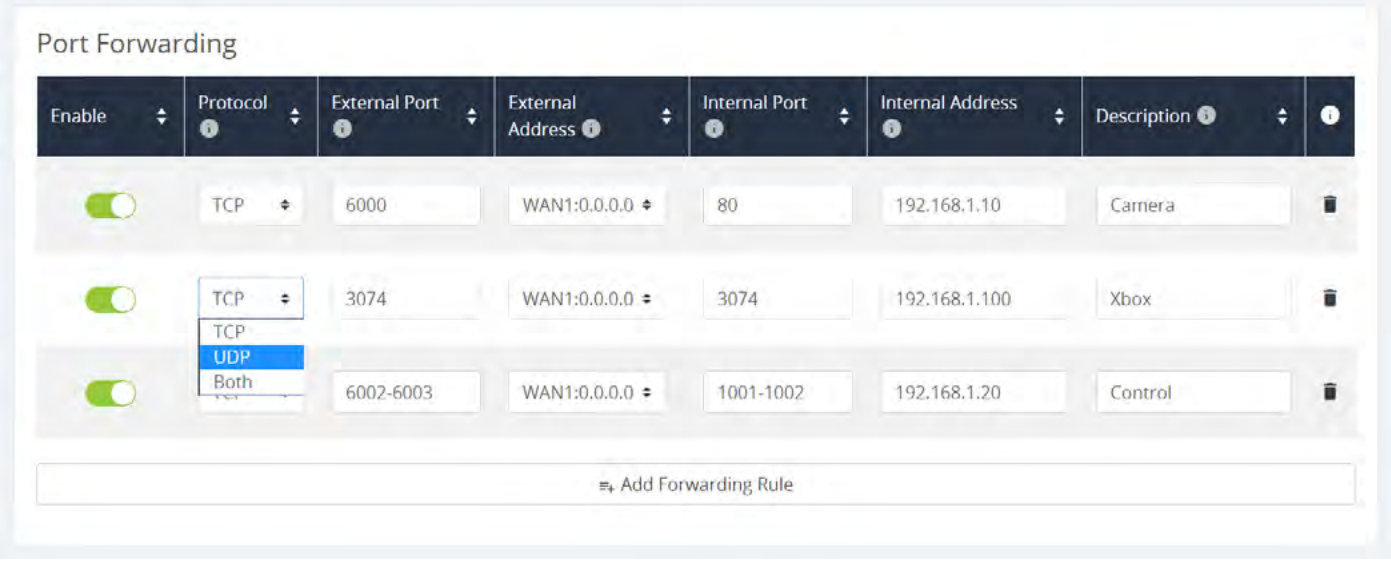
When software from LAN devices need access to and from the internet, additional ports may be forwarded to the device to allow communication through the router firewall. Common uses for port forwarding include:

- 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

A future firmware update will allow you to choose a different external address for each WAN made available.

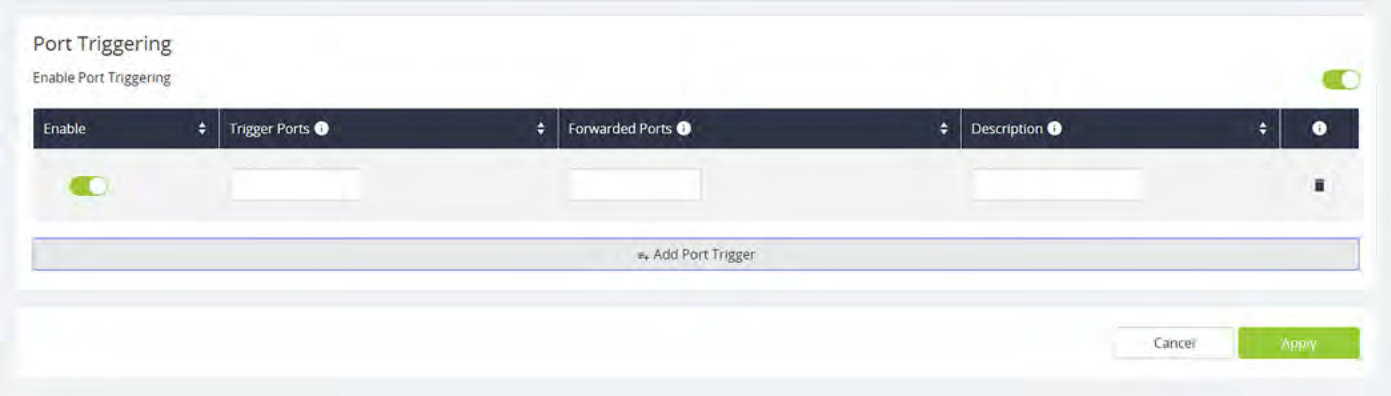


Here you can set your protocl, the external port and WAN, and the internal target address for each port you want to forward.

© 2018 Araknis Networks®

Port Triggering Section

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



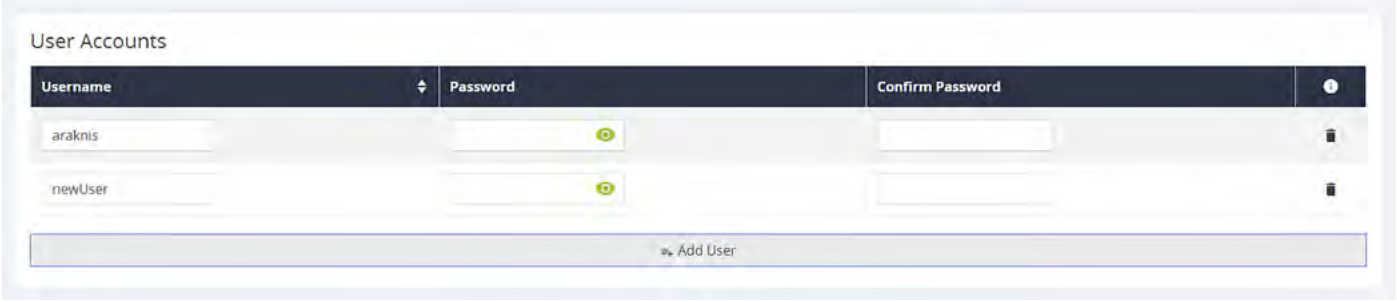
© 2018 Araknis Networks®

Settings > Security

User Accounts Section

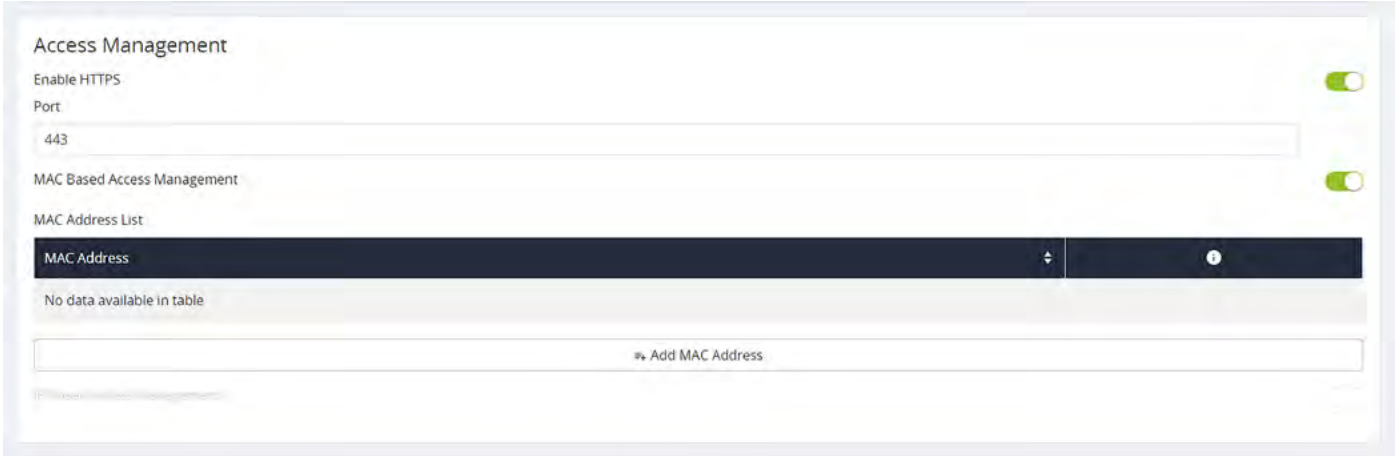
Here you can create new accounts to access the router. We recommend that you do not give anyone access to the default account.

> **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.



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.



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 enabling activate simultaneously. If you are remote, this could cause you to lose connection with your router.

Access management has no impact on DDNS.

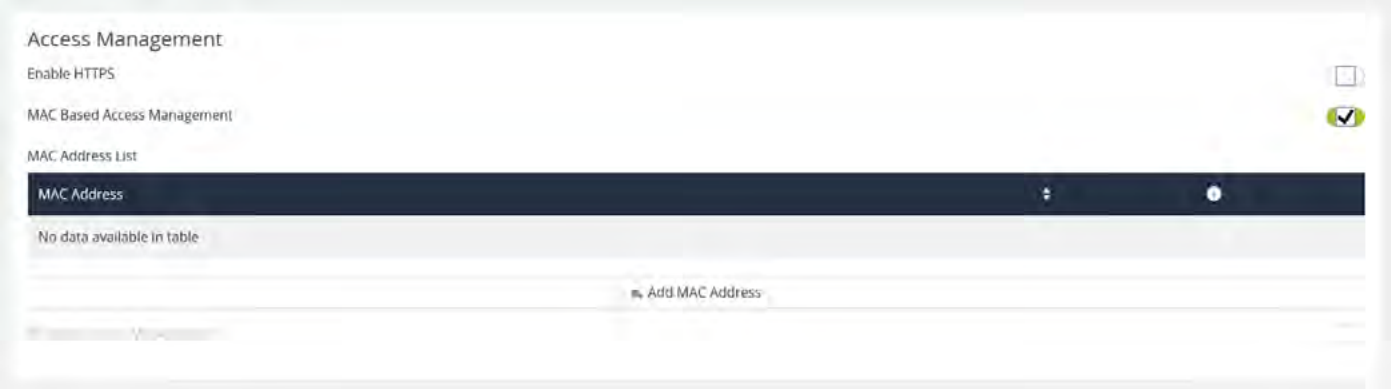
© 2018 Araknis Networks®

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.

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.



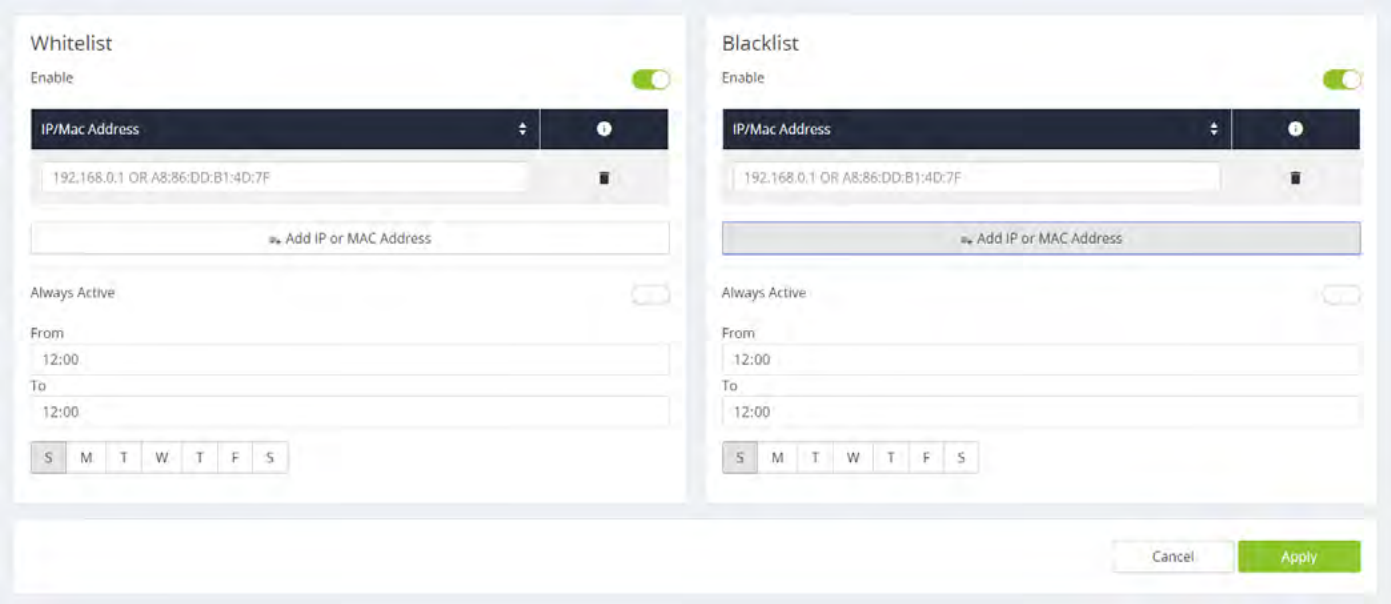
Similarly, you can enable **IP Based Access Management** to restrict access to your router to include only devices at certain IP addresses within your network.

Note that IP and MAC methods are mutually exclusive.

© 2018 Araknis Networks®

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.



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.

A schedule starts and stops the same time on each day that they are active. Each day of the week has a toggle button; you can select one, some or all of the days of the week, and they need not be contiguous.

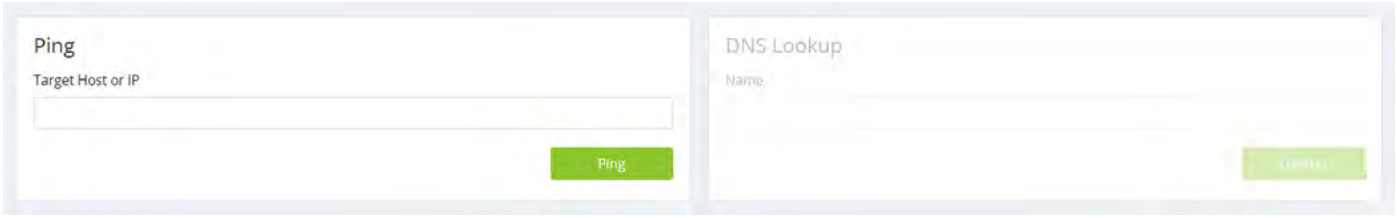
The whitelist and blacklist cannot have overlapping schedules.

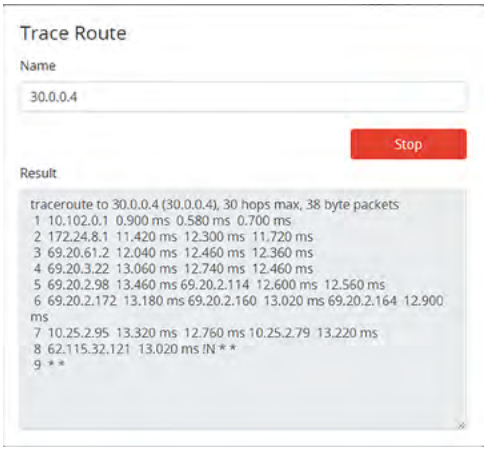
© 2018 Araknis Networks®

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.



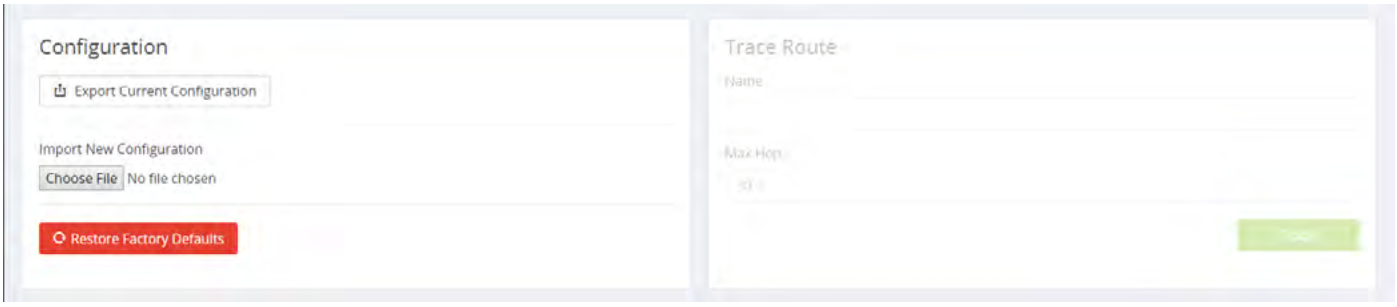


DNS Lookup Section

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

Configuration Section

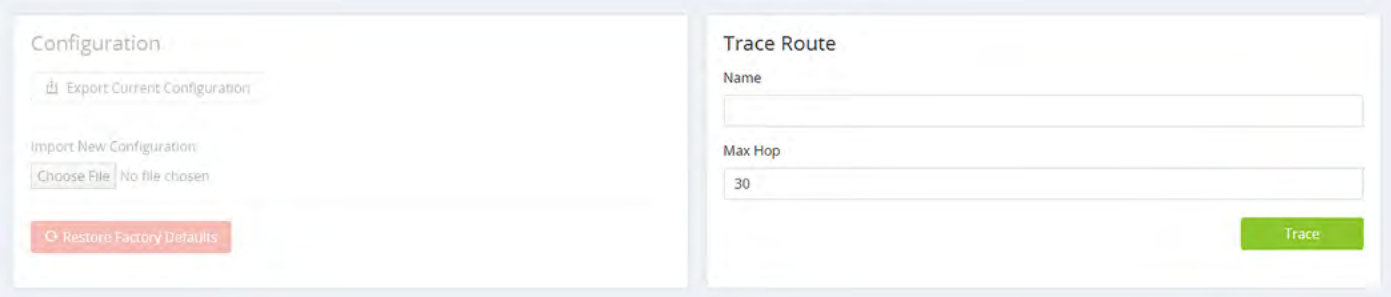
Here you can export your router's configuration (we highly recommend this before each you update the firmware), import a new configuration file, or restore the router to its factory default settings.



© 2018 Araknis Networks®

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.



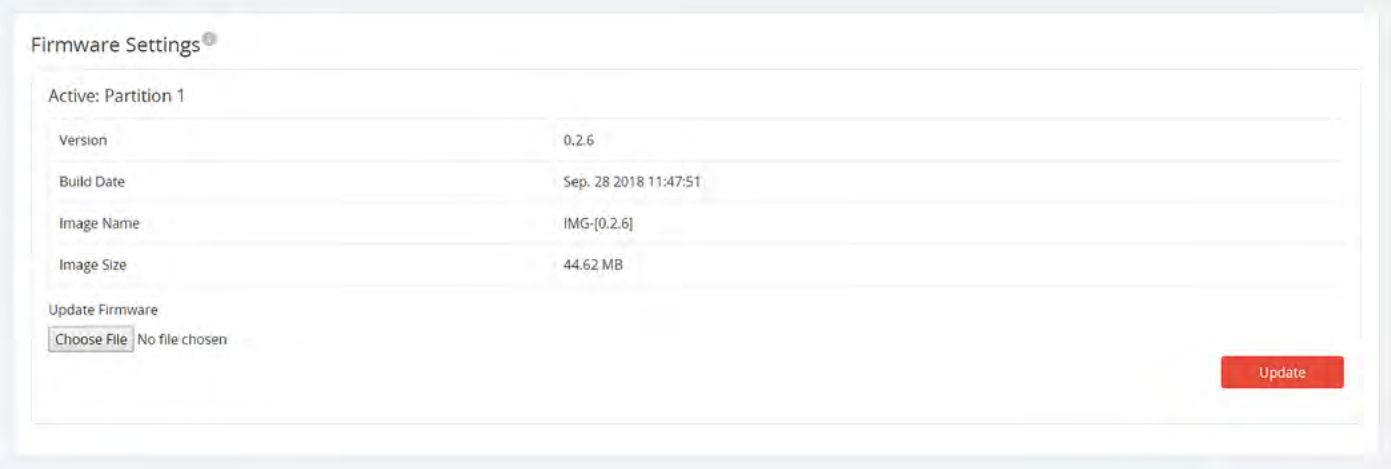
Enter the IP address of a device or web page. Click the **Start** button.

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.



© 2018 Araknis Networks®

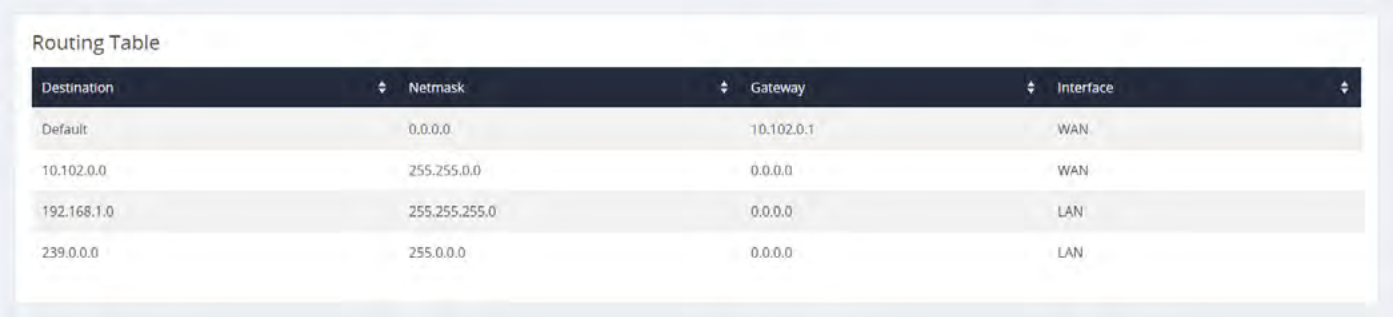
Advanced > Static Route

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.

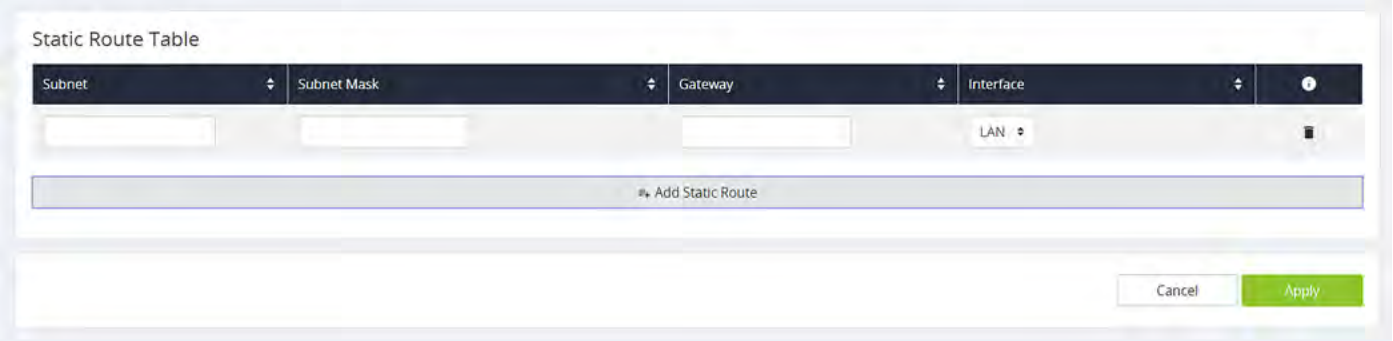
Routing Table Section

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



Static Route Table Section

Use this to add entries to the table above.



- **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.

© 2018 Araknis Networks®

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.

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

© 2018 Araknis Networks®

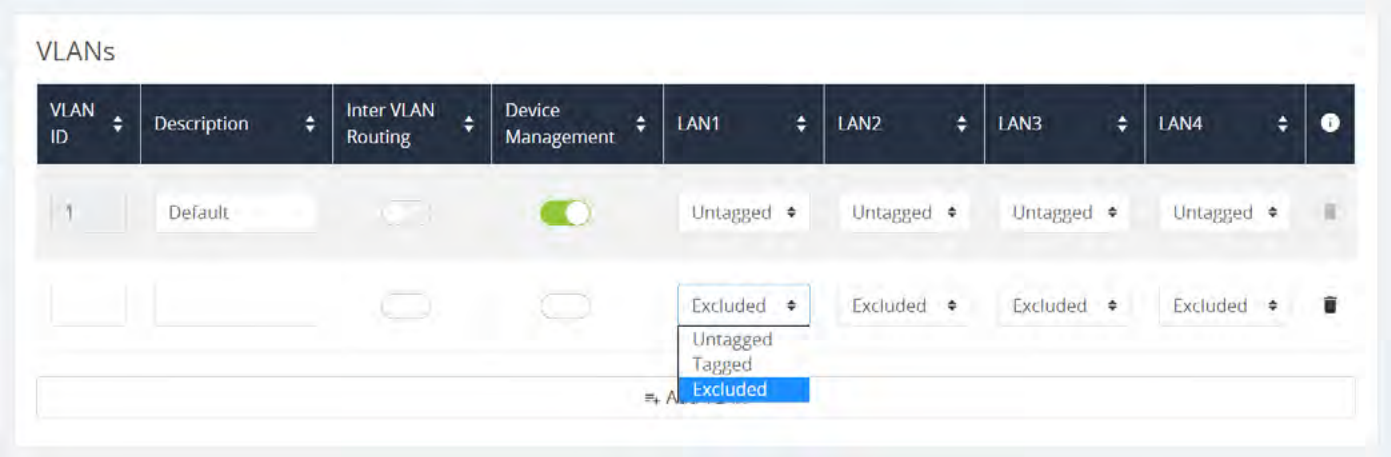
Advanced > VLANs

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.

> **Note –** LAN4 does not communicate well with LAN1–3. If you want a separate VLAN (e.g., for surveillance or a guest network), use LAN4. If you need your VLANs to communicate with each other, do not use LAN4.

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.



- **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. You must enable this feature on each VLAN that you want communicating with another.
- **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.

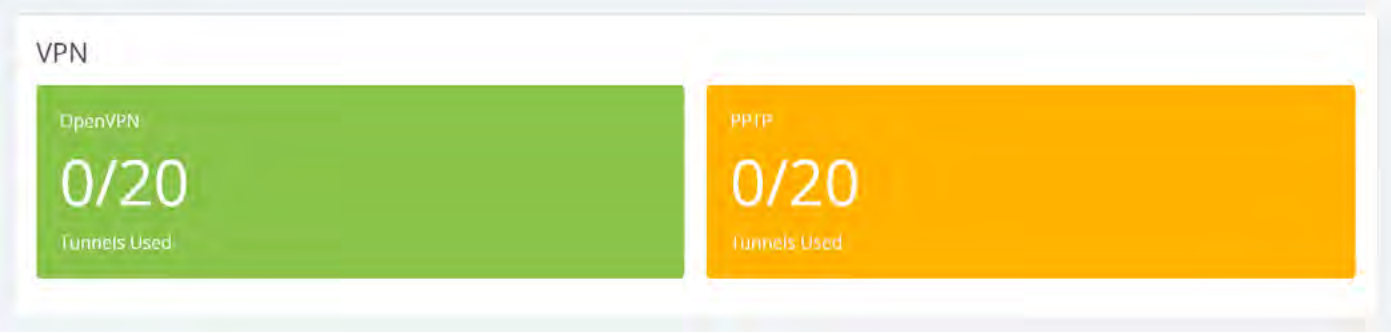
© 2018 Araknis Networks®

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

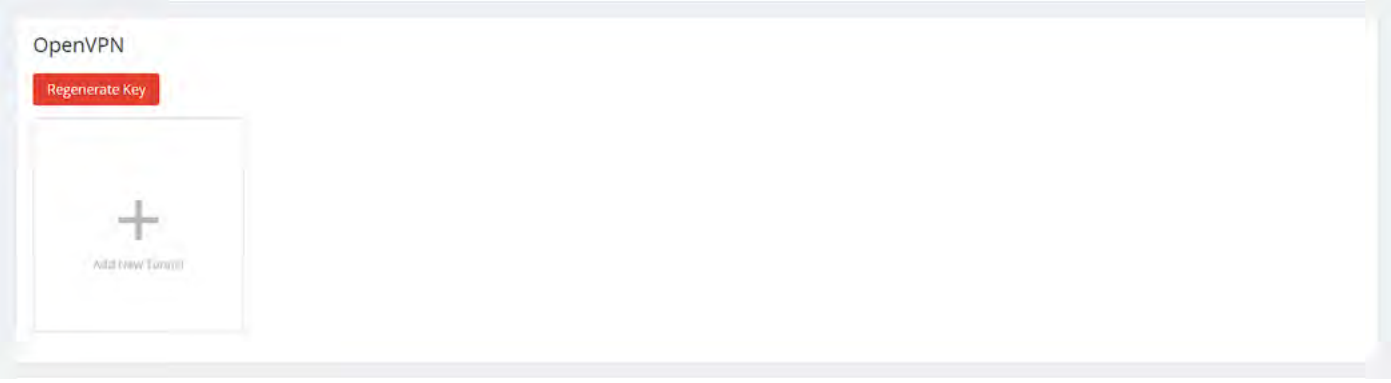
The router can support a maximum of twenty OpenVPN, as well as twenty PPTP tunnels. Both types can be active simultaneously. IPSec will be added in a future firmware update.



Open VPN Section

The AN-310 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.

© 2018 Araknis Networks®

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.

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

© 2018 Araknis Networks®

Advanced > IPV6

> **Note –** Once WAN2 is activated in a firmware upgrade, both WANs will have IPv6 settings.

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.

> **Note –** Consult with your ISP before enabling IPv6 to IPv4 tunneling.

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 IPv4 subnet.

© 2018 Araknis Networks®

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

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. This IPv6 setting is executed by specifying the number of bits used for the mask (rather than using IP notation as in IPv4).

© 2018 Araknis Networks®

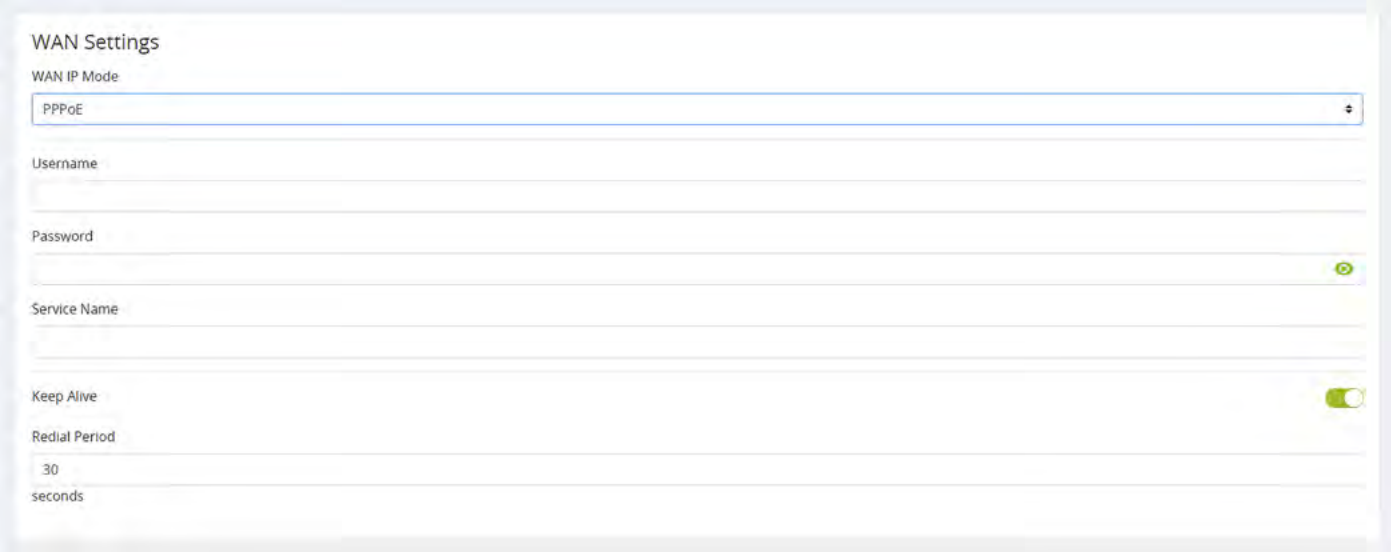
Default Gateway Address is the IPv6 address of the router.

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

© 2018 Araknis Networks®

... 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.

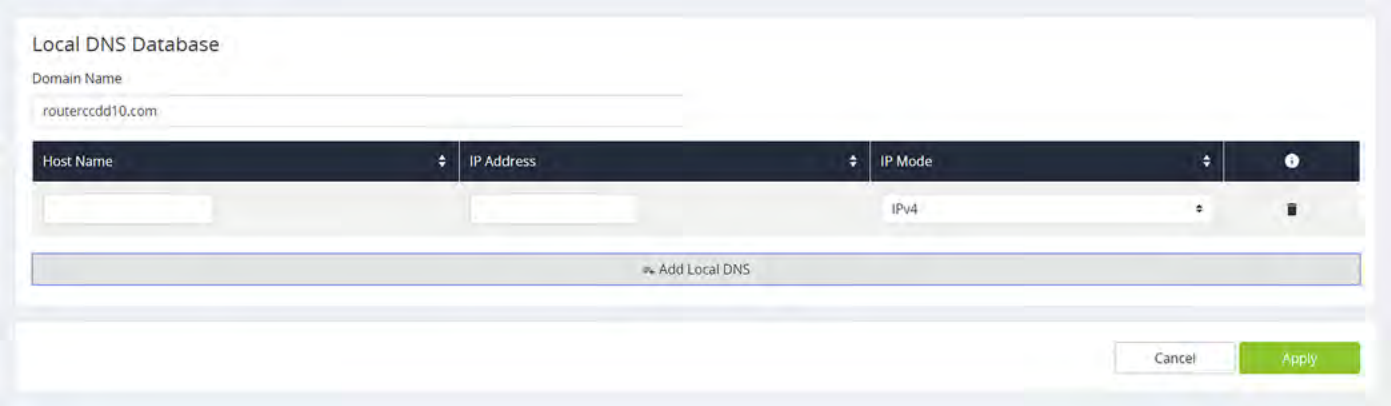


Please consult your ISP for specific settings for configuring your WAN IPv6 service using PPPoE.

© 2018 Araknis Networks®

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).



In the Domain Name text box at the top, enter the URL 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:

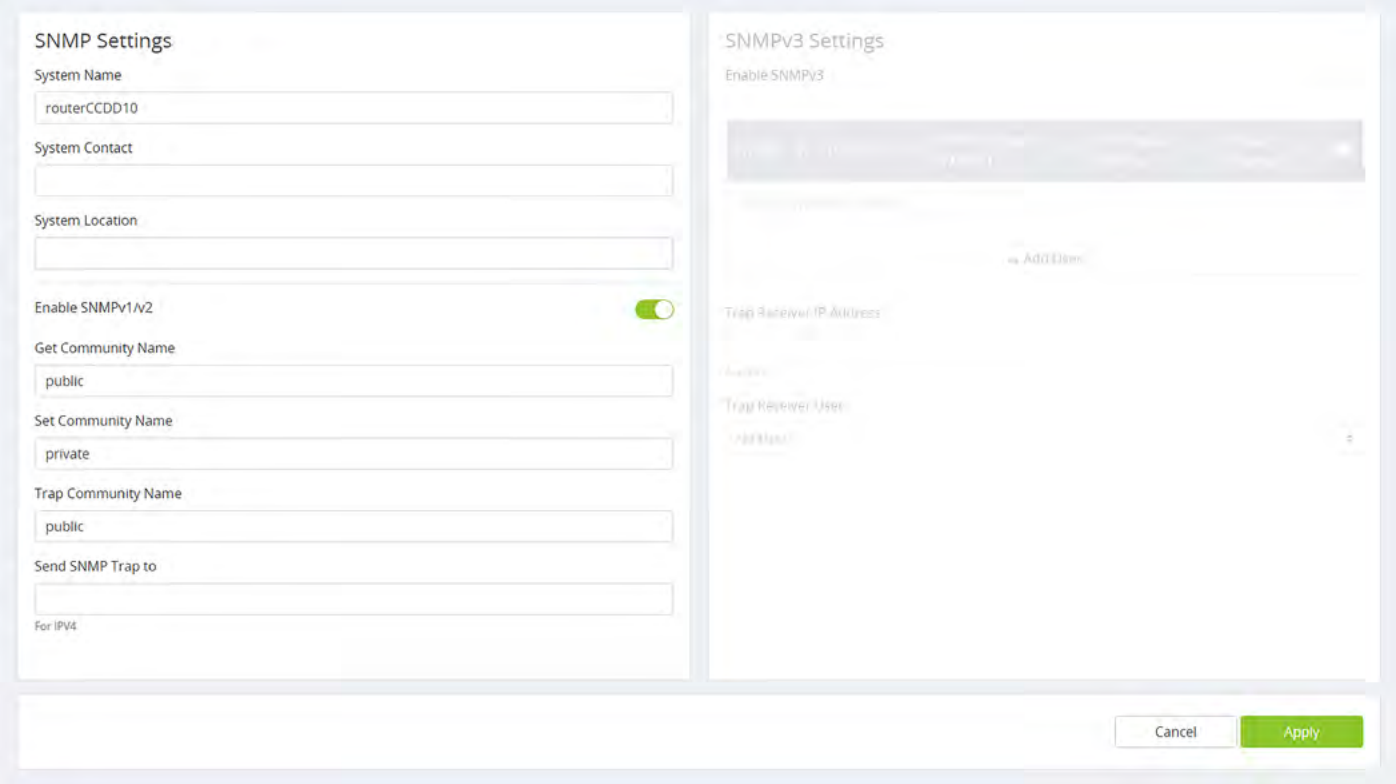
- Reserve an IP address for each device being configured, or set each device to have a static IP address. (Using a DHCP address can cause the domain name to point to a different device if the address is reissued after setup.)
- Set the DNS server setting in each device to the same IP address as the router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

© 2018 Araknis Networks®

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



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.

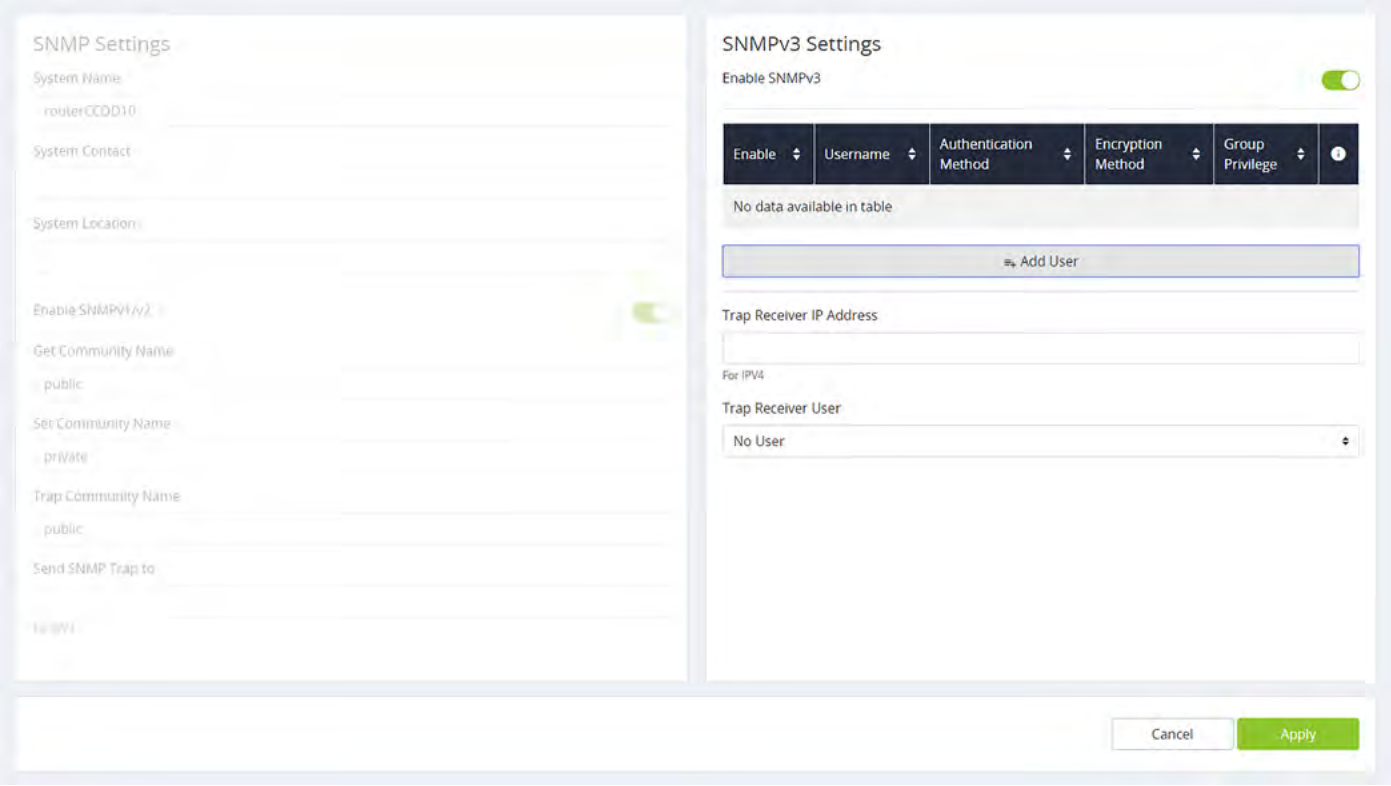
Trap Community Name: The name of the notifications community on the network.

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

© 2018 Araknis Networks®

SNMPv3 Settings Section

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

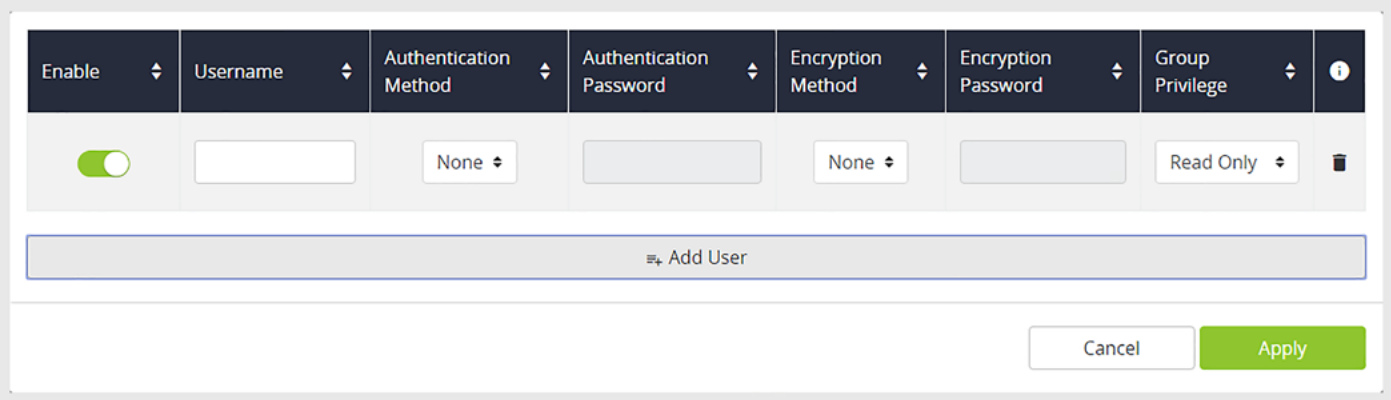


The user table lists all users currently enabled.

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:



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

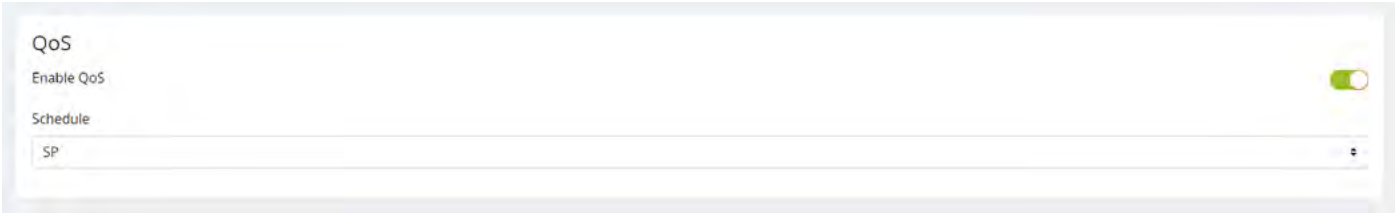
© 2018 Araknis Networks®

Advanced > QoS

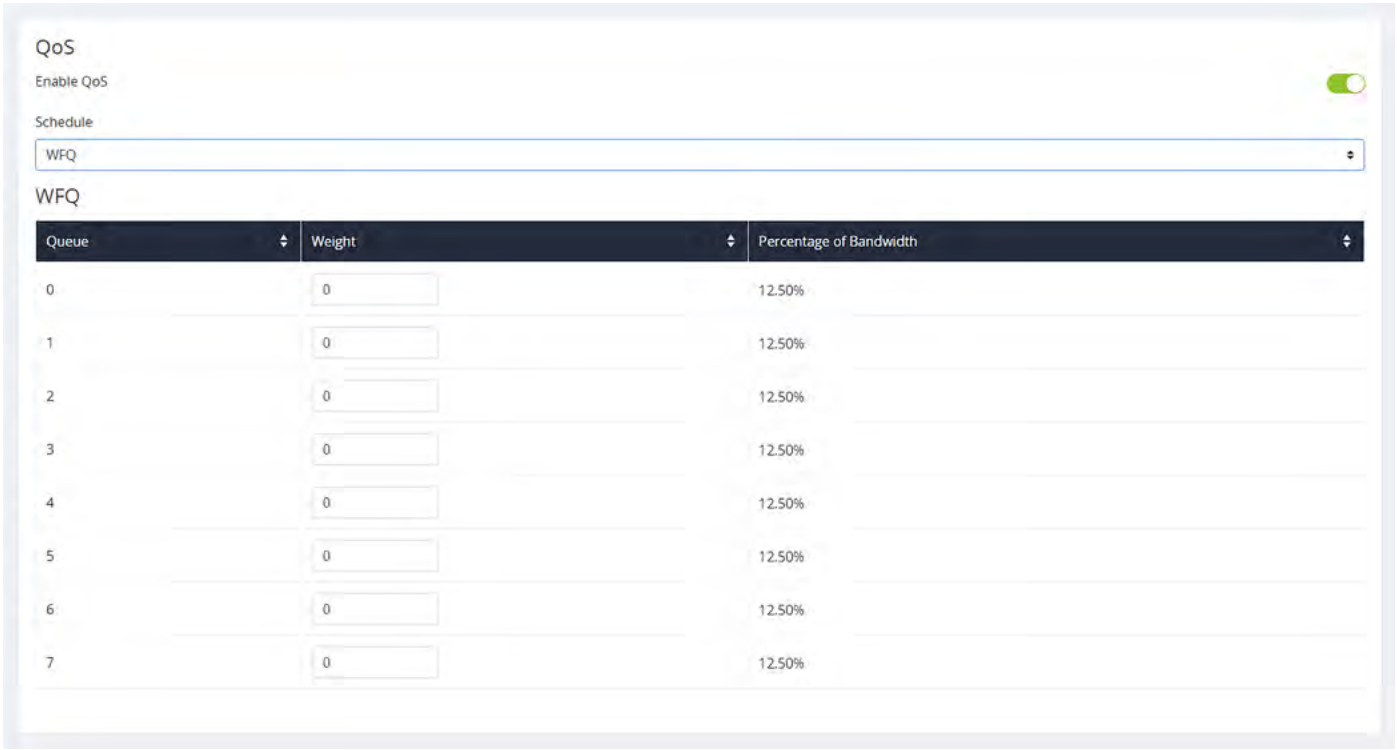
This section is for advanced users only.

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 queuing). 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).

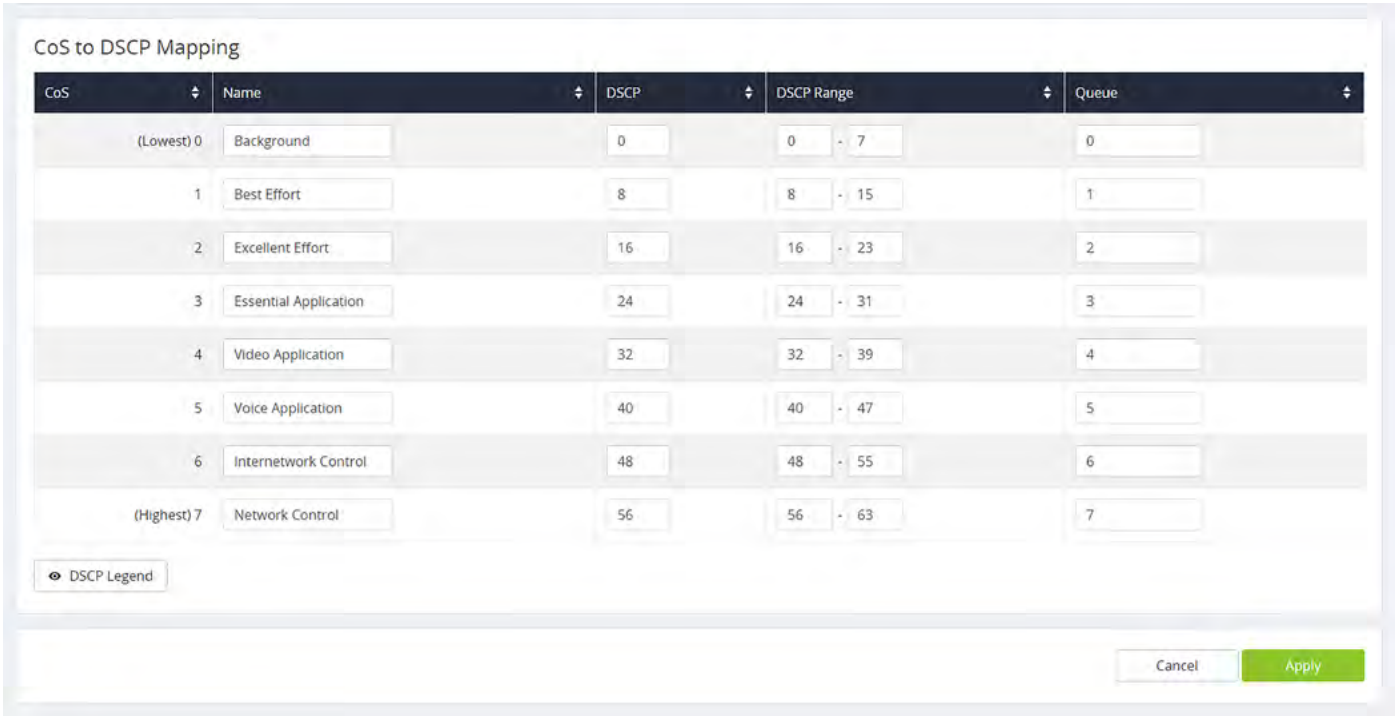
© 2018 Araknis Networks®

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.



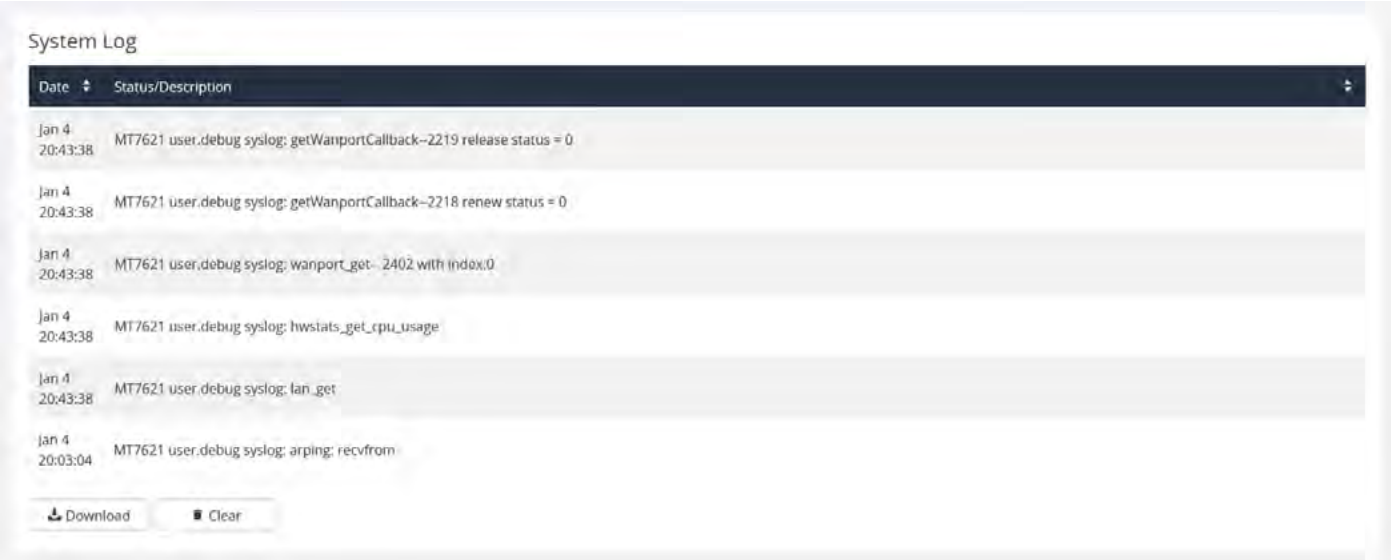
© 2018 Araknis Networks®

System Log

System Log Section

Here you see recorded activities and status changes.

At the bottom, buttons allow you to download the full log to your computer, and to clear the log entries when needed.



© 2018 Araknis Networks®

Specifications

Interfaces

Features	AN-310-RT-4L2W
WAN - RJ45 10/100/1000 Base-T	2
LAN - RJ45 10/100/1000 Base-T	3
LAN/WAN - Combo RJ45/SFP 10/100/1000Base-T	1
USB	1 (USB3.0) - Not Available at Launch
Wireless Interface	N/A
Embedded Antennas	N/A

Performance

Features	AN-310-RT-4L2W
LAN - LAN Throughput	1 Gbps
WAN - LAN Throughput (Unidirectional)	1 Gbps
WAN - LAN Throughput (Bidirectional)	500 Mbps

L2 Features

Features	AN-310-RT-4L2W
VLANs	Yes - 802.1Q
RJ45 Auto-sensing	Yes
RJ45 Auto-negotiation	Yes

L3 Features

Features	AN-310-RT-4L2W
WAN/LTE Link Failover	Not Available at Launch
Static Routing	Yes
Inter-VLAN Routing	Yes
DHCP Server	Yes
DHCP Client	Yes
DHCP Relay	Yes
DNS Relay	Yes
DDNS	Yes
1:1 NAT	Yes
PAT (Port Address Translation)	Yes
Port Trigger	Yes
DMZ Host	Yes
IPv6	Yes

© 2018 Araknis Networks®

Security

Features	AN-310-RT-4L2W
Stateful Firewall	Yes
Stateful Packet Inspection (SPI)	Yes
DoS Prevention	Yes
Ping of Death	Yes
SYN Flood	Yes
IP Spoofing	Yes
Port Forwarding	Yes
Content Filtering (URL & Keyword)	Yes
UPnP	Yes
Bonjour	Bonjour Client at Launch

VPN Features

Features	AN-310-RT-4L2W
IPSec	Not Available at Launch
PPTP Server	Yes
PPPoE	Yes
OpenVPN	Yes
Encryption (IPSec)	DES, 3DES, AES-128, AES-192, AES-256
Authentication (IPSec)	MD5/SHA-1

Management

Features	AN-310-RT-4L2W
Web Management	Yes
SNMP v1,2c,3	Yes
OvrC Pro Embedded	Yes
Download/Upload Config File	Yes
System Log	Yes
HTTP & HTTPS	Yes
System Time	NTP/Manually
Cloud Management	Yes

© 2018 Araknis Networks®

Environmental & Physical

Features	AN-310-RT-4L2W
Product Dimensions (W x H x D) in inches	12.99 x 1.73 x 9.05
External Power Supply	Internal
Temperature Range	Operating Temp. 0°C to 40°C (32°F to 104°F)
	Storage Temp. 0°C to 70°C (32°F to 158°F)
Humidity	Operating Humidity 10% to 85% Non-Condensing
	Storage Humidity 5% to 90% Non-Condensing
Certifications	CE, FCC, UL, UPnP
Rack Mountable	Can be mounted by using AN-ACC-SW-EAR-L-13

2-Year Limited Warranty

Araknis Networks products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to SnapAV or a designated service center with prior notification and an assigned return authorization number (RA).

Technical Support

P: 866-838-5052

E: techsupport@araknisnetworks.com

© 2018 Araknis Networks®