Table of Contents

snap one

AN-X20-RT

Araknis x20 Series Multi-Gig VPN Router User Manual

Quick links:

- [Araknis 220 Router Quick Start Guide](#)

- [Araknis 520 Router Quick Start Guide](#)

- [How to Configure OpenVPN on Araknis Routers](#)

- [Setting up PPTP VPNs with Araknis Router](#)

- [Araknis x20 Series Router Access Command Lists (ACLs) Setup Example](#)

- [Araknis 520 Router IPSec (Gateway to Gateway) VPN Setup Example](#)

- [How to Configure Route Binding on Araknis 520 Series Routers](#)

Interface access

Araknis routers can be configured through OvrC or the local interface. The local interface is accessible using OvrC's WebConnect feature, or typing the router's default IP address, **192.168.1.1**, into your browser's address bar.

Configuring the router in OvrC

OvrC provides remote device management, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

To add this device to your OvrC account:

1.   Connect the router to the internet

2.   Log into OvrC (**www.ovrc.com**)

3.   Create a customer in OvrC or select an existing one.

4.   Click the **Add Device** button, then enter the router's MAC address and Service Tag.

5.   Click the **WebConnect** icon to connect to the router's local interface.
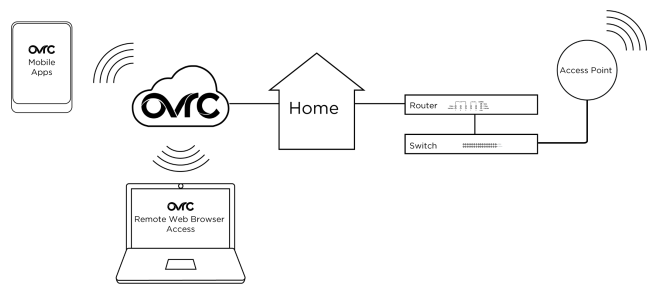
Logging in to the local interface

1. Log into the AP using the default credentials:

Username	araknis
Password	araknis

2. You must update the password after initial login.
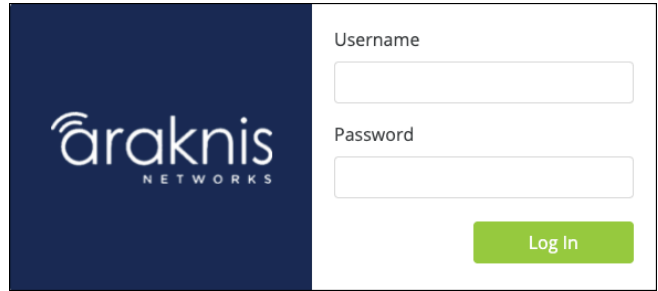
> **Pro Tip:** Strong passwords are long and unrelated to the client's public details. For example, thepepperonipizzas is stronger and easier to remember than P@ssword or thesmiths.

Next steps

Click on **Settings** to expand configuration options, such as:

- **System** — Configure the System name, IP address, time zone, and Daylight Saving Time.

- **WAN** — Configure the WAN connection type, speed, and DNS servers.

- **LAN** — Configure the default DHCP server settings and/or add another DHCP server for a VLAN.
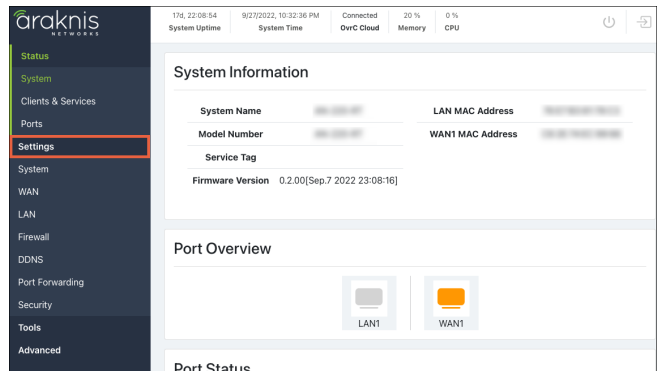
Interface overview
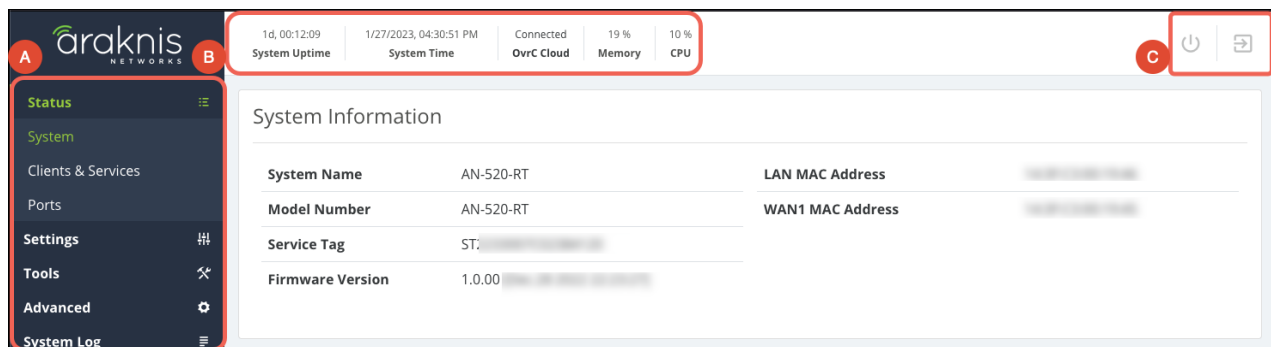
1. **Main Navigation Menu** — Click on the headers to access the submenus to configure and maintain the router.

2. **Top Bar** — Displays the overall status of the router, including the system uptime, the current time, OvrC cloud connection, memory, and system CPU usage.

3. **Restart and Logout** — Use these buttons to restart or log out of the router.

Pro Tip: Click the info icon ⓘ to learn more about individual settings.

Status

System

This page provides an overview of the router's system information, port status, and WAN configuration.

System Information

- **System Name** - The DHCP hostname of the device, which is how the router appears in network scans. Configurable under **Settings** > **System** > **System Name**.

- **Model Number** - The part number for the router (as shown on our website).

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

- **Firmware Version** - The version installed on the router. Use OvrC to check for possible updates.

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

- **LAN MAC Address** - The MAC address that appears for the router's entry on Local Area Network (LAN) scans. Use this MAC address when manually adding the router to OvrC.

Port Overview and Status

The **Port Overview** is color-coded based on its negotiated speed:

- **Gray** — The port is not detecting a connection.

- **Red** — The port is disabled.

- **Orange** — The port detects a 10/100Mbps connection.

- **Green** —The port detects a 1Gbps connection.

- **Blue** — The port detects a 2.5Gbps connection.

The **Port Status** table provides detailed information for each port on its line. These can be configured under **Settings** > **LAN** > **LAN Settings**. Click the LAN port to configure it.

WAN Status

The **WAN** status tile(s) display current information about the status of the WAN interfaces. It updates in real time.

You can also **Release** the current WAN IP address to the DHCP pool and receive a new one or **Renew** the current WAN DHCP connection. The WAN IP address may or may not change.

WAN1

Name	WAN1
IP Address	98.
Subnet Mask	255.255.248.0
Default Gateway	98.
DNS 1	209.
DNS 2	209.

🔒 Release	↻ Renew

1Gb/s

Note: 520 series routers have a WAN1 and WAN2 tile if WAN2 has been configured.

The displayed fields are configurable under **Settings** > **WAN**.

- **IP Address** — The WAN/Public IP address of the connection.

- **Subnet Mask** — The subnet mask assigned to the WAN.

- **Default Gateway** — The IP address of the WAN gateway.

- **DNS 1** — The primary domain name server (DNS) of the router.

- **DNS 2** — The secondary DNS of the router.

The maximum possible speed of the WAN port's connection is displayed at the bottom.

> **Note:** The connection speed detected is the maximum speed attainable on the connection. It does not mean that much data is passing through the connection.

Clients & Services

This page provides basic Firewall features and status reports of clients on the network, VPN tunnels, and ports being forwarded.

Firewall Status

Displays the status of configured Firewall settings. For a full list of configurable Firewall settings, go to **Settings** > **Firewall**.
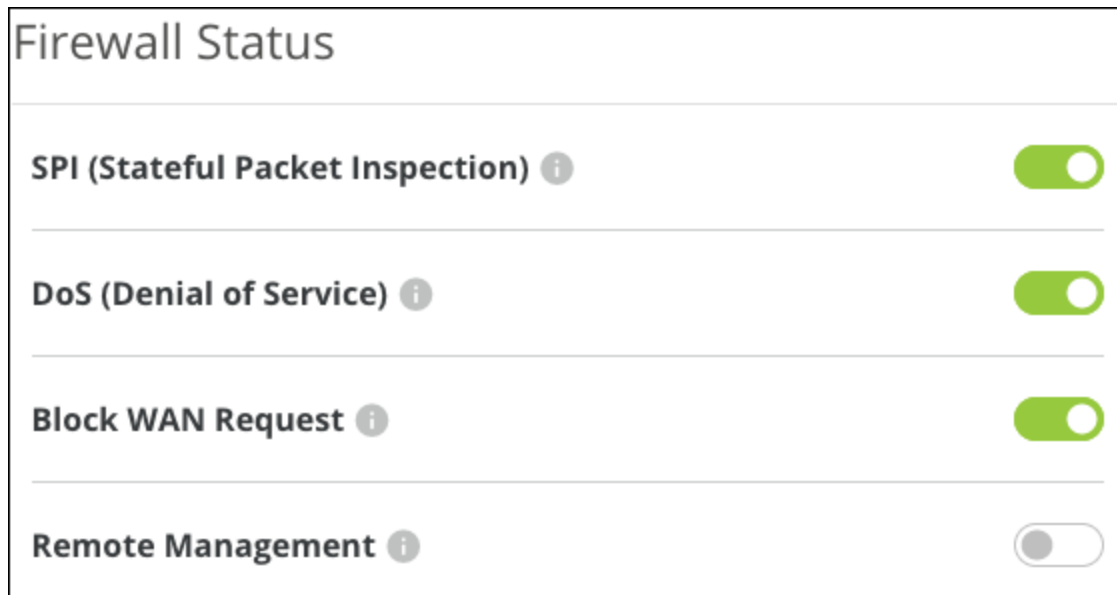
Firewall Status

- **SPI (Stateful Packet Inspection)** — Inspects incoming and outgoing packets and their connection state. Enabled by default.

- **DoS (Denial of Service)** — Prevents a denial-of-service attack, which attempts to make a network unavailable by flooding the network host with irrelevant traffic. Enabled by default.

- **Block WAN Request** — Prevents the router from responding to ping requests on the WAN port, making your network seem invisible from the outside. Enabled by default.

- **Remote Management** — Enable to configure a port to access the router remotely. The port must be configured under Settings > Firewall. Disabled by default.

Pro Tip: Use a VPN or OvrC WebConnect instead of Remote Management.

VPN Tunnel Status

This table provides the amount and type of VPN tunnels used on the router and how many VPN tunnels can be configured.

Note: The 220 series router does not support IPSec.

snap one™

VPN Tunnel Status		
	Used	**Available**
OpenVPN	0	20
IPSec	0	50
PPTP	0	20

DHCP Clients and Status

The router presents tiles for the total number of clients connected to the network and separates them into DHCP clients that the router has assigned an IP address and the total number of static clients that have manually been assigned IP addresses.

Total Clients	Total DHCP Clients	Total Static Clients
26	26	0
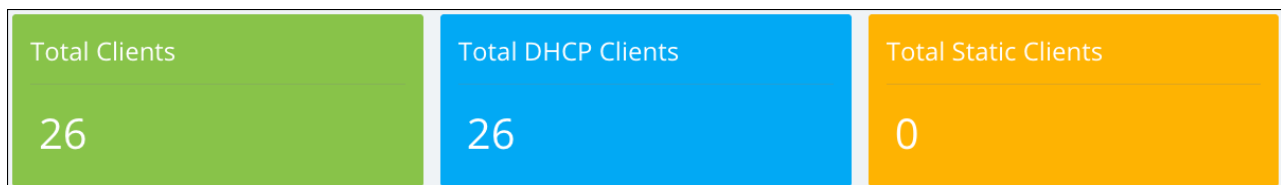
The **DHCP Status** table shows how many networks have been configured on the router, the IP address range, the number of DHCP IPs used, how many IPs are still available, and the total number of IPs in the DHCP pool.

DHCP Status				
Network	**Range**	**DHCP IPs Used**	**DHCP IPs Available**	**Total DHCP Pool**
192.168.1.1	192.168.1.100 - 192.168.1.199	26	74	100

The **Client Table** provides an entire list of connected client devices and information about them. Use the **Show** filter to limit the table to DHCP or Static clients.

Client Table

Client Host Name	IP Address	MAC Address	Manufacturer	ℹ	ℹ
4CH NVR	192.168.1.114 ⏲			⊘	🗑
new-host3	192.168.1.115 ⏲		Nintendo Co.,Ltd	⊟₊	🗑
new-host9	192.168.1.117 ⏲		Nintendo Co., Ltd.	⊟₊	🗑
EmergencysMBP2	192.168.1.118 ⏲		Apple, Inc.	⊟₊	🗑
OvrC-MoIP	192.168.1.119 ⏲		SnapAV	⊟₊	🗑
Kitchen	192.168.1.120 ⏲		Apple, Inc.	⊟₊	🗑
Front Door Chime	192.168.1.122 ⏲			⊘	🗑
WattBox	192.168.1.123 ⏲		SnapAV	⊟₊	🗑

Note: Clients with a prohibitory icon (⊘) in their row did not obtain an IP address from the DHCP server. These clients either had an IP address statically assigned to them or had an IP assigned to them before the DHCP server starting up, like if the router had been restarted.

How to make a DHCP (MAC) Reservation

Click the **Add Reservation** button, then click **Apply** at the bottom of the page. To change the IP address of the reservation, go to **Settings** > **LAN** > **DHCP Reservation Table**.

Multiple reservations can be made at once.

OvrC-MoIP	192.168.1.119 ⏲		SnapAV	⊟₊	🗑

Note: You can make DHCP reservations on the Router's Details page in OvrC. Then use WebConnect to change the IP address for the reservation.

Port Forwarding table

This table shows the rules configured under **Settings** > **Port Forwarding**. If a port forwarding rule was added by UPnP the entry displays the amount of minutes left in its **Lease Time** column. Manually configured port forwarding rules display a dash as their lease time.

Port Forwarding

External Port ↕	Interface ↕	External Address ↕	Internal Port ↕	Internal Address ↕	Protocol ↕	Lease Time (Minutes) ↕	Description ↕
No data available in table							

Caution: Port forwarding is not secure and should only be configured for specific situations. Use a VPN or OvrC WebConnect instead.

Ports

This page provides the connection status, type, and how much data has been sent and received on the LAN and WAN ports.

Port Overview

LAN1   LAN2   WAN1

Port Status

Interface ↕	Name ↕	Speed ↕	Duplex ↕	VLAN ID ↕	Sent ↕	Received ↕	Errors ↕
LAN1	LAN1	1Gb/s	Full	1	92.4 GB	5.7 GB	0
LAN2	LAN2	N/C	N/C	1	0.0 KB	0.0 KB	0
WAN1	WAN1	1Gb/s	Full	N/A	5.4 GB	95.8 GB	0

The **Port Overview** is color-coded based on its negotiated speed:

- **Gray** — The port is not detecting a connection.

- **Red** — The port is disabled.

- **Orange** — The port detects a 10/100Mbps connection.

- **Green** — The port detects a 1Gbps connection.

- **Blue** — The port detects a 2.5Gbps connection.

Settings

System

System Settings

- **System Name** — Also known as the hostname. The router's model number is used by default. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), and periods.

- **System IP Address** — Enter a LAN IP address of the router using IPv4. (IPv6 options are found under **Advanced** > **IPv6**).

- **System Subnet Mask** — Displays the subnet mask of the router's default DHCP pool. This is configurable under **System** > **LAN**.

- **System LEDs** — Toggle the router's LEDs on or off.

- **System Reset** — Toggle off to disable the hardware reset process to default the router's username and password. When disabled, the reset button can only be used to restart the router or restore it to factory settings.

snap one™

Time Settings

The router uses an NTP (Network Time Protocol) server to automatically set the router's time. Use the **Time Zone** and **NTP Server** dropdown to modify these settings.

By default, the router uses the NIST (National Institute of Standards and Technology) servers to synchronize to Coordinated Universal Time.

Toggle set local time automatically (NTP) to manually enter the date and time.

Pro Tip:	Do not set the time manually unless the router is being used without an internet connection. Any device's internal clock can drift, which causes network issues.

You can toggle **Enable Daylight Saving Time** on or off. Use the **Start** and **End Date** dropdowns to configure the proper times for your part of the world. Check local regulations before configuring Daylight Saving Time.

Auto-Reboot

Enable Auto-Reboot to create a schedule for the router to restart regularly to help ensure the router is always up and functioning for the client.

Pro Tip: Set Auto-Reboot to restart the router in the early morning hours when the network is not being used. If you have other devices configured to auto-reboot, don't set them all to restart at the same time.

The network devices should start in an order that ensures every device obtains an IP address. For example, the modem should power on first, then the router, core switch, intermediate switch, then the AP, etc.

WAN

WAN Settings

- **Name** — Type to enter a new name for the WAN port, such as the name of the internet service, if you're using two WAN connections. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Speed** — Use the dropdown to select a specific connection speed or to disable the port. Options include Auto, 2.5Gbps, 1Gbps, 100Mbps, 10Mbps, and Disabled.

  - **If 100 or 10Mbps are selected,** you may set the WAN ports **Duplex** to **Full** or **Half**.

- **Connection Type** — Set to DHCP by default, options include Static, PPPoE, and Transparent Bridge.

- **PPPoE** includes fields for the Username, Password, a Keep Alive toggle, and the Redial Period. This option is typically used with DSL and other peer-to-peer Internet Service Providers (ISPs). The PPPoE password can have a maximum of 63 characters which include This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, =, and periods.

- **Transparent Bridge** requires an Internal LAN IP Range, an IP Address for the router to adopt, a Subnet Mask, a Default Gateway, and DNS Servers to be manually entered. Transparent Bridge disables all routing functions or your router. Use this feature if you must use an ISP-provided router on the network.

- **IP Address** — Editable when you select a Connection Type other than Auto.

- **Subnet Mask** — Editable when you select a Connection Type other than Auto.

- **Default Gateway** — Editable when you select a Connection Type other than Auto.

- **Use Static DNS** — Toggle on to manually enter a value for **DNS Server 1** and **2**.

- **Auto MTU —** Leave this enabled for optimal performance. The MTU (Maximum Transmission Unit) specifies the largest packet or frame allowed to be transmitted across the WAN interface.

- **MSS Clamping** — Enabled by default, MSS (Multiple Segment Size) Clamping makes outgoing traffic handle differing MTU values along the traffic path. This is commonly used with PPPoE.

- **VLAN** — Enable to enter a VLAN ID for the WAN port.

DHCP Options

DHCP options are commonly used with VoIP (Voice Over IP), as certain manufacturers require specific DHCP options for the system to work. Common DHCP options are given to assist with the configuration.

DHCP Options						
Name	**Option**	**Code**	**Type**		**Value**	**Delete**
	Host Name (12) ⌄	12	Text ⌄			🗑
≡+ Add DHCP Option						

<div align="right">Cancel   Apply</div>

Click **Add DHCP Option** to configure a new setting. Consult the service you're configuring for more information.

Release & Renew

Click to **Release** the current WAN IP address to the DHCP pool and receive a new one or **Renew** the current WAN DHCP connection. The WAN IP address may or may not change.

> **Note:** The Release and Renew buttons only work if the WAN type is DHCP or PPPoE.

🔒 Release	↻ Renew
1Gb/s	

> **Note:** The WAN speed is highlighted at the bottom of the WAN tile. If this is gray then the router does not detect a WAN connection.

Multi-WAN (520 router only)

To use WAN2 you must go to **Settings** > **LAN** and click on LAN 2 at the top of the page, then click the **Enable WAN Mode** toggle.
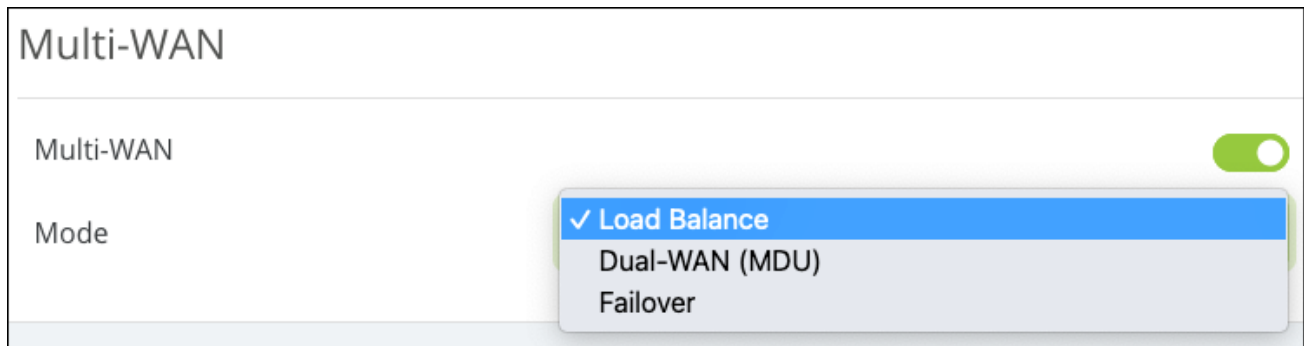
Go back to **Settings** > **WAN** to configure the WAN2 settings and enable Multi-WAN.

The Multi-WAN feature has three modes:

- **Load Balance** — Evenly distributes the bandwidth from two WAN connections to the LAN. When enabled, you can route traffic to specific WAN interfaces using advanced features like Route Binding or ACLs.

> **Note:** Load balancing marks the flow of traffic from both WAN ports with a probability of 50%, instead of marking each flow as WAN1 and WAN2. This does not apply to route binding rules.

- **Dual-WAN (MDU)** — Multiple Dwelling Unit (MDU) should be selected if the router is being used within a complex with multiple residences, like a condominium. Enable this feature in the router if it's being fed from the head router of an MDU. Connect WAN1 to the ISP and WAN2 to the callbox network.

- **Failover** — Logs and then fails over to the secondary WAN interface. The router fails back to the primary WAN when its connection is restored.

Network Service Detection (NSD)

Toggle on to configure the detection system used to determine if the WAN port is down, and what actions the router should take.

> **Note:** All configured conditions must be met for NSD to take **Action**. If Ping Remote IPs and Resolve Domain Names are configured, but only the pings are failing, NSD will not fail over.

Network Service Detection (NSD)

Network Service Detection WAN1 ⓘ   🟢

Retry Count ⓘ   `5`

Time Between Retries ⓘ   `30`

Action ⓘ   Log Only ⌄

Ping Default Gateway   🟢

Ping Remote IP(s)   🟢

Ping Remote IP(s) ⇅	ⓘ ⇅
8.8.8.8	🗑
4.2.2.2	🗑

⇉ Add IP Destination

Resolve Domain Names   🟢

Resolve Domain Names ⇅	ⓘ ⇅
www.google.com	🗑

⇉ Add URL

- **Retry Count** —The number of times the router must fail to reach the specified IP Address(es) and/or Domain Names before taking the Action specified.

- **Time Between Retries** — The amount of time in seconds between attempts to reach the specified IP Address(es) and/or Domain Names.

- **Action** — Determines what happens when the WAN interface does not detect a connection. Options include:

  - **Log Only** — Logs the events in the System Log.

  - **Log and Reboot Interface** — Logs the events in the System Log and restarts the interface (port).

- **Ping Default Gateway** — Enabled by default. This tells the NSD to try pinging the gateway address that's providing an IP address to the WAN port.

- **Ping Remote IP(s)** — Enable to ping IP addresses other than the default gateway. Do not enter local IP addresses. You can change the default remote IPs by typing in the field or add further IP addresses by clicking **Add IP Destination**.

- **Resolve Domain Names** — Enable to use a domain name instead of IP addresses, like www.google.com. Click **Add URL** to add more domain names to ping.

LAN

LAN Settings

The LAN Settings display the LAN ports, their speed (color coded), and their duplex settings. Each port is color-coded based on its negotiated speed:

- **Gray** — The port is not detecting a connection.

- **Red** — The port is disabled.

- **Orange** — The port detects a 10/100Mbps connection.

- **Green** —The port detects a 1Gbps connection.

- **Blue** — The port detects a 2.5Gbps connection.
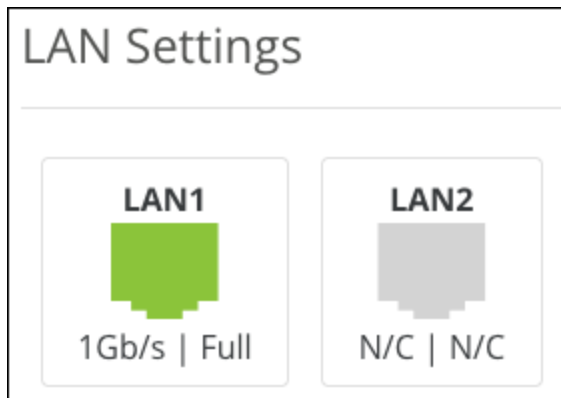
Click on a port to open a new window to configure the port's **Name**, **Speed**, and enable **Jumbo Frames**. The **MTU** (Maximum Transmission Unit) can be edited when Jumbo Frames are enabled.

LAN 2 (520 routers only) has an Enable WAN Mode option to enable the multi-WAN feature.

DHCP Server Settings

Click a DHCP card to edit the settings or click **Add a DHCP Server** to configure a new one.

This opens a new window with configurable settings.

- **VLAN ID** — The VLAN ID is assigned to the DHCP server. This cannot be changed for the default DHCP server.

- **Name** — Enter a name for the DHCP server. This field accepts alphanumeric (a - z and A - Z) characters, spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Default Gateway** —The IP address of the router for this DHCP server. **Device Management** must be enabled on the VLAN ID to access the router at this address.

- **Subnet Mask** — Type in this field to edit the Subnet Mask.

- **DHCP Mode** — VLAN1 is set to **Server**, by default, to allow the router to hand out DHCP requests to connected client devices. When creating new VLANS, your options are:

    - **Server** — Allows the router to hand out DHCP requests to connected client devices.

    - **None** — The DHCP server cannot hand out DHCP requests.

    - **Relay** — Forwards DHCP requests to a separate device acting as the DHCP server.

- **IP Range** — Enter the beginning and end address of the IP range the DHCP server can assign to connected clients.

- **Lease Time (Minutes)** — The amount of time before the DHCP server renews the IP of a client device. The client may receive a new IP address or the old one again.

- **DNS Server Mode** — Set to **Proxy**, by default. This provides the Gateway IP address as the DNS server to DHCP clients. Setting the DNS Server Mode to **Static** allows you to designate a specific DNS server to the DHCP clients.

- **DHCP Options** — Select which DHCP options should be used with the DHCP server.

DHCP Options

DHCP options are commonly used with VoIP (Voice Over IP), as certain manufacturers require specific DHCP options for the system to work. Common DHCP options are given to assist with the configuration.

Click **Add DHCP Option** to configure a new setting. Consult the service you're configuring for more information.

VLAN Settings

The **VLAN Settings** button takes you to the VLAN Settings page under **Advanced** > **VLANs**.

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

VLANs							
VLAN ID ⬍	Name ⬍	Inter-VLAN Routing ⬍	Device Management ⬍	LAN 1 ⬍	LAN 2 ⬍	❶ ⬍
1	Default	⬤	⬤	Untagged ∨	Untagged ∨	🗑
2	Guest	⬤	⬤	Tagged ∨	Excluded ∨	🗑
➥ Add VLAN							

To create a new VLAN, click the **+ Add VLAN button** and configure the below settings:

- **VLAN ID** — A unique numerical identifier for the VLAN between 1 and 4095. The default VLAN is always set to 1. The maximum number of VLANs is listed below:

    - For AN-220 routers, 32 total VLANs.

    - For AN-520 routers, 48 total VLANs.

- **Name** — Enter a name that describes what the VLAN is being configured for. Like a Guest network or Surveillance devices. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Inter VLAN Routing** — Toggle on to allow communication between client devices connected to VLANs with this setting enabled. Do not use this feature if security between VLANs is a concern.

> **Note:**   You must enable this feature on each VLAN that you want to communicate with each other.

- **Device Management** — Allows devices connected to this VLAN to access the router at its default gateway IP address.

- **LAN 1 and 2** — Each LAN port may be configured as one of one following options:

  - **Untagged** — VLAN frames handled through this port are not tagged with a VLAN ID.

  - **Tagged** —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.

Note: LAN ports can only allow Untagged traffic from one VLAN.

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

DHCP Reservation Table

This shows a list of all DHCP addresses reserved by your system. DHCP (MAC) Reservations can be created in OvrC or the router.

Click **Add DHCP Reservation** to create a new reservation from this page. You must provide the MAC address of the device you wish to reserve.

Pro Tip: It's easier to make the reservation in OvrC or under **Status** > **Clients & Services** > **Client Table**, then change the IP address on this page.

DHCP Reservation Table

Enable	Static IP Address	MAC Address	Name	Delete 🛈
⬤	192.168.1.180		Philips hue	🗑
⬤	192.168.1.114		4CH NVR	🗑
⬤	192.168.1.122		Front Door Chime	🗑
⬤	192.168.1.119		OvrC-MoIP	🗑
		⇥ Add DHCP Reservation		

The **Name** field accepts alphanumeric (a - z and A - Z) characters, spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

You can quickly **Enable** or disable reservations from this page. Or click the trash icon to **Delete** them.

To change the IP address of the reservation, enter the desired address under **Static IP Address**, then click **Apply**. Reservations can be made outside the IP range specified in the LAN settings.

> **Note:**   You must restart the reserved device for the change to take effect.

Firewall

Use this page for more advanced Firewall features, compared to the options on the **Status** > **Clients & Services** page.

- **Enable Firewall** — Toggle the Firewall settings on or off. Default is on.

- **Block ICMP Broadcast** — Enabled by default, this feature prevents the router from responding to ICMP (Internet Control Message Protocol) probe packets.

- **SPI (Stateful Packet Inspection)** — Inspects incoming and outgoing packets and their connection state. Enabled by default.

- **DoS (Denial of Service) Prevention** — Prevents a Denial of Service attack, which attempts to make a network unavailable by flooding the network host with irrelevant traffic. Enabled by default.

- **Block WAN Request** — Prevents the router from responding to ping requests on the WAN port, making your network seem invisible from the outside. Enabled by default.

- **Remote Management** — Enable to configure a port to access the router remotely. The port must be configured under Settings > Firewall. Disabled by default.

Pro Tip: Use a VPN or OvrC WebConnect instead of Remote Management.

- **Multicast Passthrough** — Enables multicast traffic to pass from WAN to LAN. Typically used when a multicast source is on the WAN side of the network. Disabled by default.

- **IPSec Passthrough** — Allows IPsec VPN traffic to pass from WAN to LAN. Typically used in Double NAT topologies where there is an IPsec tunnel established upstream to the WAN side of this router. Disabled by default.

Note: This feature must be enabled for Wi-Fi calling to work for most phone providers.

- **PPTP Passthrough** — Allows PPTP VPN traffic to pass from WAN to LAN. Typically used in Double NAT topologies where there is a PPTP tunnel established upstream to the WAN side of this router. Disabled by default.

- **Enable DMZ** — Use this feature when the ISP does not support bridging or bypassing their firewall or NAT (Net Address Translation). You must enter the DMZ address in IPv4 format. Disabled by default.

Misc. Settings

- **UPnP** — Enables Universal Plug and Play (UPnP), a protocol that permits the network to discover and operate devices and applications seamlessly. Disabled by default.

- **Bonjour Client** — Bonjour is Apple's implementation of Zero Configuration networking, which allows users to search, locate, and set up Apple devices on the network. Enabled by default.

Note: Bonjour must be enabled in Safari's **Preferences**. Then it is accessible in Safari's **Bookmarks** feature.

- **Flow Control** — Enables IEEE 802.3x protocols around managing congestion on the network. Only enable this feature if a use case specifically asks for it. Disabled by default.

- **SIP ALG** — Enables the Application Layer Gateway, a feature that inspects and modifies VoIP traffic, so it is not rejected by the firewall. Consult your VoIP hardware and service provider before enabling this feature. Disabled by default.

- **UDP Timeout (Seconds)** — The amount of time before the UDP session times out. Increase this value to ensure persistent connectivity of VoIP devices. Serves as Consistent NAT. Default value is 60.

- **NAT Loopback** — Allows remote access mechanisms like DDNS to be used on the local network. For example, if you're using a DDNS for remote access to a camera system, you can use the DDNS address while you're connected to the local network. Enabled by default.

DDNS

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

Select which DNS **Service** to use and enter your desired URL into the **Host Name** field, then click **Apply.** A unique ID (often two to four digits) is added to the hostname if that specific URL is already being used. If you do not like this assignment, try a different hostname or DNS service.

For example, If you choose myhome as your hostname, your system's URL is myhome.AraknisDNS.com. If someone has already claimed the myhome URL, your DDNS URL would look like myhome13.AraknisDNS.com.

DDNS hostnames can include alphanumeric (a - z and A - Z) characters and hyphens (-). NO-IP and DynDNS accept periods for domain suffixes.

Port Forwarding

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 is processed as if you entered 192.168.1.20:80.

When software from LAN devices needs access to and from the internet, additional ports may be forwarded to the device to allow communication through the router's firewall.

> **Caution:** Port forwarding is not a secure method of remote access. Consider using a VPN or OvrC WebConnect instead.

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 (APs, managed switches, power monitoring devices)

> **Note:** Many popular programs and protocols use specific port numbers by default. For instance, HTTPS services typically use port 443, and SMTP mail services typically use port 25.

Port Forwarding

External Port ↕	Interface ↕	External Address ↕	Internal Port ↕	Internal Address ↕	Protocol ↕	Lease Time (Minutes) ↕	Description ↕
No data available in table							

To configure a port forwarding rule:

1. Click **Add Forwarding** Rule.

2. Enter the **External port** to be used when connecting to the device interface on an outside network. For example, if you enter 87, you'll add**:87** at the end of the URL.

3. If using multiple WANs, select the WAN port from the **External Address** dropdown with the ISP you want to use.

4. Enter the **Internal Port** that the local device application is using.

5. Enter a meaningful **Name** for the port forwarding rule. This field accepts alphanumeric (a - z and A - Z) characters, spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Port Triggering

Port Triggering is similar to port forwarding, except the ports only open when there is a specific request to open the port from an application.

The **Name** field accepts alphanumeric (a - z and A - Z) characters, spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Security

User Accounts

The first time you log into the Araknis router you must change the default password. To change the password again, enter a new **Password**, then enter it once more to **Confirm** and click **Apply**.

User Accounts			
Username ⬍	Password	Confirm Password	❶ ⬍
araknis	👁		🗑
⇉ Add User			

Click **Add User** to add a secondary user to the router. You cannot set permission levels, but this does allow you to delete the user should they no longer require access to the router.

Usernames can contain alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Passwords must contain at least 8 characters. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Access Management

For security reasons, **Enable HTTPS** is enabled by default to encrypt all user communication with the router.
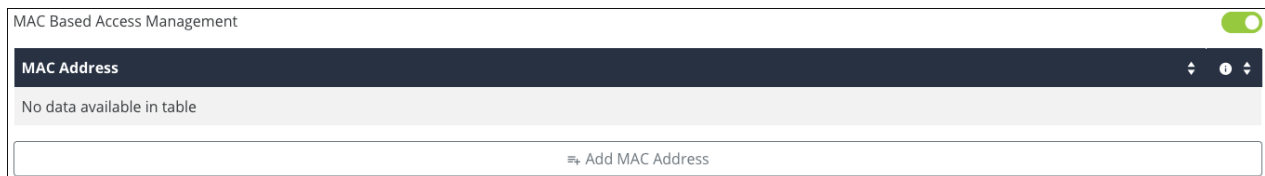

For convenience **Enable Automatic HTTP to HTTPS Redirect** is also enabled by default. This feature automatically takes you to the router's user interface without manually typing the HTTPS port at the end of the address.

If disabled, you must enter the router's IP address and the HTTPS port to access the router's interface. For example, 192.168.1.1:443.

A new HTTPS **Port** can be entered if you wish to use something other than the default 443.

MAC and IP Based Access Management

MAC Based Access Management limits access to the router's interface to the MAC addresses listed in the table. Click **Add MAC Address** to enter up to 16 devices.

IP Based Access Management limits access to the router's interface to the IP

addresses listed in the table. Click **Add IP Address** to enter up to 16 addresses.

> **Note:**   You cannot use both MAC based and IP based access management at the same time.

Whitelist & Blacklist

The **Whitelist** specifies which devices can access the network. This includes the local

network and the internet.

> **Caution:**   All devices not on the whitelist will be blocked from network access.

The **Blacklist** specifies which devices cannot access the network.
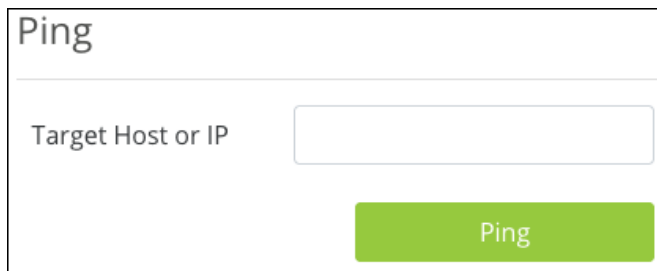
Both options have a toggle to make the list **Always Active**, or you can set a schedule.

Tools

Ping

Use a ping test to measure the amount of time it takes to reach an address on the local network or the internet. You can enter the IP address or the hostname, such as www.wikipedia.com.

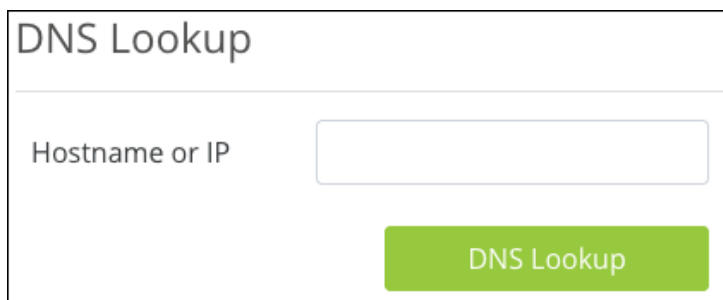**Pro Tip:**   Before selecting a DNS server, use a ping test to measure the fastest response time.

DNS Lookup

Enter a hostname (domain name) or IP address and click **DNS Lookup** to see the address it resolves to.
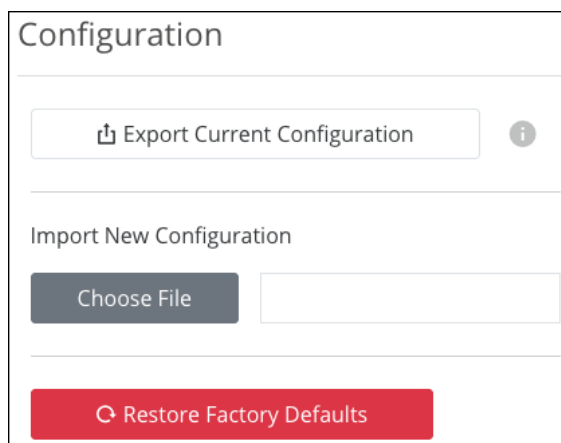
Configuration

Click **Export Current Configuration** to save a profile of all the settings currently applied to the router.

Pro Tip:	Do this before updating the firmware or restoring to factory defaults, just in case.

Note:	Router backups do not include OpenVPN certificates. You must re-download the Client Configurations to your devices after restoring the backup.

Click **Choose File** to import a configuration file

Note:	A router can only take configuration files from the same model router.

Pro Tip:	The shorter the file path to the configuration file the better. If the file upload continues to fail, place the file on your desktop and try again.

Click **Restore Factory Defaults** to set the router back to factory settings.

Trace Route

Use a traceroute to diagnose network interruptions between the switch and an address on the local network or the internet. You can enter an IP address or a hostname, such as www.youtube.com.

Enter a **Hostname or IP address**, then enter the **Maximum Hops** to test.

Trace Route

Hostname or IP	
Max Hops	30

Traceroute

Firmware Settings

The Firmware Settings tile displays information about the current firmware version installed on the router.

Use OvrC to keep the router on the latest firmware.

Download the latest firmware from the router's support tab to update the firmware manually. Then click **Browse** to upload the firmware file to the router.

Pro Tip: The shorter the file path to the firmware file the better. If the file upload continues to fail, place the file on your desktop and try again.

Advanced

Static Route

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

Static routes are commonly used to pass 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 using an IP address of 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

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

Routing Table

Destination	Subnet Mask	Gateway	Interface
0.0.0.0	0.0.0.0	98.	WAN1
10.	255.255.255.0	10.	tun0
10.	255.255.255.255	0.0.0.0	tun0
98.	255.255.248.0	0.0.0.0	WAN1
98.	255.255.255.255	0.0.0.0	WAN1
192.168.1.0	255.255.255.0	0.0.0.0	LAN

Static Routing Table

This table displays configured Static Routes.

snap one

Static Routing Table

Destination	Subnet Mask	Gateway	Interface	Delete ⓘ
			WAN1 ⌄	🗑
			LAN ⌄	🗑
≕₊ Add Static Route				

Click **Add Static Route** and enter the following information to create a static route:

- **Destination** — The subnet you're configuring a static route for.

- **Subnet Mask** — The subnet mask of the Destination.

- **Gateway** — The IP address of the subnet's gateway. An asterisk (*) can be used as a wildcard.

- **Interface** — Select the WAN or LAN port for the static route to exist on.

Click the **trashcan** icon to delete a static route.

NAT

Net Address Translation (NAT) allows you to map local IP addresses to a specific public IP address.

1:1 NAT

Use this table to view and configure NAT. **Enable 1:1 NAT** to allow the LAN IP entries to appear under the WAN IP entries.

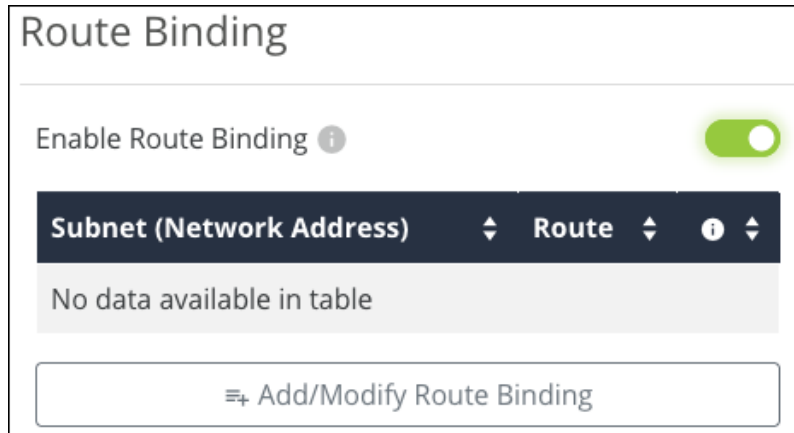Click **Add 1:1 NAT Rule** to map a LAN IP address to a WAN IP address.

Click the **trashcan** icon to delete an entry.

Route Binding (520 routers only)

Use Route Binding to force a subnet route through a specific WAN interface.

Click **Enable Route Binding to Add** a new entry or make the previously configured entries active.
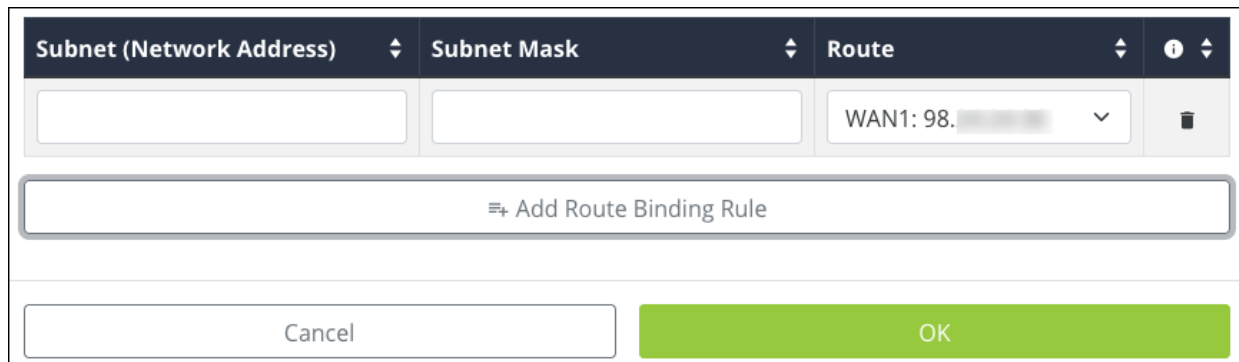

Click **Add/Modify Route Binding** to add or modify a Route Binding rule and modify the below information.

- **Subnet (Network Address)** — The starting IP address of the subnet.

- **Subnet Mask** — The subnet mask of the Subnet (Network Address).

- **Route** — Select the WAN port for the traffic to pass through.

Click the **trashcan** icon to delete a static route.

VLANs

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

To create a new VLAN, click the **+ Add VLAN button**, and configure the below settings:

- **VLAN ID** — A unique numerical identifier for the VLAN between 1 and 4095. The default VLAN is always set to 1. The maximum number of VLANs is listed below:

    - For AN-220 routers, 32 total VLANs.

    - For AN-520 routers, 48 total VLANs.

- **Name** — Enter a name that describes what the VLAN is being configured for. Like a Guest network or Surveillance devices. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Inter VLAN Routing** — Toggle on to allow communication between client devices connected to VLANs with this setting enabled. Do not use this feature if security between VLANs is a concern.

> **Note:**   You must enable this feature on each VLAN that you want to communicate with each other.

- **Device Management** — Allows devices connected to this VLAN to access the router.

- **LAN 1 and 2** — Each LAN port may be configured as one of one following options:

48

- **Untagged** — VLAN frames handled through this port are not tagged with a VLAN ID.

- **Tagged** —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.

Note: LAN ports can only allow Untagged traffic from one VLAN.

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

VPN

A Virtual Private Network (VPN) connects 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 networks. VPNs may be configured using OpenVPN, PPTP, or IPSec standards.

Total number of supported VPNs per router:

Router Series	OpenVPN	PPTP	IPSec
220	20	5	x
520	20	50	50

Note: The 220 series router does not support IPSec.

Open VPN

The Araknis router has 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.
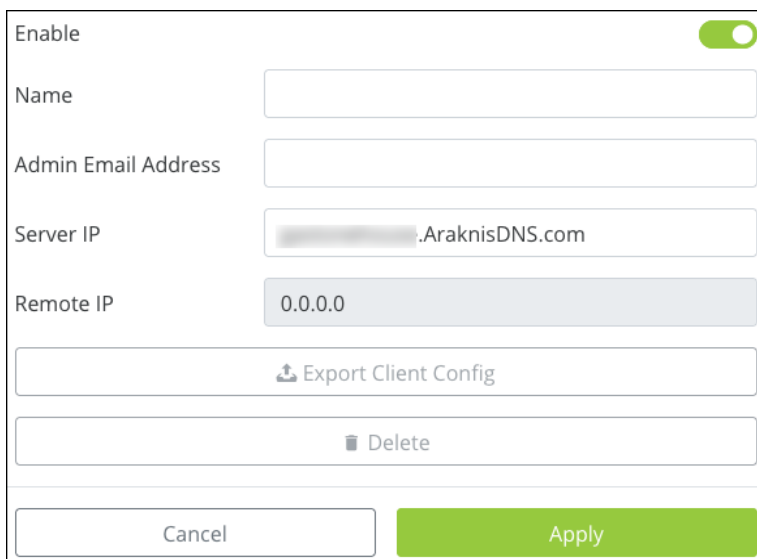

To create an OpenVPN tunnel:

1. Select a **Protocol Type**.

   - **UDP** offers faster speeds, lower latency, and is the preferred OpenVPN connection method. In rare occasions, UDP can be less reliable because the protocol does not guarantee delivery of the packets.

   - **TCP** offers a more stable connection, as the protocol guarantees the delivery of the packets and is less likely to be blocked by firewalls. This method tends to slow transfer rates down.

2. Enable **Redirect Gateway,** if desired. This feature ensures all internet traffic is routed through the VPN tunnel, but it also reduces VPN connection speed.

> **Note:** If this feature is enabled after you configured the VPN you must re-export the configuration.

3. Click **Add New Tunnel**.

4. Enter a **Name** for the tunnel. This field accepts alphanumeric (a - z and A - Z) characters, spaces, hyphens (-), and underscores (_).

5. The **Server IP** automatically populates with a public IP or a DDNS (if there is a DDNS configured in the router). The Remote IP field cannot be edited. This field accepts alphanumeric characters (a - z and A - Z), spaces, hyphens (-), and underscores (_).

6. Click **Apply**.

7. Click **Export Client Config** and save the file in an easy-to-remember location.

The OpenVPN config file can be imported to the OpenVPN app available in the App Store, Google Play Store, or from OpenVPN when using Windows. MacOS has multiple third-party options for OpenVPN clients. Follow the instructions provided by the OpenVPN client on the machine.
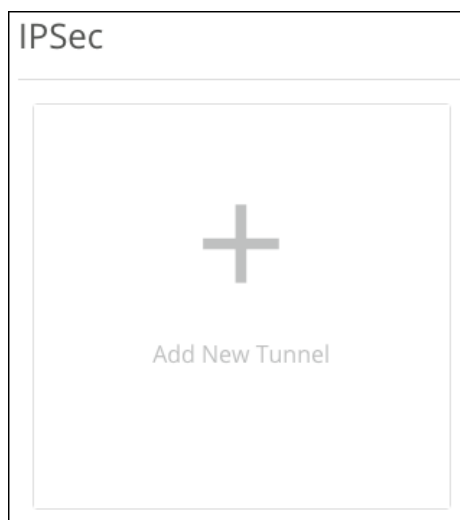
IPSec

IPSec, sometimes known as Gateway-to-Gateway, allows you to configure a VPN tunnel between two routers so that devices on each network can communicate with each other.

> **Note:** Because IPSec VPNs connect two sites, you must configure the VPN on both routers.

> **Note:** SHA-512 in Phase 1 does not work between Araknis x10 and x20 routers. A lower authentication should be used to ensure compatibility with x10 or 3rd party routers.

> **Note:** Compress cannot be used when IKEv1 with Phase 2 Authentication SHA-256/SHA-512 is selected.

IPSec

To create an IPSec VPN:

1. Click **Add a New Tunnel** and **Enable** it.

2. Give your tunnel a **Nam**e. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

> **Note:** The Mode cannot be modified.

3.   Use the **Interface** dropdown to select a WAN port for the tunnel to use.

4.   **Remote IP** is the site you're connecting to. Use the dropdown menu to select **IP Address** or **URL** (DDNS). Enter the WAN IP, or DDNS, in the **IP Address** field below.

Enable	⬤
Name	
Mode	Gateway to Gateway ⌄
Interface	WAN1 : ▓▓▓▓ ⌄
Remote IP	IP Address ⌄
IP Address	0.0.0.0

5.   The Local Group Setup fields auto-populate but can be modified. Selections differ based on the **Local Security Gateway Type** and **Local Security Group Type** selected.

Local Group Setup

Local Security Gateway Type	IP Only ⌄
IP Address	▓▓▓▓
Local Security Group Type	Subnet ⌄
Subnet Mask	192.168.1.0/24

Note: Each router must use a different IP scheme to connect to the tunnel.

6.   The **Remote Group Setup** auto-fills with the information you entered in Step 4. The **Subnet Mask** field shows the CIDR notation of the Remote Group.

snap one™

Remote Group Setup

Remote Security Gateway Type	IP Only ⌄
IP Address	0.0.0.0
Remote Security Group Type	Subnet ⌄
Subnet Mask	0.0.0.0/24

Pro Tip: Verify the last digit is zero, to include the entire IP range.

7.   The IPSec Setup fields are customizable but can be left at their defaults. Click **Apply**.

Note: The **Preshared Key** must match on both routers. The password must be between 6 −64 characters and accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

IPSec Setup

Keying Change	IKE V2
Phase 1 DH Group	Group 5
Phase 1 Encryption	AES-128
Phase 1 Authentication	SHA-1
Phase 1 SA Lifetime	28800
Phase 2 DH Group	Group 5
Phase 2 Encryption	AES-128
Phase 2 Authentication	SHA-1
Phase 2 SA Lifetime	3600
Preshared Key	

Advanced Options

🗑 Delete

Cancel   Apply

The second router's setup should be the same. Keep in mind your **Local** and **Remote Groups** are switched and each router must use a different IP scheme to connect.

Advanced Options

- **Aggressive Mode** — Enable for a less secure, but faster VPN authentication.

- **Compress** — Enable to compress the traffic sent over the VPN, before it's encrypted.

  Note: Compress cannot be used when IKEv1 with Phase 2 Authentication SHA-256/SHA-512 is selected.

- **Dead Peer Detection Interval** — Enable for the router to send a Dead Peer Detection Packet (DPD) to verify if the router on the other side of the tunnel is still active, then the number of seconds between DPD transmissions. If the router doesn't get a response, it terminates the IPSec tunnel connection. The router will attempt to re-establish the connection, so the user does not have to manually connect the VPN again.

PPTP

Point-to-Point Tunneling Protocol (PPTP) is an older VPN type that does not require encryption or authentication.

Caution: PPTP tunnels are not secure. If possible, use OpenVPN or IPsec tunnels.

If using a PPTP tunnel, set the **IP range** for the tunnel to use, click **Apply**, then click the **Add New Tunnel** button to create a new PPTP tunnel.

To configure a PPTP tunnel, you must create the following:

- **Name** — Accepts alphanumeric characters (a - z and A - Z), spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Username** — alphanumeric characters (a - z and A - Z), spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Password** — Must be between 8-63 characters and accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

For more information on configuring PPTP tunnels on your computer, read our Tech Community article.

IPv6

The Araknis router can handle IPv6 in one of two ways:

- **Dual-Stack IP (IPv4 and IPv6)** is 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 by encapsulating the IPv6 packets into IPv4 packets, and the opposite way (IPv4 packets encapsulated in IPv6 packets).

IP Mode	
Dual-Stack IP (IPv4 and IPv6)	🟢
IPv6 to IPv4 Tunnel	⚪

Dual-Stack IP (IPv4 and IPv6) Settings

LAN Settings

- **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.

- **IPv6 Range** — Enter a starting and ending IPv6 address for the DHCP server address range.

- **DNS 1 and DNS 2** — Enter the primary and secondary IPv6 DNS addresses.

- **Client Lease Time** — Enter the number of minutes that a DHCP lease lasts.

WAN Settings

The options change based on the selected **WAN IP Mode**.

DHCP WAN IP Mode

- **Static DNS —** Enable to enter specific DNS servers. You must enter the IPv6 addresses for the DNS servers.

- **Auto MTU —** Leave this enabled for optimal performance. The MTU (Maximum Transmission Unit) specifies the largest packet or frame allowed to be transmitted across the WAN interface.

Static IP WAN IP Mode

- **WAN IP Address** — Enter the IPv6 address to act as the root of the IPv6 WAN.

- **Prefix Length** — Acts as the IPv6 subnet mask for the LAN. This IPv6 setting is executed by specifying the number of bits used for the mask (rather than using IP notation as in IPv4).

- **Default Gateway Address** — Enter the IPv6 address for the router to use.

- **DNS Servers 1 and 2** — Enable to enter specific DNS servers. You must enter the IPv6 addresses for the DNS servers.

- **Auto MTU —** Leave this enabled for optimal performance. The MTU (Maximum Transmission Unit) specifies the largest packet or frame allowed to be transmitted across the WAN interface.
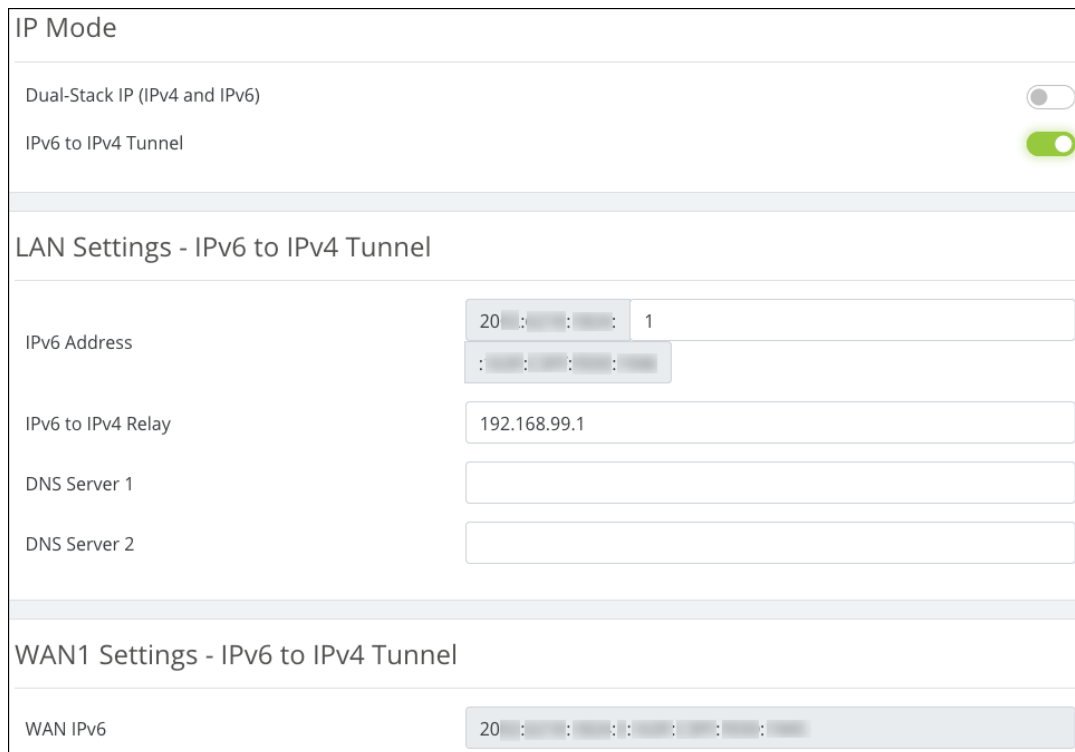
PPoE WAN IP Mode

Using IPv6 for PPPoE is like IPv4 in that the WAN connection is authenticated using encapsulated Point-to-Point Protocol (PPP) frames.

The password has a maximum character limit of 63 and accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

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

snap one

IPv6 to IPv4 Tunnel Settings

IP Mode

Dual-Stack IP (IPv4 and IPv6)	⬜
IPv6 to IPv4 Tunnel	🟢

LAN Settings - IPv6 to IPv4 Tunnel

IPv6 Address	20■ : ■ : ■ : 1 ┃ ■ : ■ : ■ : ■
IPv6 to IPv4 Relay	192.168.99.1
DNS Server 1	
DNS Server 2	

WAN1 Settings - IPv6 to IPv4 Tunnel

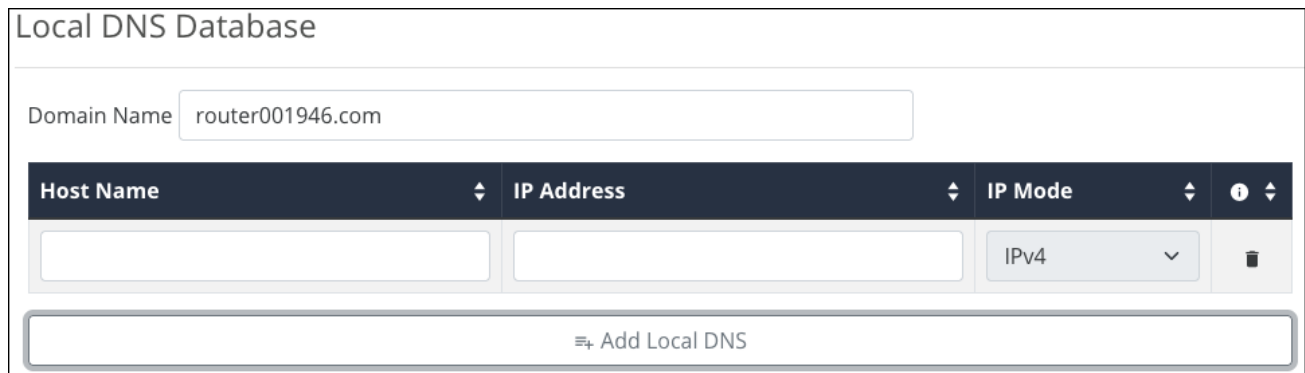|	
WAN IPv6	20■ : ■ : ■ : : ■ : ■ : ■

- **IPv6 Address** — An IPv6 address for the tunnel. This field is automatically generated but can be edited.

- **IPv6 to IPv4 Relay** — An IPv4 address for the relay server running on the router.

- **DNS Servers 1 and 2** — Enter DNS server addresses for the IPv6 requests to resolve to.

- **WAN IPv6 Address** — The WAN port's IPv6 address. This field cannot be edited.

Local DNS

Local DNS creates a 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 to serve as the local DNS for your network. This field accepts up to 63 characters, including alphanumeric (a - z and A - Z) characters, hyphens (-), and underscores (_).

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, then select its IP mode. This field accepts up to 63 characters, including alphanumeric (a - z and A - Z) characters, hyphens (-), and underscores (_).

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

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)

SNMP

Network administrators use Simple Network Management Protocol (SNMP) to monitor the performance and settings of network devices. Configure SNMP to communicate with management on the network.

> **Note:**   SNMP communities should be managed on a network-wide basis and require coordinated settings for managers and agents on the network.

> **Pro Tip:**   Do not enable both SNMP v1/2 and SNMPv3 because SNMP3 is not backward compatible with v1 and 2. Consult the client device recommendations when choosing which SNMP version to use.

SNMP Settings

- **System Name** — This field is auto-generated but can be edited. This field accepts alphanumeric characters (a - z and A - Z), spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **System Contact** — Enter a contact name, email address, or phone number for who should be contacted for more information about the SNMP server. This field can be left blank. This field accepts alphanumeric characters (a - z and A - Z), spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **System Location** — Enter the location of the server, if desired. This field can be left blank. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **Enable SNMP v1/v2** — Enable to edit the following entries.

- **Get Community Name (public)** — Enter a name for the read-only community on the network.

- **Set Community Name (private)** — Enter a name for the read-write community on the network.

- **Trap Community Name** — Enter a name for the notifications generated by the community.

- **Send SNMP Trap to (for IPv4)** — Enter an IPv4 address to send all the Trap Community messages from the SNMP-capable devices on the network.

SNMPv3 Settings

Enable to configure an SNMPv3 server.

Click **Add User** to determine who has access and privileges to the SNMP traffic.

Enable ⇕	Username ⇕	Authentication Method ⇕	Authentication Password ⇕	Encryption Method ⇕	Encryption Password ⇕	Group Privilege ⇕	❶ ⇕
🟢		None ⌄		None ⌄		Read Only ⌄	🗑
⇛ Add User							

Click **Add User** once more, and enter a **Username**, **Authentication Method, Encryption Method**, and the **Privileges** they should have (Read Only or Read/Write). Then click **Apply**.

These fields have the following character limitations:

- **SNMPv3 Username** — Alphanumeric (a - z and A - Z) characters

- **SNMPv3 Auth Password** — Between 8-32 characters. Accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

- **SNMPv3 Encryption Password** — Between 8-32 characters. Accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Trap Receiver IP Address	
Trap Receiver User	No User ⌄

For the **Trap Receiver IP Address**, enter an IPv4 address to send all the Trap Community messages from all SNMP devices on the network.

The **Trap Receiver User** has access to the Trap Community messages.

ACLs

Access Command Lists (ACLs) are commonly used to block undesired port uses, like Remote Desktop (RDP). They can also be used to allow a printer across VLANs while restricting access to the rest of the VLAN or to restrict access to specific websites.

Service Management

The router comes with a list of common services, including the protocol(s) and port range they typically use. These services are selectable when creating ACL rules.

Service Names have a maximum of 32 characters and accept alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Service Management

Service Name	Protocol	Port			
All Traffic	TCP+UDP	1	-	65535	🗑
DNS	UDP	53	-	53	🗑
FTP	TCP	21	-	21	🗑
HTTP	TCP	80	-	80	🗑
HTTP Secondary	TCP	8080	-	8080	🗑

Click **Add Service** if you don't see the service you'd like to create an ACL for. Click the **trashcan** icon to delete a service from the table.

Access Control List Settings

Access Control List Settings

Priority	Enable	Name	Action	Service	Source	Destination	ⓘ
No data available in table							

≡₊ Add ACL

Click **Add ACL** to create a new rule and configure the below settings:

• **Enable** – Toggle the rule on or off.

• **Name** – Enter a name to identify the rule, with a maximum of 63 characters. This field accepts alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

• **Priority** – Select the priority of the rule. The rules are enforced in order, meaning Priority 1 takes precedence over all other rules (2, 3, 4, etc.).

• **Action** – Select whether the rule should **Permit** or **Deny** traffic.

• **Service** – Select a previously configured service from the Service Management table.

• **Log packets that match this rule** – Enable to record activity in the system log.

• **Incoming Interface** – Select a LAN or WAN port from the dropdown.

• **Outgoing Interface** – Select a LAN or WAN port from the dropdown.

• **Source** – Enter a **Single IP**, **IP Range**, or **MAC address** of the originating device(s).

• **Destination** – Enter a **Single IP** or **IP Range** of the receiving device(s).

• **Always Active** – Leave enabled if the rule should always be active. Toggle it off to create a schedule for the rule.

Enable	⬤
Name	
Priority	1
Action	Permit
Service	All Traffic
Log packets that match this rule	◯
Incoming Interface	LAN
Outgoing Interface	LAN
Source	Single IP
Source Single IP	0.0.0.0
Destination	Single IP
Destination Single IP	0.0.0.0
Always Active	⬤

Cancel   Apply

QoS

Quality of Service (QoS) is a protocol that optimizes traffic across the network by tagging packets and giving them priority based on policy. This is an advanced feature that rarely needs to be implemented except in large, congested networks that require prioritization of network services.

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

Caution: QoS can cause network performance and reliability issues when configured incorrectly.

snap one™

Click to **Enable QoS** and select a **Schedule**. Options include:

- **SP** – Strict Priority.

- **WFQ** – Weighted Fair Queuing. When selected, you must assign a **Weight** to each **Queue** number. The router calculates the **Percentage of Bandwidth** as you determine an appropriate weight value. The Queue runs from 0 (minimal) to 7 (very high). Weight runs from 0 (minimal) to 15 (very high).

QoS

Enable QoS		
Schedule	WFQ	

Queue	Weight	Percentage of Bandwidth
0	0	12.5%
1	0	12.5%
2	0	12.5%
3	0	12.5%
4	0	12.5%
5	0	12.5%
6	0	12.5%
7	0	12.5%

CoS to DSCP Mapping

Class of Service (CoS) monitors the types of traffic on a network and assigns priority based on that.

Use this table to map CoS values to Differentiated Services Code Pointes (DSCP) values and ranges and an associated Queue.

Click the **DSCP Legend** button for a reference of policy classifications for implementation on the network.

The **Name** field has a maximum of 63 characters and accepts alphanumeric characters (a – z and A – Z), spaces, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

CoS to DSCP Mapping

Cos ⬍	Name ⬍	To DSCP ⬍	DSCP Range	⬍	Queue ⬍
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
7	Network Control	56	56	- 63	7

👁 DSCP Legend

snap one™

Bandwidth Control

Bandwidth Control allows you to manage WAN interface bandwidth for specific network clients based on their IP addresses, using upstream or downstream traffic limits.

Rules can be "stacked" to further segment the use of bandwidth.

Caution: Bandwidth control can cause network performance and reliability issues when configured incorrectly.

Bandwidth Control	
Enable Bandwidth Control	🟢

Enable Bandwidth Control to configure rules and apply them. Disable the feature to turn off all the configured rules.

Before You Begin

- Calculate the bandwidth requirements for all Bandwidth Control rules and make sure that the remaining bandwidth is sufficient for unregulated clients.

- Reserve no more than 80% of the available bandwidth from the ISP in the rules you create. This guarantees available bandwidth for the IP addresses not included.

Service Management

The Service Management table shows commonly used services, their protocol(s), and port range. These services are selectable when creating Bandwidth Control rules.

Click **Add Service**, at the bottom of the table, to add more services. **Service Names** have a maximum of 32 characters and accept alphanumeric (a - z and A - Z) characters, hyphens (-), underscores (_), !, @, #, $, %, ^, &, *, (,), ?, +, and periods.

Click the **trashcan** icon to delete a service.

Bandwidth Control Settings

Click **Add Bandwidth Settings** to create a new rule.

- **Interface** – Select a WAN port to apply the rule to.

- **Service** – Select one of the previously configured services from the Service Table.

- **IP Range** – Enter the IP address range to apply the rule to.

- **Direction** – Select whether the rule affects upstream or downstream traffic.

- **Bandwidth (kbit/s)** – The number of kilobits per second to allot for the bandwidth rule.

- **Bandwidth Sharing** – Select **Sharing total bandwidth for all IP's** to split the specified bandwidth among the clients, or **Assign for each IP** to allow the full specified bandwidth for each IP address.

- **Enable** – Toggle the rule on or off.

Click the **trashcan** icon to delete a rule.

Example configuration

You have a client with a guest network, but they do not want guests using all their bandwidth downloading movies or games. Bandwidth control can be used to limit the amount of bandwidth the guest network can use.

The configuration above has the IP Range of the Guest network entered and the Service is set to **All Traffic**. The **Direction** is set to **Both**, and the **Bandwidth** has been set to **30,000kbits**. Enough for a few guests to stream content and browse the internet.

Bandwidth Sharing is set to **Sharing total bandwidth for all IPs** so that each guest is not allotted the full 30,000kbits.

System Log

Use the system log page to view and download events recorded by the router. The filter at the top of the page allows you to set the number of events listed per page.

Buttons to select a page, **Download** or **Clear** the logs are at the bottom of the list.

System Log

View [50 ⌄] per page

Date ⬍	Status/Description ⬍
02/13/2023 06:46 PM	HTTPS Encrypted authentication success for user: araknis 192.168.
02/13/2023 06:33 PM	HTTPS Encrypted authentication success for user: araknis 192.168.
02/13/2023 06:29 PM	(DHCP) DHCPACK (br-vlan1): 192.168.1. 00:0F
02/13/2023 06:29 PM	(DHCP) DHCPREQUEST (br-vlan1): 192.168.1. 00:0F:
02/13/2023 06:22 PM	(DHCP) DHCPACK (br-vlan1): 192.168.1. 7C:BB:
02/13/2023 06:22 PM	(DHCP) DHCPREQUEST (br-vlan1): 192.168.1. 7C:BB:
02/13/2023 06:09 PM	HTTPS Encrypted authentication success for user: araknis 192.168.1.

Technical Support

For chat and telephone, visit **snp1.co/techsupport** • Email: **TechSupport@SnapOne.com**. Visit **snp1.co/tc** for discussions, instructional videos, news, and more.

Warranty and Legal Notices

Find details of the product's Limited Warranty and other resources such as regulatory notices and patent and safety information, at **snapone.com/legal** or request a paper copy from Customer Service at **866.424.4489**.

230615

200-AN-220-RT_QSG200-AN-520-RT_QSG-A