antaira®

making connectivity simple...

Wireless Router Software User's Manual

Version 1.1.3

(October 2023)

Firmware: Antaira r53423 (08/24/23)

Trademark Information

Antaira is a registered trademark of Antaira Technologies, LLC., Microsoft Windows and the Windows logo are the trademarks of Microsoft Corp. All other brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Antaira Technologies, LLC. provides this manual without warranty of any kind, expressed or implied, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Antaira Technologies, LLC. may make improvements and/or changes to the product and/or specifications of the product described in this manual, without prior notice. Antaira Technologies, LLC. will not be liable for any technical inaccuracies or typographical errors found in this guide. Changes are periodically made to the information contained herein and will be incorporated into later versions of the manual. The information contained is subject to change without prior notice.

FCC Notice

This equipment has been tested and found to comply with the limits for a Class-A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy. It may cause harmful interference to radio communications if the equipment is not installed and used in accordance with the instructions. 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 or more 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.

Caution: Any changes or modifications not expressly approved by the grantee of this device could void the user's authority to operate the equipment.

CE Mark 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.

Industrial Ethernet Wireless APs

Software User Manual

This manual supports the following models

- ARS-7235-AC(-T)
- ARS-7235-PD-AC(-T)
- ARS-7235-PSE-AC(-T)
- ARS-7235-5E-AC(-T)
- ARX-7235-AC-PD-T
- ARY-7235-AC-PD
- ARS-7131(-T)
- ARS-7131-AC(-T)
- ARS-7231-AC(-T)

Please check our website (www.antaira.com) for any updated manual or contact us by e-mail (support@antaira.com).

Table of Contents

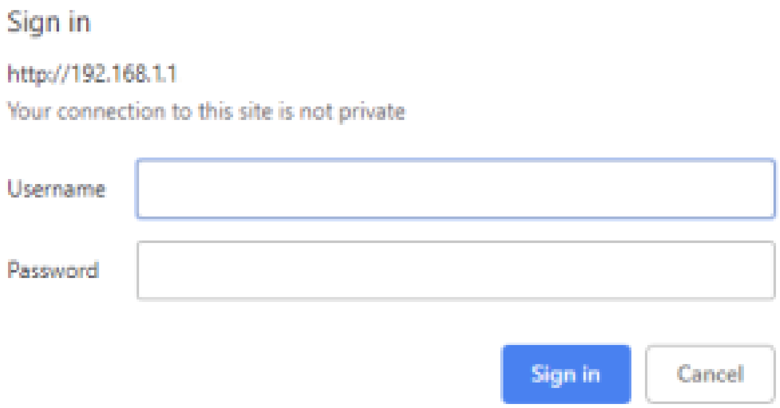
1 Access with Web Browser

1.1 Web GUI Login

All of Antaira's industrial managed devices are embedded with HTML web GUI interfaces. They provide user-friendly management features through its design and allows users to manage the devices from anywhere on the network through a web browser.

Step 1: To access the WEB GUI, open a web browser and type the following IP address: http://192.168.1.1

Step 2: The default WEB GUI login:
Username: root
Password: admin



Sign in

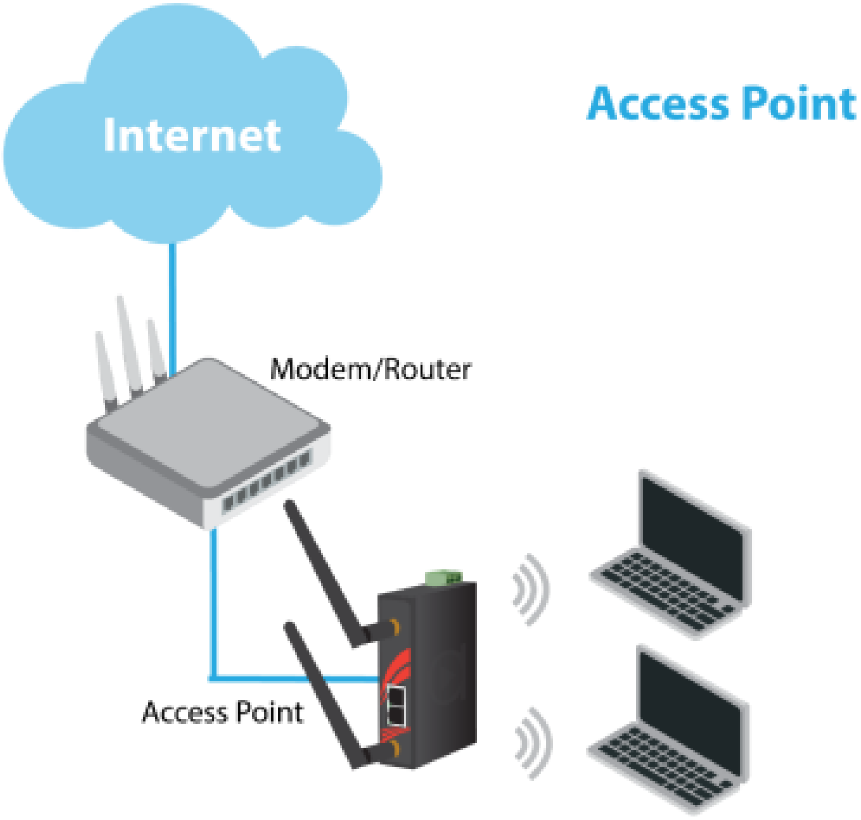
http://192.168.1.1

Your connection to this site is not private

1.2 Operation Modes

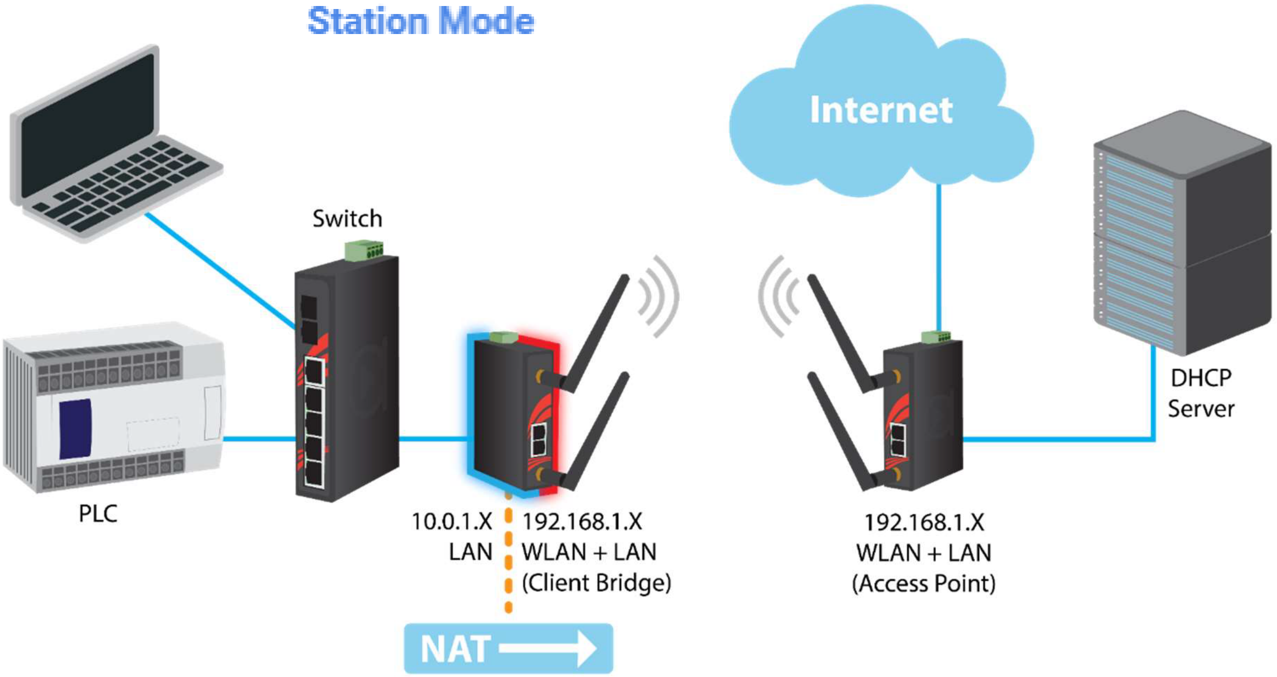
1.2.1 Access Point

The access point mode allows Wi-Fi devices to connect to a wired network. In this mode, multiple wireless devices can be supported on a single wired local area network. In the example below, Internet is provided via the Modem/Router. The Access Point is connected directly to the Modem/Router by an Ethernet cable. Multiple devices can then connect to the access point's Wi-Fi and access the Internet



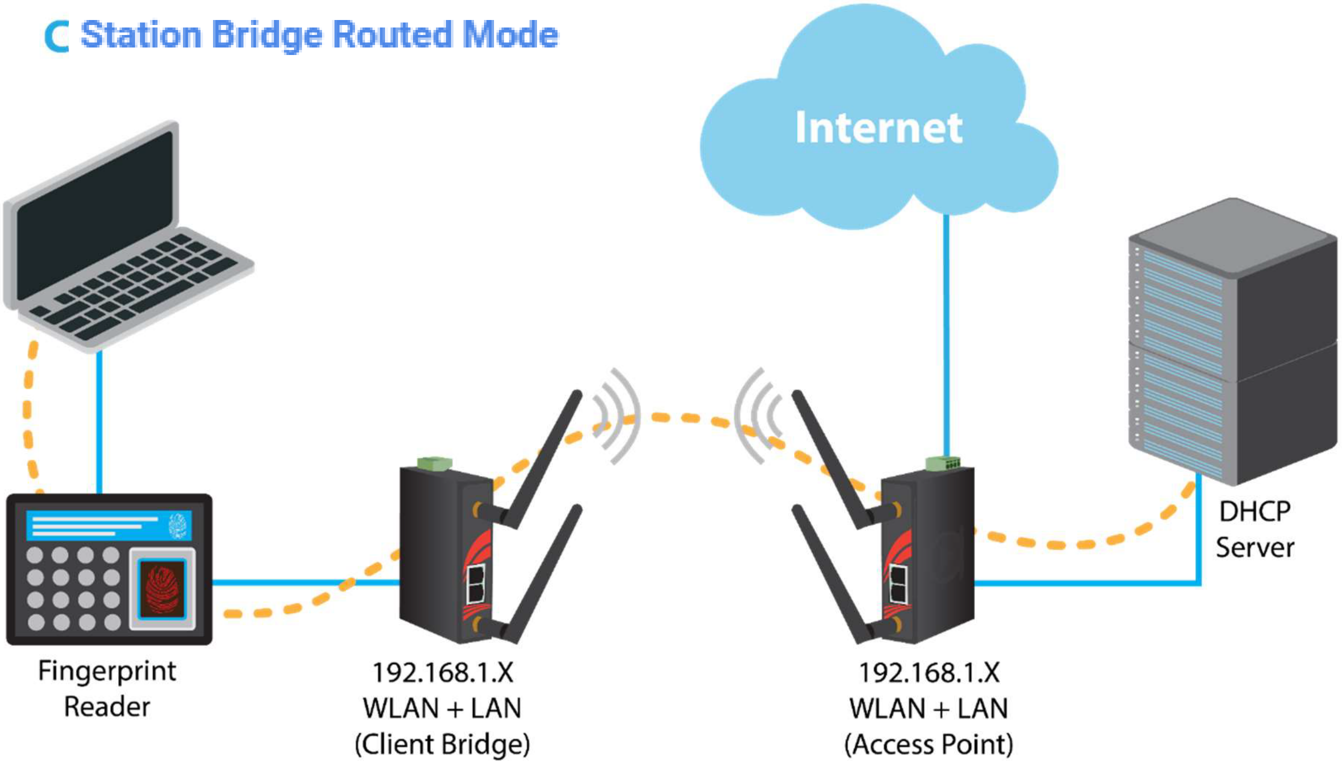
1.2.2 Station Mode

Station mode allows the router to connect to other access points as a client. This turns the Wireless Local Area Network (WLAN) portion of your router into the Wide Area Network (WAN). In this mode, the router will no longer function as an access point (does not allow clients), therefore, you will need to be wired to make configurations. In client mode, the WLAN and the LAN will not be bridged, allowing two different subnets. Port forwarding (From the WLAN to the LAN) will be necessary for FTP servers, VNC servers, etc that are located behind the client mode router. For this reason, most users choose to use Client Bridge Mode instead.



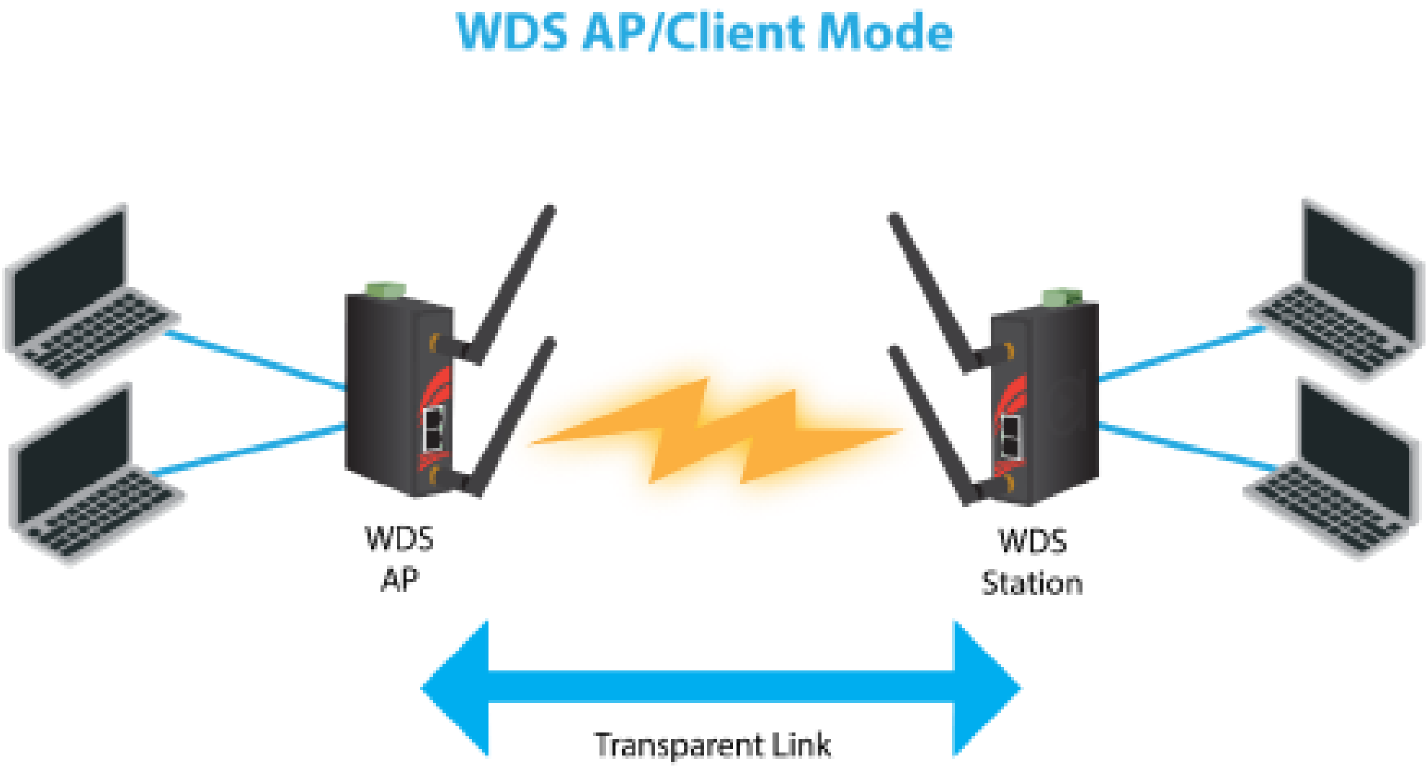
1.2.3 Station Bridge Routed Mode

In Station Bridge Routed Mode the radio interface is used to connect the LAN side of the router to a remote access point. The LAN and the remote AP will be in the same subnet (This is called a "bridge" between two network segments). The WAN side of the router is unused and can be disabled. Use this mode, e.g., to make the router act as a "WLAN adapter" for a device connected to one of the LAN Ethernet ports.



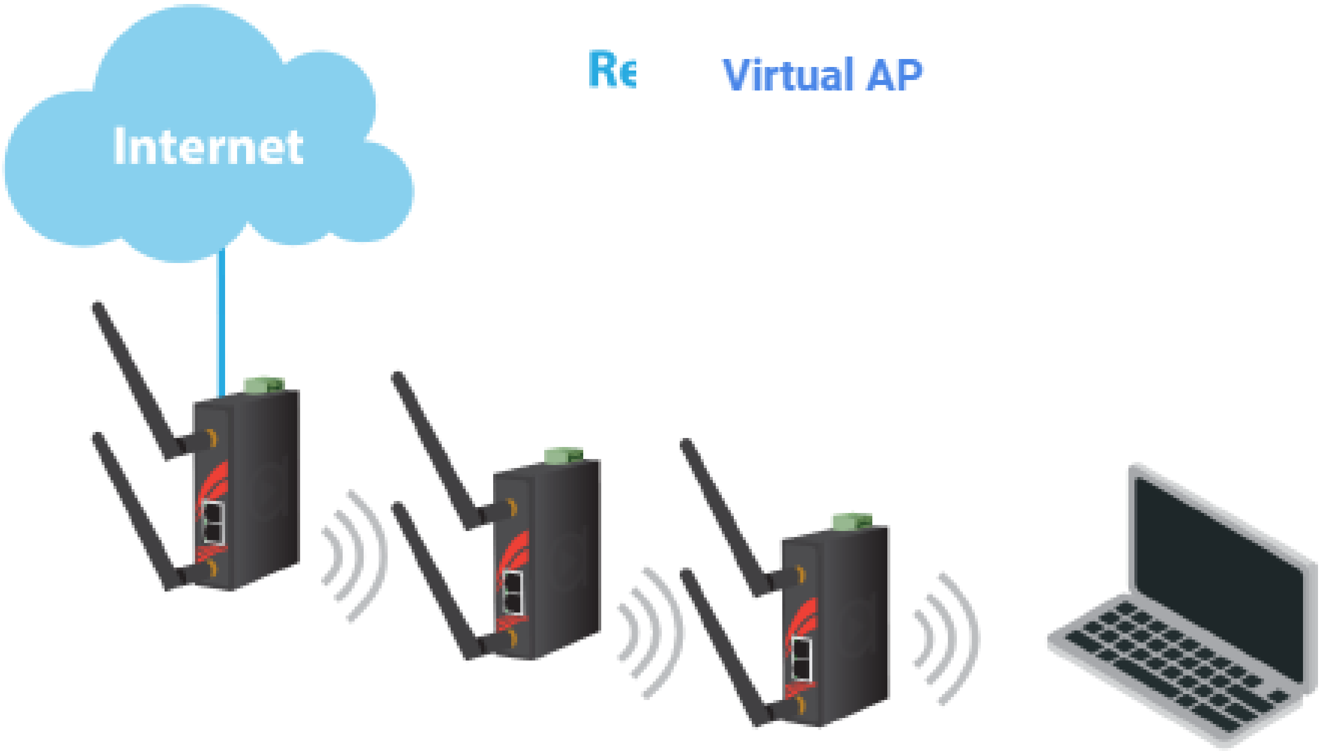
1.2.4 WDS Station/WDS Mikrotik Point

In a typical Access Point to Station/Client connection, whenever traffic is passed through the AP, the MAC address of the client packet changes to the MAC address of the AP. This can add overhead and latency. A Wireless Distribution System (WDS) allows one or more access points to connect wirelessly and share internet access across. WDS also preserves the MAC addresses of client frames across links between the WDS AP to WDS Stations, reducing the latency caused in typical wireless setups. WDS Stations can only be paired with WDS AP.



1.2.5 Virtual Interfaces AP Mode

In Virtual Interfaces AP Mode, the access point will act as a relay for another wireless signal. Repeater Mode takes an existing signal from a wireless AP or wireless router and rebroadcasts it. This mode is beneficial for extending the wireless range and coverage. The drawback is that the re-transmitted signal throughput is halved for every repeater used.

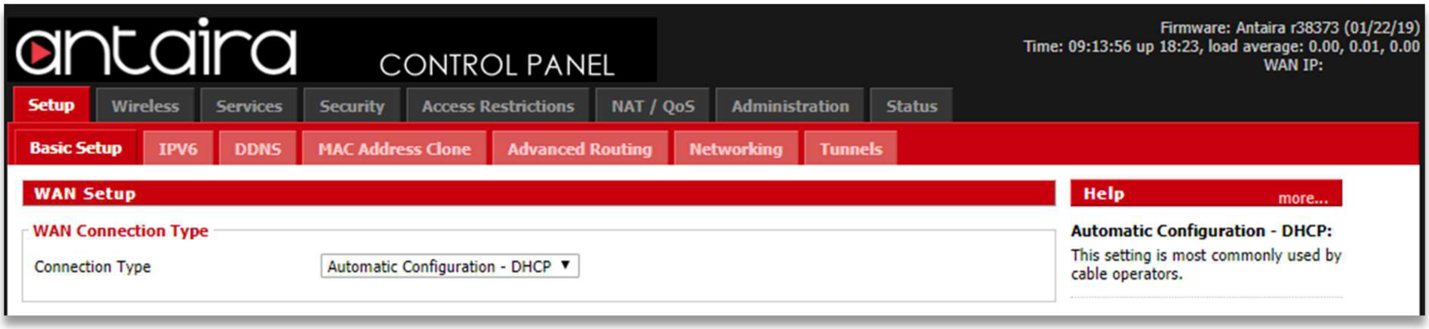


2 Setup

2.1 Basic Setup

The Setup Screen is the first screen you will see when accessing the router. After you have configured and made changes to these settings, it is recommended to set a new password for the router. This will increase security by protecting the router from unauthorized changes. All users who try to access the router's web interface will be prompted for the router's password.

Setup > Basic Setup



Firmware: Antaira r38373 (01/22/19)
Time: 09:13:56 up 18:23, load average: 0.00, 0.01, 0.00
WAN IP:

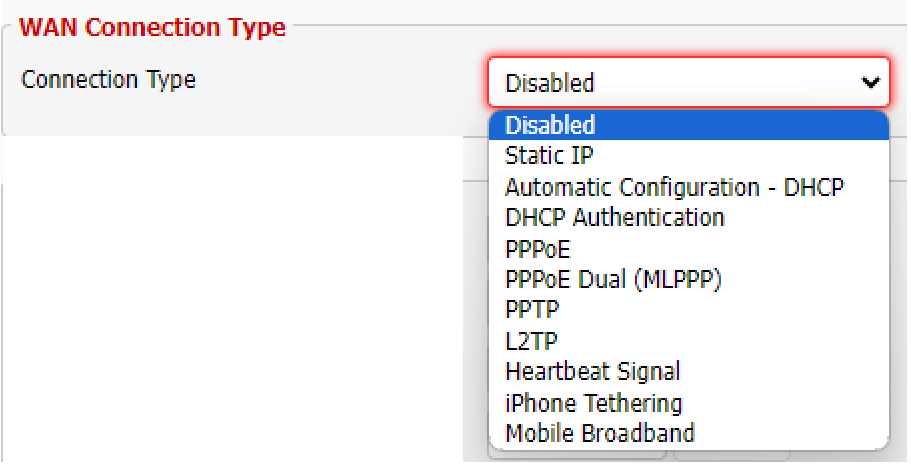
WAN Setup

WAN Connection Type

Connection Type: Automatic Configuration - DHCP

Automatic Configuration - DHCP:
This setting is most commonly used by cable operators.

2.1.1 WAN Setup



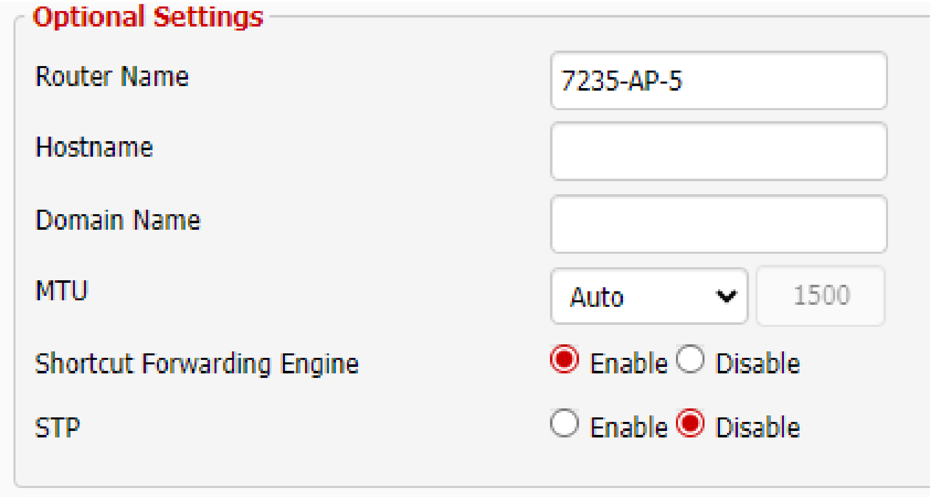
WAN Connection Type

Connection Type: Disabled

WAN Connection Type	Description
Disabled	Disable the WAN port.
Static IP	A static IP address is used. **Required:** IP address, subnet mask, gateway, and server to be entered manually.
Automatic Configuration - DHCP	The WAN port will obtain its IP address from a DHCP server.
PPPoE	Configure as PPPoE Client. **Required:** Username and Password. **Advanced Options:** Service Name, T-Online VLAN 7 Support, PPP Compression, MPPE Encryption, Single Line Multi Link, and Connection Strategy.
PPPoE Dual	Allows users to set multiple paths of the WAN.
PPTP	Establishes a connection via PPTP. **Required:** Gateway, Username, Password, and encryption information.
L2TP	Establishes a connection via L2TP. Required: Gateway, Username, Password, and encryption information.
HeartBeat Signal	Short frames sent by the wireless device that contains information, such as the SSID, encryption information, data rates, and other information. This information is only used if the IPS supports heartbeat signals.
IPhone Tethering	Establishes a connection via IPhone tethering.
Mobile Broadband	Establishes a connection via mobile broadband.

2.1.2 Optional Settings

Setup > Basic Setup > Optional Settings



Optional Settings

Router Name 7235-AP-5

Hostname

Domain Name

MTU Auto 1500

Shortcut Forwarding Engine ● Enable ○ Disable

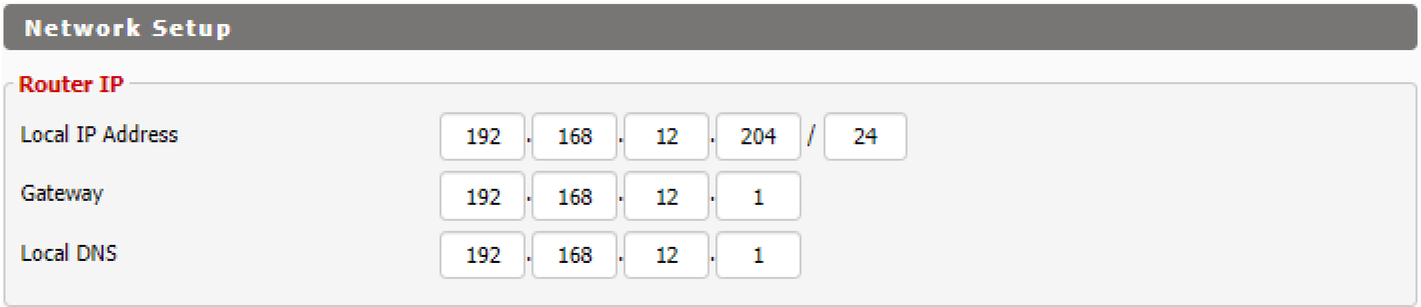
STP ○ Enable ● Disable

Optional Settings	Description
Router Name	The desired name to appear for the router.
Hostname	Necessary for some ISPs and can be provided by the ISP.
Domain Name	Necessary for some ISPs and can be provided by the ISP.
MTU	Maximum Transmission Unit: Specifies the largest packet size permitted for Internet transmission. Auto will allow the device to select the best MTU for Internet connection. Manual values entered should be in the range 1200 – 1500.
Shortcut Forwarding Engine	Enable or disable this feature.
STP	Spanning Tree Protocol: Creates the best path between devices without creating loops.

2.1.3 Router IP

Enter the desired LAN side IP address, Subnet mask, Gateway, and Local DNS information.

Setup > Basic Setup > Network Setup



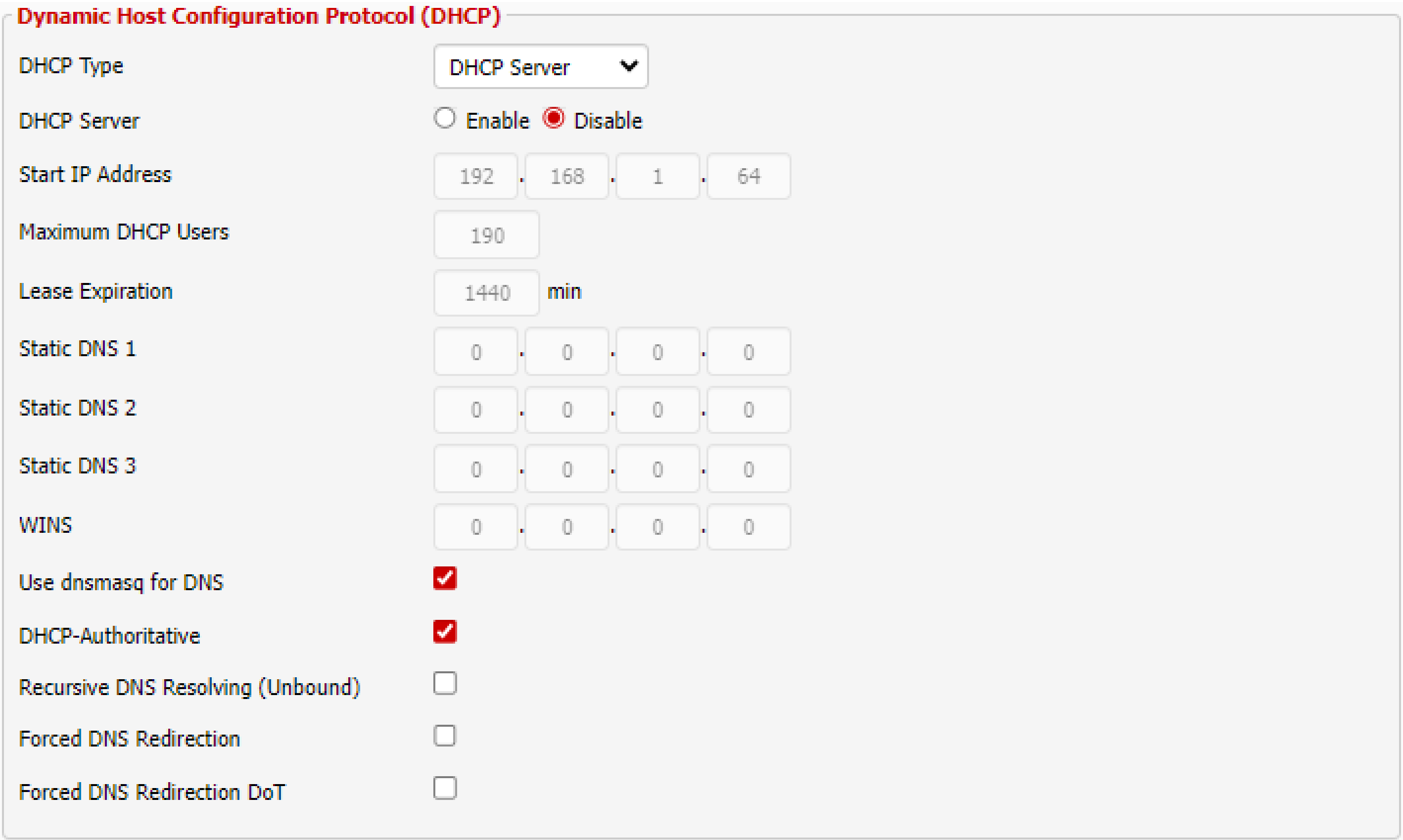
Network Setup

Router IP

Local IP Address	192 . 168 . 12 . 204 / 24
Gateway	192 . 168 . 12 . 1
Local DNS	192 . 168 . 12 . 1

2.1.4 Network Address Server Settings (DHCP)

Setup > Basic Setup > Network Address Server Settings



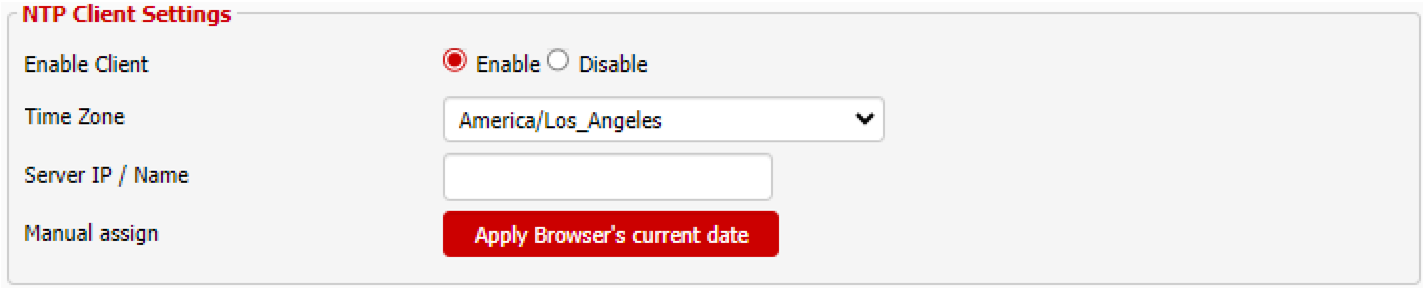
Dynamic Host Configuration Protocol (DHCP)

DHCP Type	DHCP Server
DHCP Server	○ Enable ● Disable
Start IP Address	192 . 168 . 1 . 64
Maximum DHCP Users	190
Lease Expiration	1440 min
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
WINS	0 . 0 . 0 . 0
Use dnsmasq for DNS	☑
DHCP-Authoritative	☑
Recursive DNS Resolving (Unbound)	□
Forced DNS Redirection	□
Forced DNS Redirection DoT	□

Network Address Server Settings	Description
DHCP Type	**Server:** This device will function as the DHCP server. If there is already a DHCP server on the network, select **Disable**. **Forwarder:** Additional routers can be hardwired to the main router on the network. The additional routers will have the type set as Forwarder. Any devices connected to the additional routers will receive their DHCP information from the main router.
DHCP Server	**Enable** if you want this router to provide DHCP addressing. Disable if there is an existing DHCP server on the network.
Start IP Address	A numerical value for the DHCP server to start its addressing with when assigning IP addresses. ****Do not start with the routers IP address. ****
Maximum DHCP Users	The maximum number of devices the router will assign IP address through DHCP.
Client Lease Time	The lease time of an IP address given by the DHCP server before it expires.
Static DNS #	The Domain Name System is how domain names are translated to IP addresses. The ISP provider will typically provide at least one unique DNS IP address.
WINS	Windows Internet Naming Services: Manages the PC's interaction with the internet.

2.1.5 Time Settings

Setup > Basic Setup > Time Settings



NTP Client Settings

Enable Client: ● Enable ○ Disable

Time Zone: America/Los_Angeles

Server IP / Name:

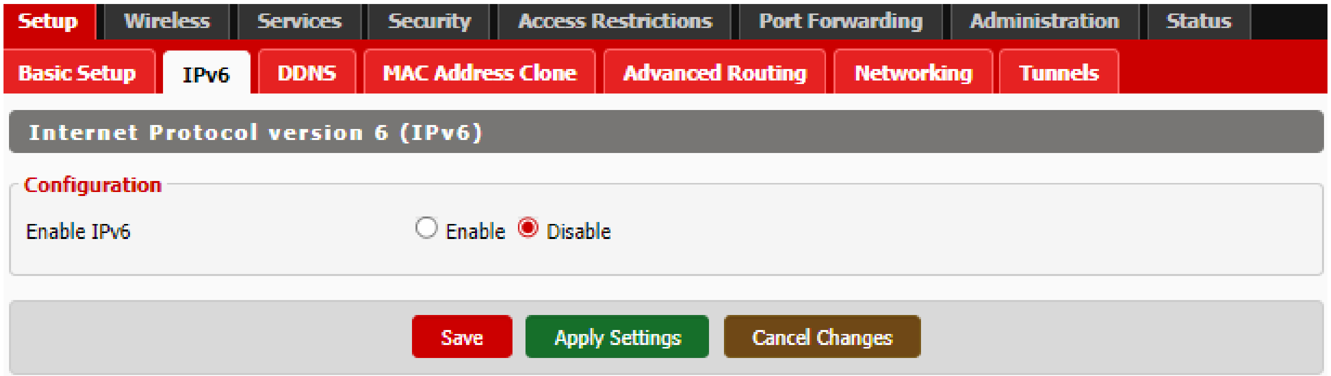
Manual assign

Time Settings	Description
NTP Client	Network Time Protocol: Used for time synchronization between the client and the network time server.
Time Zone	Select time zone for the unit.
Server IP/Name	Enter either the server's IP address or assigned domain name.
Manual Assign	Applies the browser's current date.

2.2 IPv6

Internet Protocol version 6 (IPv6) is a network layer IP standard used by electronic devices to exchange data across a packet switched network. It follows IPv4 as the second version of the Internet Protocol to be formally adopted for general use.

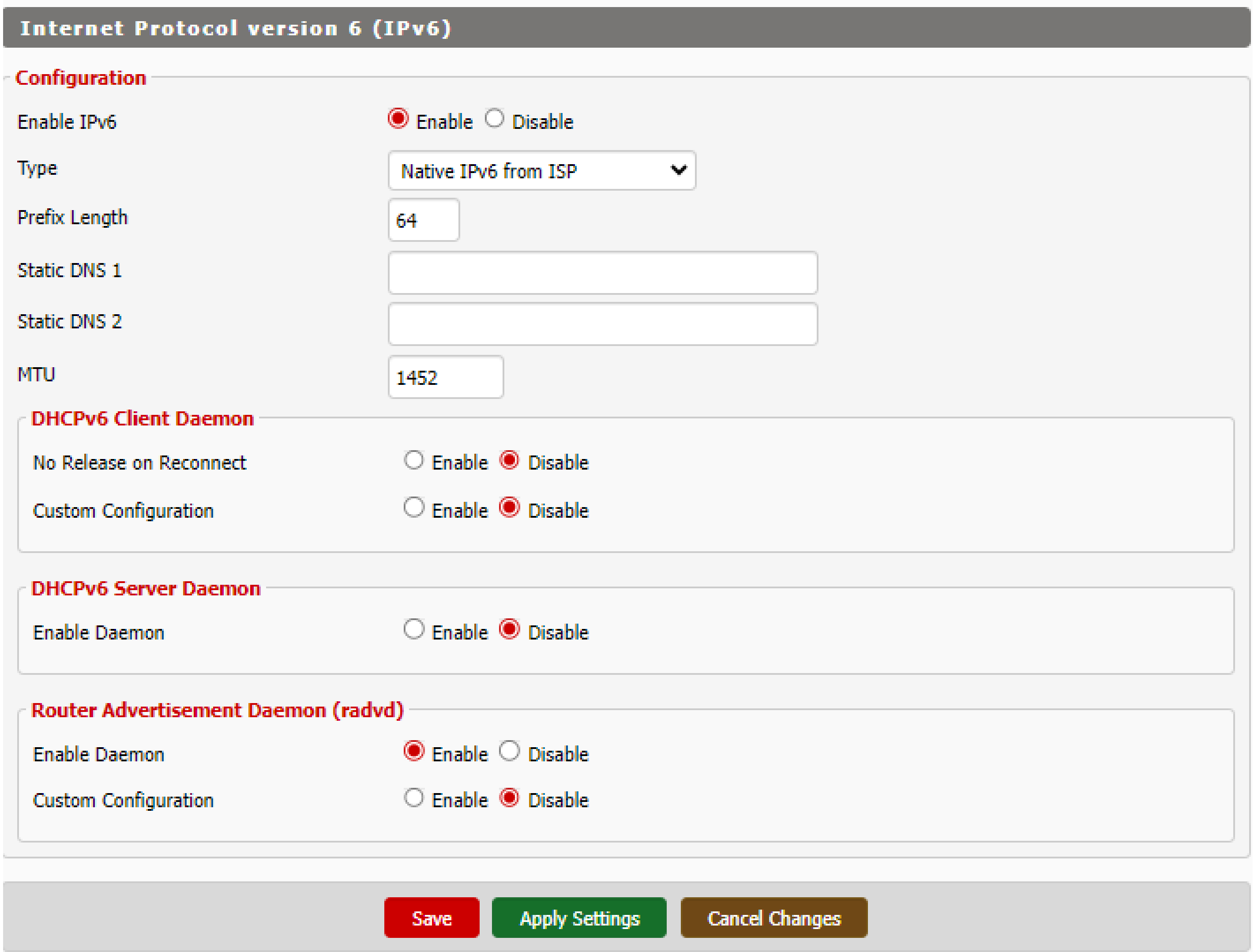
Setup > IPv6



Internet Protocol version 6 (IPv6)

Configuration

Enable IPv6: ○ Enable ● Disable



Internet Protocol version 6 (IPv6)

Configuration

Enable IPv6: ● Enable ○ Disable

Type: Native IPv6 from ISP

Prefix Length: 64

Static DNS 1:

Static DNS 2:

MTU: 1452

DHCPv6 Client Daemon

No Release on Reconnect: ○ Enable ● Disable

Custom Configuration: ○ Enable ● Disable

DHCPv6 Server Daemon

Enable Daemon: ○ Enable ● Disable

Router Advertisement Daemon (radvd)

Enable Daemon: ● Enable ○ Disable

Custom Configuration: ○ Enable ● Disable

IPv6	Description
IPv6	Enable or disable IPv6.
IPv6 Type	Select between *Native IPv6 from ISP*, *DHCPv6 with Prefix Delegation*, or *6in4 Static Tunnel*.
Prefix Length	Enter a prefix length.
Static DNS	Enter a static DNS if needed.

MTU	Maximum Transmission Unit: Specifies the largest packet size permitted for Internet transmission. Auto will allow the device to select the best MTU for Internet connection. Manual values entered should be in the range 1200 – 1500.

Dhcp6c custom	This option is used to request and configure IPv6 addresses and host network configuration information (e.g., DNS) for a network interface from the DHCPv6 server.
Dhcp6s	This option provides IPv6 addresses and prefix assignment administrative policy and configuration information for DHCPv6 clients.
Radvd	Linux IPv6 Router Advertisement Daemon
Radvd custom	Custom options for radvd configuration.

2.3 DDNS

The router offers a Dynamic Domain Name System (DDNS). The DDNS allows users to assign a fixed host and domain name to a dynamic internet IP address. This is useful when hosting a website or FTP server.

Setup > DDNS

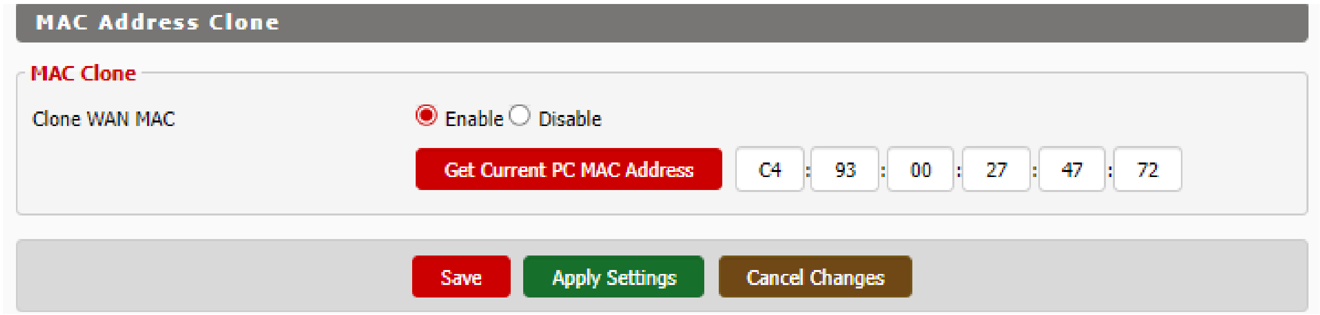
DDNS Settings	Description
DDNS Service	Sign up for a DDNS service through a DDNS service provider.
Username	Setup a Username through the DDNS service provider.
Password	Setup a Password through the DDNS service provider.
Hostname	Setup a Hostname through the DDNS service provider.
Type	**Dynamic:** Allows a hostname (chosen by the user through the DDNS service provider) to point to the users IP address.
	Static: Like Dynamic service, but the DNS host will not expire after 35 days without updates.

	Custom: Creates a managed primary DNS that provides the user more control over the DNS.
Wildcard	Enabling the Wildcard feature allows the user's host to be aliased to the same IP address and the DNS server.
External IP Check	Allows the DDNS function to pick up the WAN IP from the router instead of checking on an external site.
Force Update Interval	The number represents how often (in days) an update will be performed.

2.4 MAC Address Clone

By enabling the MAC address clone, the user is able to clone the MAC address of the network adapter onto the router.

Setup > MAC Address Clone



MAC Address Clone

MAC Clone

Clone WAN MAC ● Enable ○ Disable

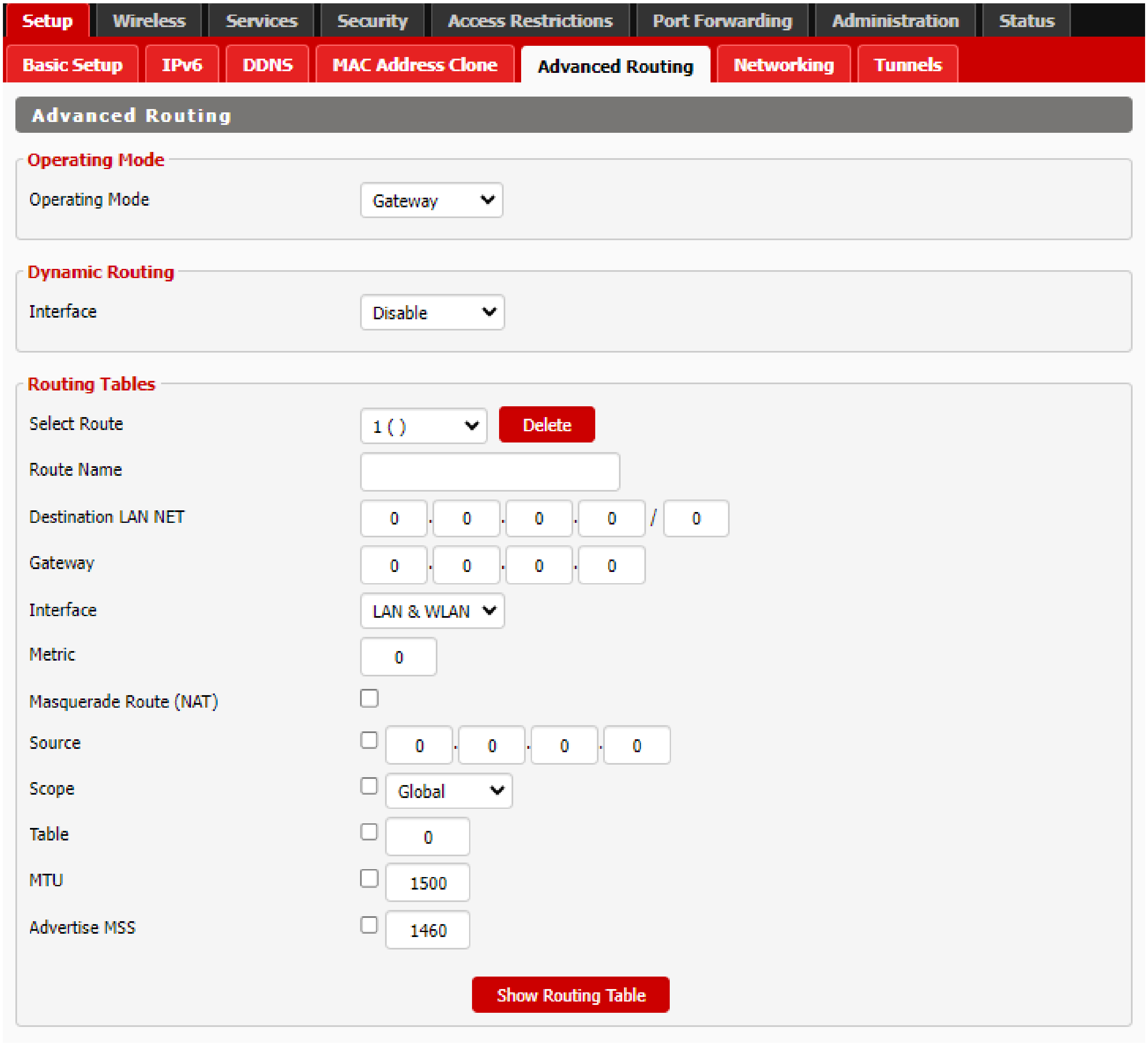
C4 : 93 : 00 : 27 : 47 : 72

Enter the MAC address of the network adapter in the **Clone WAN MAC** section or click the **Get Current PC MAC Address** to fill in the MAC address of the PC currently connected. Get Current PC Mac is typically used when establishing a service with certain ISP providers.

2.5 Advanced Routing

On the Advanced Routing screen, you can set the routing mode and settings of the router. Choose the appropriate working mode for you needs. Generally, if the router is hosting your network's connection to the Internet, use **Gateway** mode. In Gateway mode, the router performs NAT, while in other modes it does not.

Setup > Advanced Routing



Advanced Routing

Operating Mode

Operating Mode: Gateway

Dynamic Routing

Interface: Disable

Routing Tables

Select Route	1 ( ) Delete
Route Name	
Destination LAN NET	0 . 0 . 0 . 0 / 0
Gateway	0 . 0 . 0 . 0
Interface	LAN & WLAN
Metric	0
Masquerade Route (NAT)	□
Source	□ 0 . 0 . 0 . 0
Scope	□ Global
Table	□ 0
MTU	□ 1500
Advertise MSS	□ 1460

Show Routing Table

2.5.1 Gateway

In the Gateway operating mode, the router will route packets between the LAN/WLAN and the Internet (through the WAN port). This is the default setting and most common when the router is hosting the network’s Internet connection through the WAN port.

Setup > Advanced Routing > Operating Mode > Gateway

Gateway	Description
Operating Mode	**Gateway:** If the router is hosting the Internet connection, the router will perform NAT in Gateway mode.
	BGP: Boarder Gateway Protocol.
	RIP2 Router: Routing Information Protocol.
	OSPF Router: Open Shortest Path First.
	OSPF & RIP2 Router: Uses a combination of RIP and OSPF.
	OLSR Router: Optimized Link State Routing Protocol.
	Router: Static routes.
Dynamic Routing – Interface	Tells the end user if the destination IP address is on the LAN & WAN, WAN or Loopback.
Select Set Number	A unique router number. You can set up to 50 routes.
Route Name	The name assigned to a specific route number.
Metric	Enter a metric number.
Masquerade Route (NAT)	Enable or disable masquerading (NAT).
Destination LAN Net	The remote host assigned to the static route.
Subnet Mask	Enter a subnet mask.
Gateway	Enter a gateway IP address.
Interface	Select the interface that the static route will apply to.
Destination LAN NET	Network address of destination LAN.

Subnet Mask	Subnet mask of destination LAN.
Gateway	Gateway IP address.
Interface	Select the interface for the path of the route.

2.5.3 Router

Router Mode allows users to set static routes.

Setup > Advanced Routing > Operating Mode > Router

Router	Description
Select Set Number	This is the unique router number. You may set up to 50 routes.
Route Name	Enter the name you would like to assign to this route.
Metric	
Destination LAN NET	This is the remote host to which you would like to assign the static route.
Subnet Mask	Enter the subnet mask.
Gateway	Enter the gateway IP address.
Interface	Select the interface that the static route will apply to.

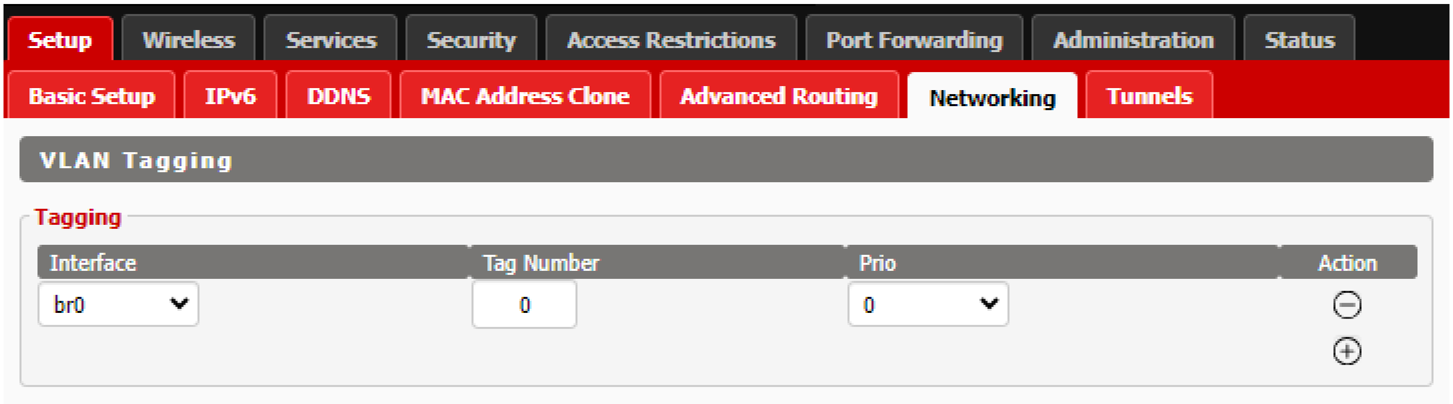
2.6 Networking

2.6.1 VLAN Tagging

VLAN Tagging allows the user to create new VLAN interfaces from the standard interfaces by filtering defined tag numbers.

Tagging: Allows you to create a new VLAN interface out of a standard interface by filtering the interface using a defined TAG number.

Setup > Networking > VLAN Tagging



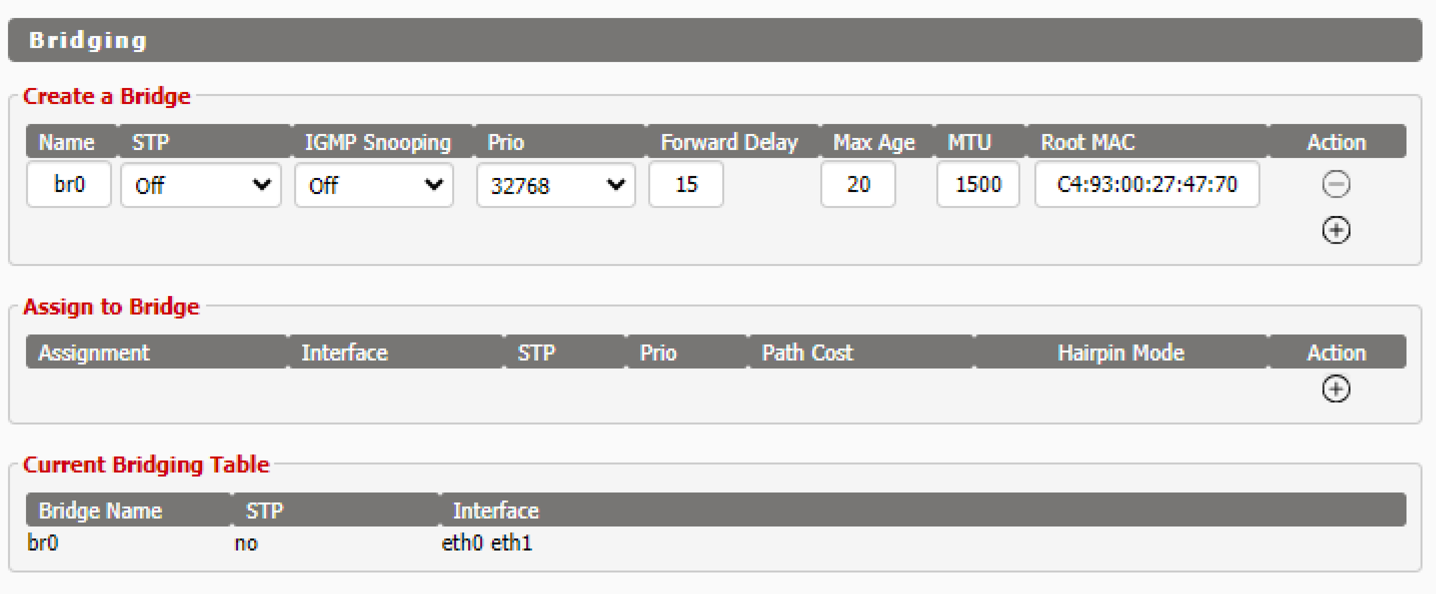
VLAN Tagging

Tagging

Interface	Tag Number	Prio	Action
br0	0	0	⊖ ⊕

2.6.2 Bridging

Setup > Networking > Bridging



Bridging

Create a Bridge

Name	STP	IGMP Snooping	Prio	Forward Delay	Max Age	MTU	Root MAC	Action
br0	Off	Off	32768	15	20	1500	C4:93:00:27:47:70	⊖ ⊕

Assign to Bridge

Assignment	Interface	STP	Prio	Path Cost	Hairpin Mode	Action
						⊕

Current Bridging Table

Bridge Name	STP	Interface
br0	no	eth0 eth1

Current Bridging Table: A table with all of the current bridges and their components can be seen it the Bridging section of the networking tab.

Create Bridge	Description
Add	Create a new network bridge.
STP	Spanning Tree Protocol. Turn on or off.
IGMP Snooping	Turn on or off IGMP Snooping.

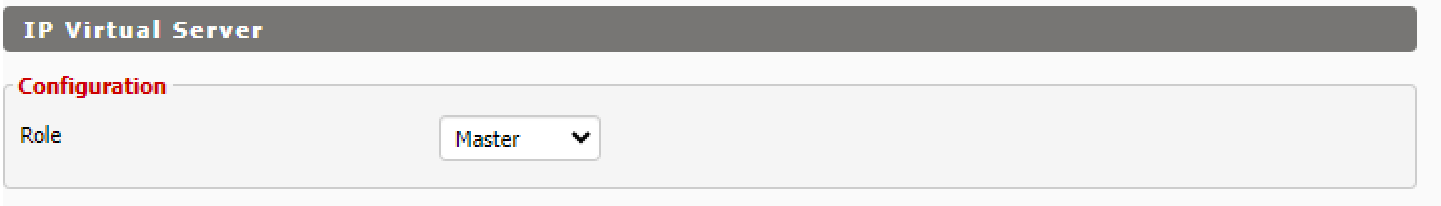
Prio	Sets the bridge priority order. (Lower numbers are higher priority.)
MTU	Maximum Transmission Unit: Specifies the largest packet size permitted for Internet transmission. Auto will allow the device to select the best MTU for Internet connection. Manual values entered should be in the range 1200 – 1500.
Root MAC	The Root MAC address.

Assign to Bridge: Allows a user to assign an interface to a network bridge.

Assign to Bridge	**Description**
Assignment	Assign any valid interface to a network bridge.
Interface	Select the interface to assign to the bridge.
STP	Spanning Tree Protocol. Turn on or off.
Priority	Sets the priority order (Lower numbers are higher priority).
Path Cost	Set the path cost.
Hairpin Mode	Enables Hairpin routing.

2.6.3 IP Virtual Server

Setup > Networking > IP Virtual Server



IP Virtual Server

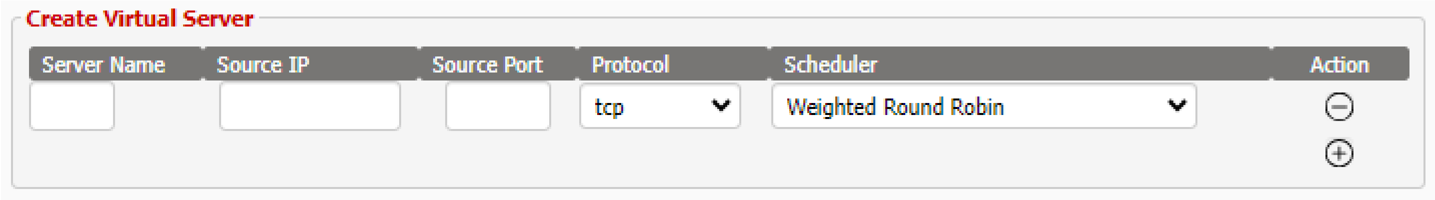
Configuration

Role: Master

Role	**Description**
Role	Select the role of the IP virtual server: Master or Backup.

2.6.4 Create Virtual Server

Setup > Networking > Create Virtual Server



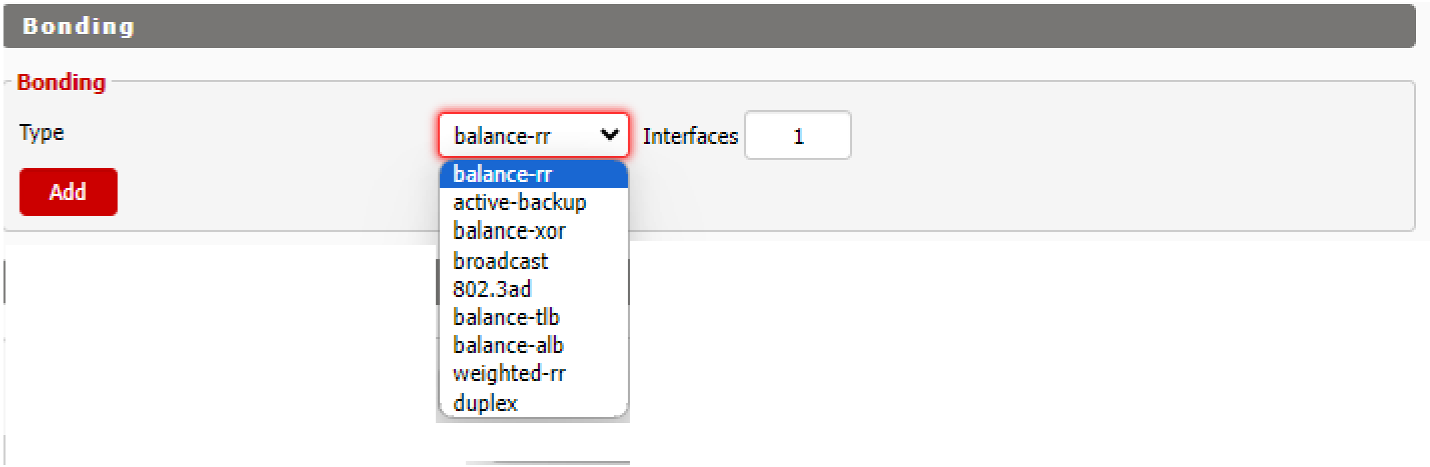
Create Virtual Server

Server Name	Source IP	Source Port	Protocol	Scheduler	Action
			tcp	Weighted Round Robin	⊖ ⊕

Create Virtual Server	Description
Server Name	Enter a server name.
Source IP	Enter a source IP address.
Source Port	Enter a source port.
Protocol	Choose between TCP, UDP, or SIP protocol.
Scheduler	Select the scheduler from the drop-down menu.

2.6.5 Bonding

Setup > Networking > Bonding



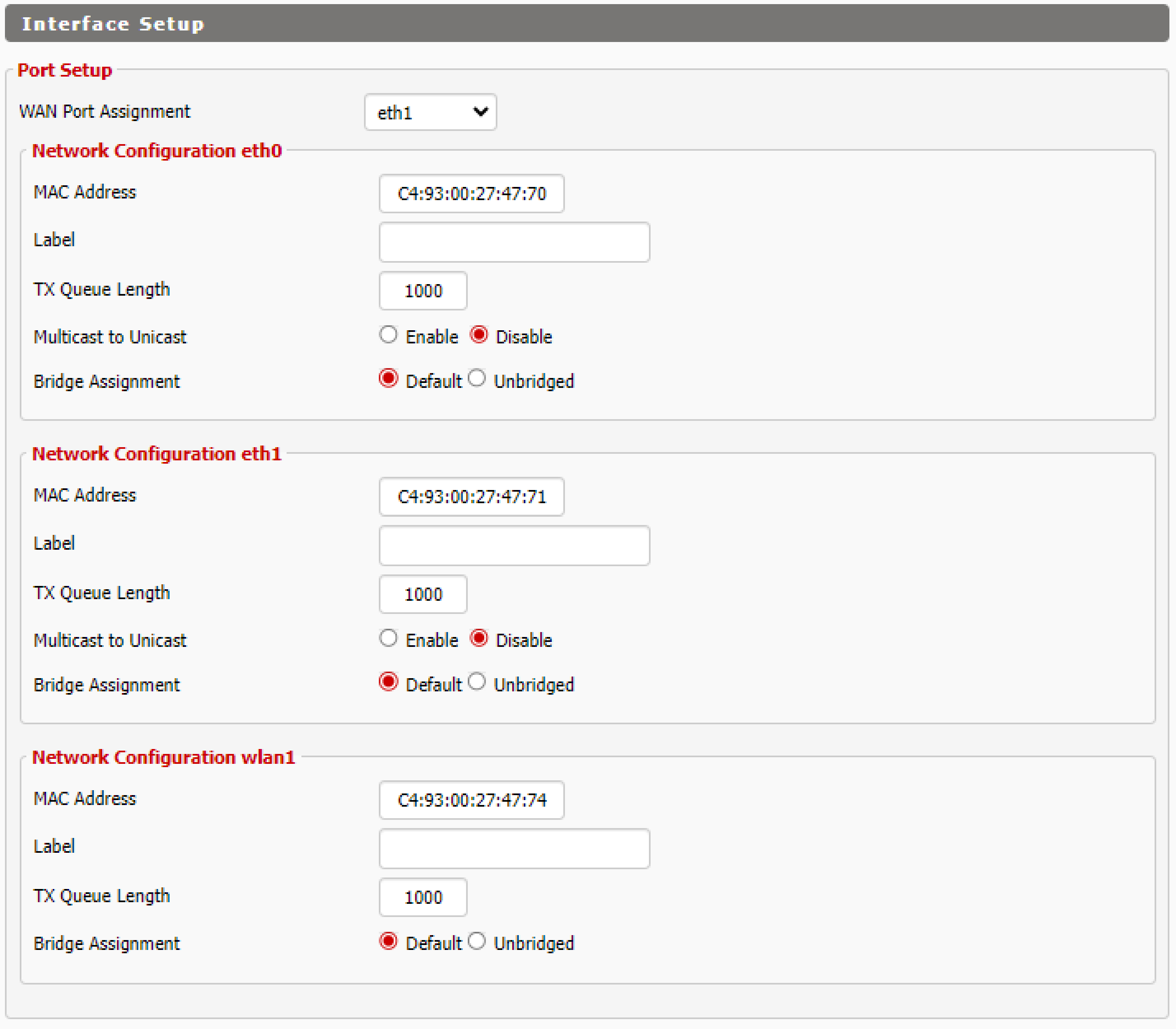
Bonding

Bonding

Type: balance-rr — Interfaces: 1

2.6.6 Port Setup

Setup > Networking > Port Setup



Interface Setup

Port Setup

WAN Port Assignment: eth1

Network Configuration eth0

MAC Address: C4:93:00:27:47:70

Label:

TX Queue Length: 1000

Multicast to Unicast: ○ Enable ● Disable

Bridge Assignment: ● Default ○ Unbridged

Network Configuration eth1

MAC Address: C4:93:00:27:47:71

Label:

TX Queue Length: 1000

Multicast to Unicast: ○ Enable ● Disable

Bridge Assignment: ● Default ○ Unbridged

Network Configuration wlan1

MAC Address: C4:93:00:27:47:74

Label:

TX Queue Length: 1000

Bridge Assignment: ● Default ○ Unbridged

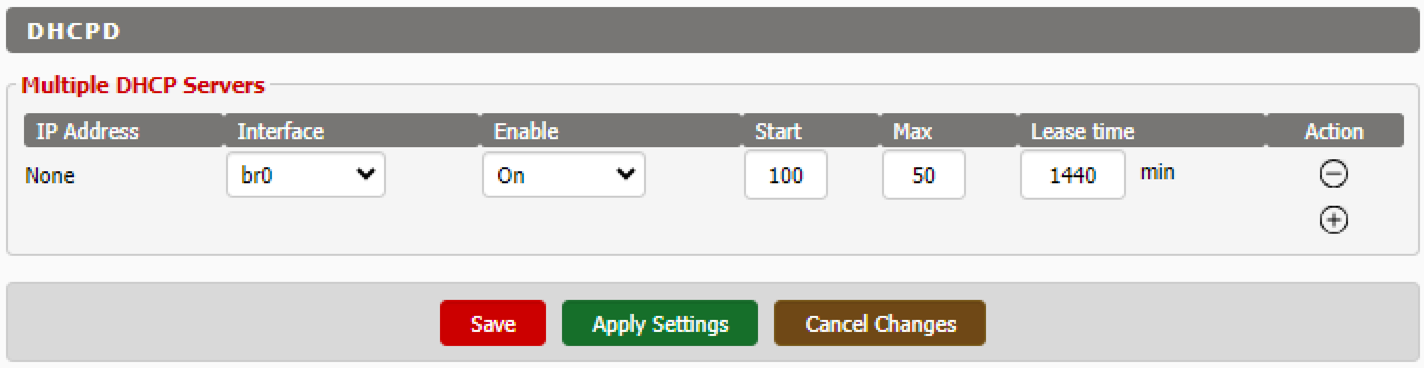
Port Setup	Description
WAN Port Assignment	Select a WAN Port.
MAC Address	MAC Address of the configured WAN port.

Label	Input a label if desired.
TX Queue Length	Set the TX-queue length.
Bridge Assignment	Select the bridge assignment: Unbridged or Default.

2.6.7 DHCPD

This feature allows you to configure a DHCP server on a specific port.

Setup > Networking > DHCPD



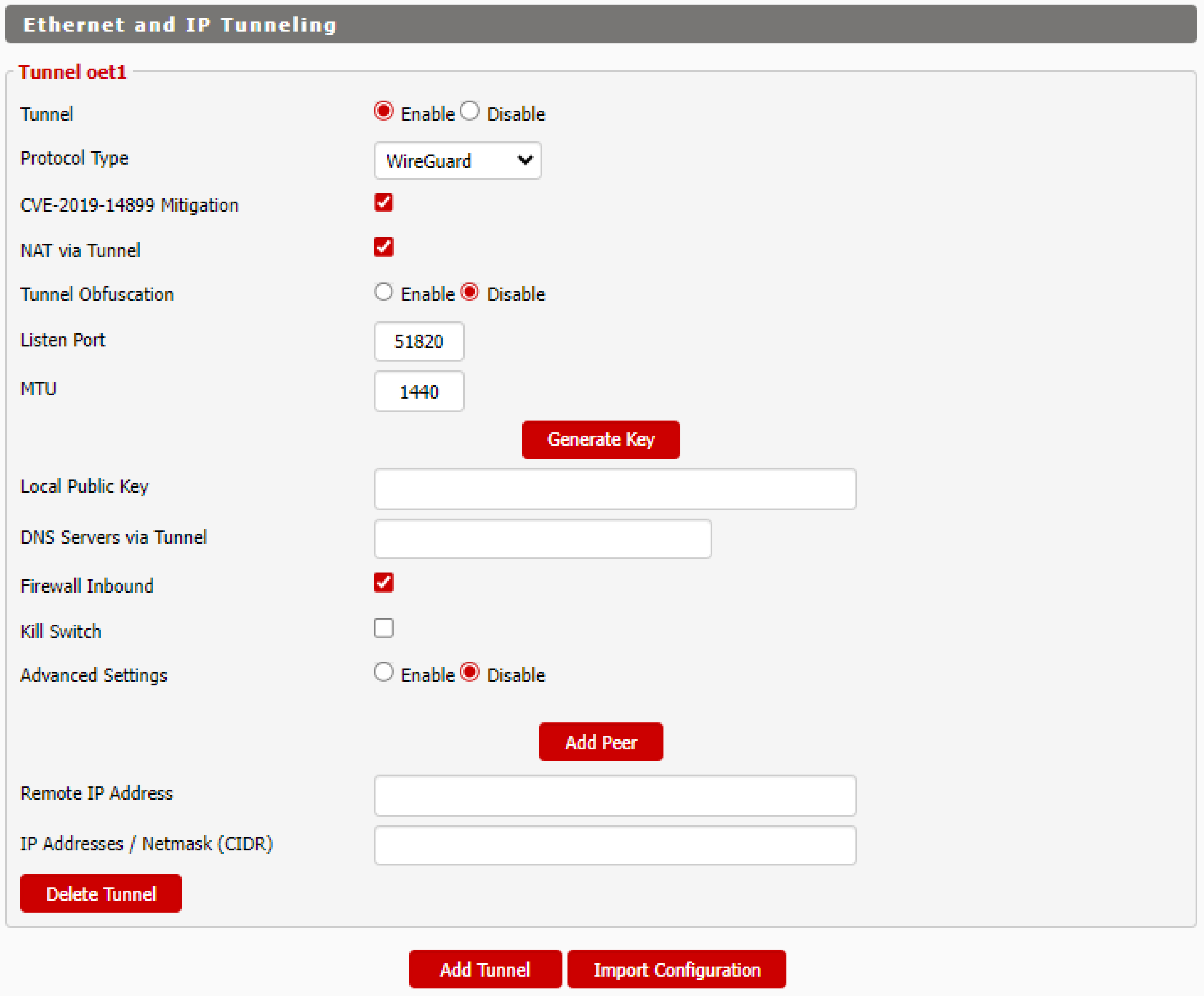
IP Address	Interface	Enable	Start	Max	Lease time	Action
None	br0	On	100	50	1440 min	⊖ ⊕

2.7 Tunnels

2.7.1 Ethernet and IP Tunneling

Ethernet over IP (EoIP) tunneling enables you to create an Ethernet tunnel between two routers on top of an IP connection. The EoIP interface appears as an Ethernet interface. When the bridging function of the router is enabled, all Ethernet traffic will be bridged just as if there was a physical connection between the two routers.

Setup > Tunnels



Ethernet and IP Tunneling

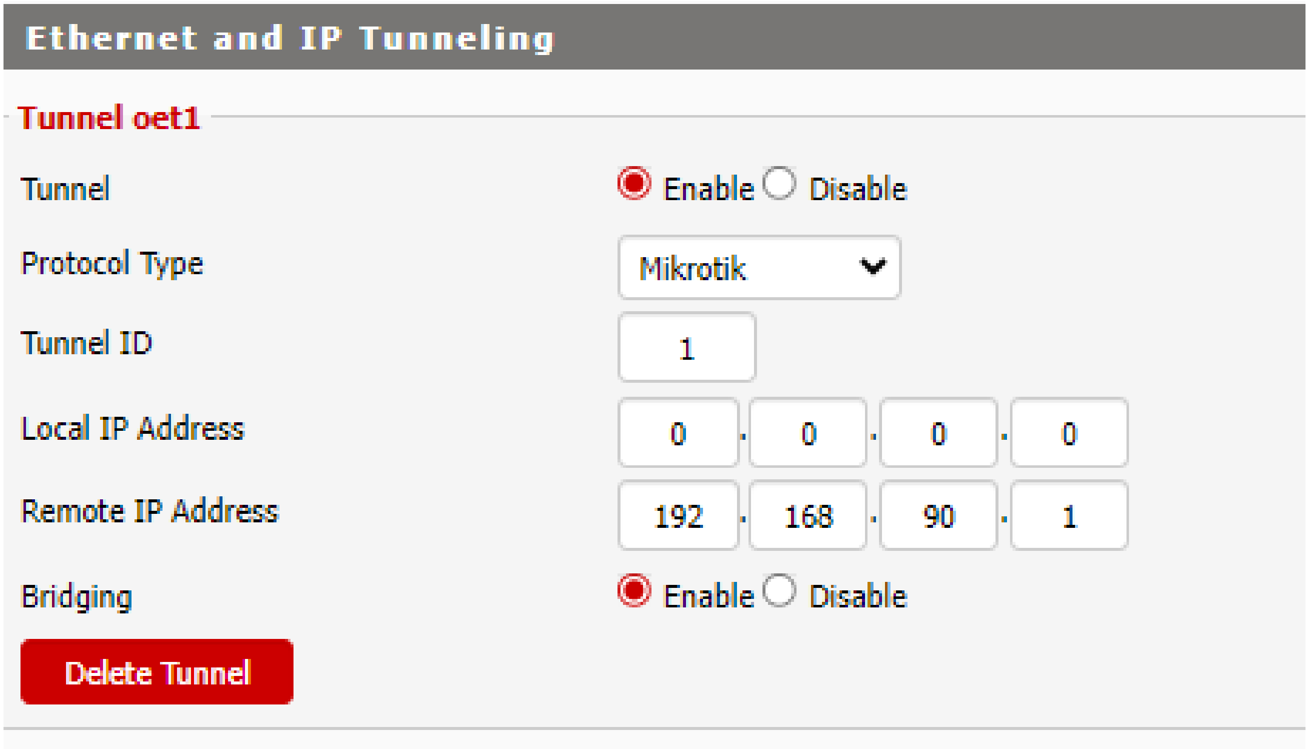
Tunnel oet1

Tunnel	● Enable ○ Disable
Protocol Type	WireGuard
CVE-2019-14899 Mitigation	☑
NAT via Tunnel	☑
Tunnel Obfuscation	○ Enable ● Disable
Listen Port	51820
MTU	1440
Local Public Key	
DNS Servers via Tunnel	
Firewall Inbound	☑
Kill Switch	☐
Advanced Settings	○ Enable ● Disable
Remote IP Address	
IP Addresses / Netmask (CIDR)	

Tunnel	Description
Tunnel	Enable or disable tunneling.
Protocol Type	Select the protocol type.
Local IP Address	Enter a local IP address.
Remote IP Address	Enter a remote IP address.
Bridging	Enable or disable bridging.

2.7.1.1 Mikrotik

Setup > Tunnels > Ethernet and IP Tunneling > Mikrotik



Ethernet and IP Tunneling

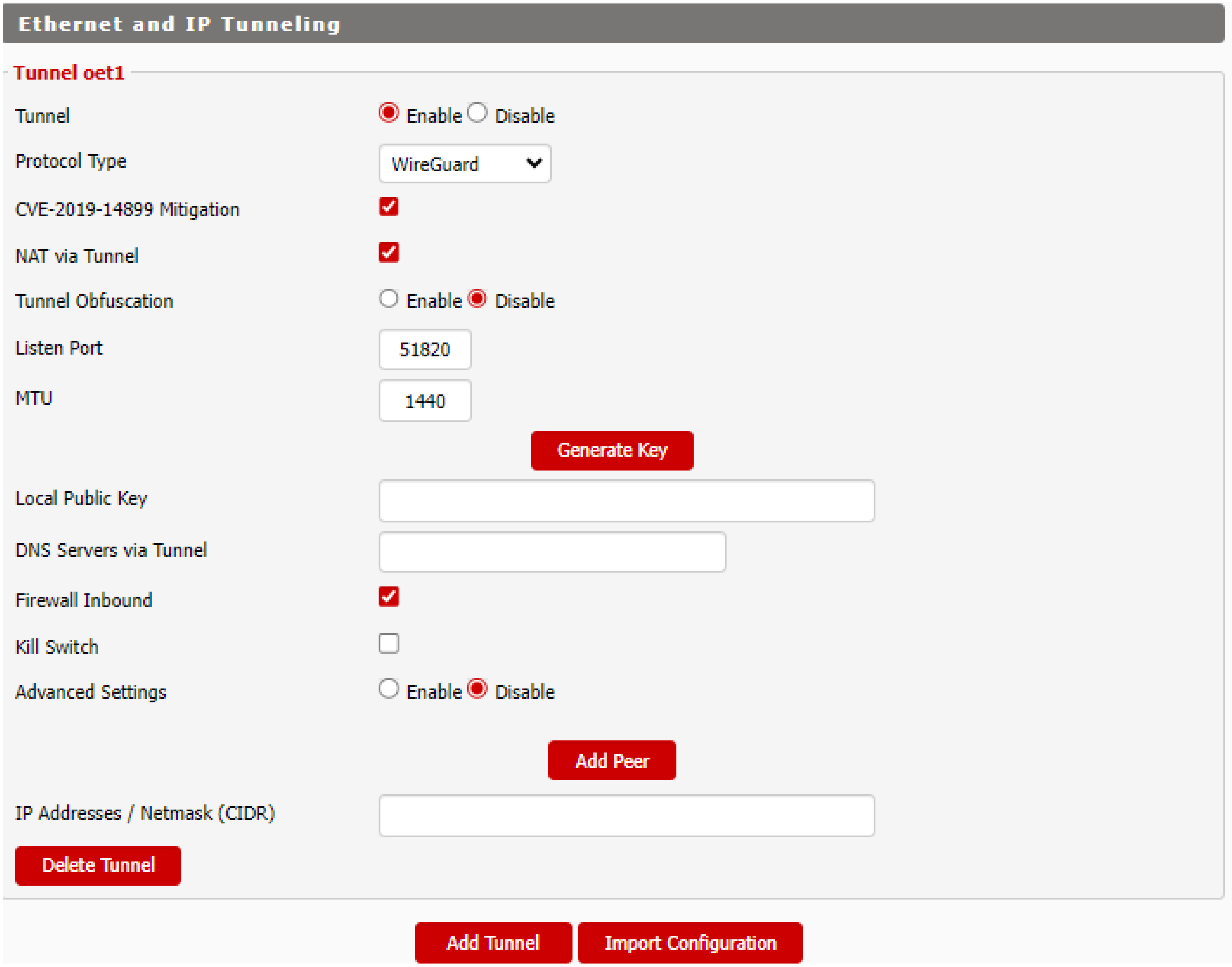
Tunnel oet1

Tunnel	● Enable ○ Disable
Protocol Type	Mikrotik
Tunnel ID	1
Local IP Address	0 . 0 . 0 . 0
Remote IP Address	192 . 168 . 90 . 1
Bridging	● Enable ○ Disable

Tunnel - Mikrotik	Description
Tunnel	Enable or disable tunneling.
Protocol Type	Select the protocol type.
Tunnel ID	Enter a tunnel ID.
Local IP Address	Enter a local IP address.
Remote IP Address	Enter a remote IP address.
Bridging	Enable or disable bridging.

2.7.1.2 WireGuard

Setup > Tunnels > Ethernet and IP Tunneling > WireGuard



Ethernet and IP Tunneling

Tunnel oet1

Tunnel	● Enable ○ Disable
Protocol Type	WireGuard
CVE-2019-14899 Mitigation	☑
NAT via Tunnel	☑
Tunnel Obfuscation	○ Enable ● Disable
Listen Port	51820
MTU	1440
	Generate Key
Local Public Key	
DNS Servers via Tunnel	
Firewall Inbound	☑
Kill Switch	□
Advanced Settings	○ Enable ● Disable
	Add Peer
IP Addresses / Netmask (CIDR)	

Tunnel – WireGuard	Description
Tunnel	Enable or disable tunneling.
Protocol Type	Select the protocol type.
Local Port	Enter a local port number.
Local Public Key	Enter or generate a local public key.
IP Address	Enter an IP address.
Subnet Mask	Enter a subnet mask.

3. Wireless

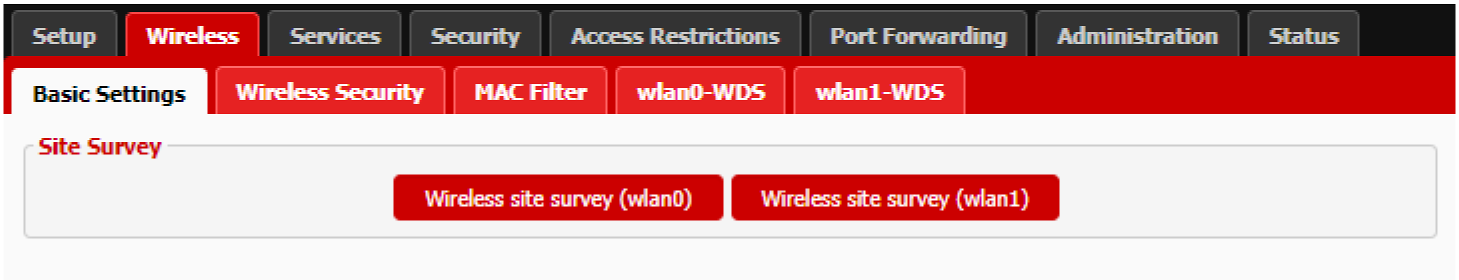
3.1 Basic Settings

All basic wireless settings can be configured here. Users can change the Wireless Mode, Network Mode, Channel Width, Wireless Channel, and SSID.

3.1.1 Wireless Site Survey

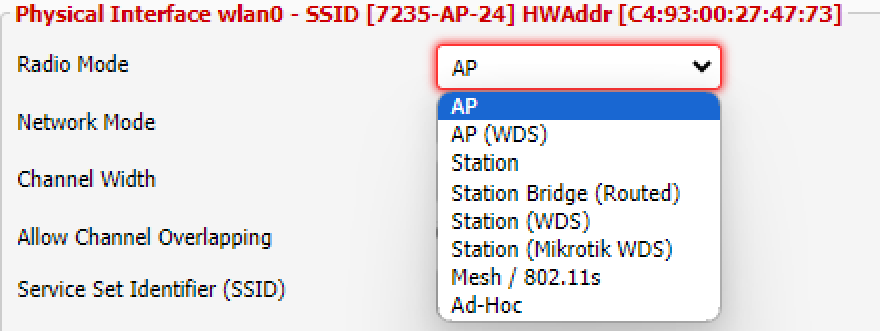
Wireless > Basic Settings

Wireless > Basic Settings > Wireless Site Survey



3.1.2 Wireless Mode

Wireless > Basic Settings > Wireless Mode


Physical Interface wlan0 - SSID [7235-AP-24] HWAddr [C4:93:00:27:47:73]

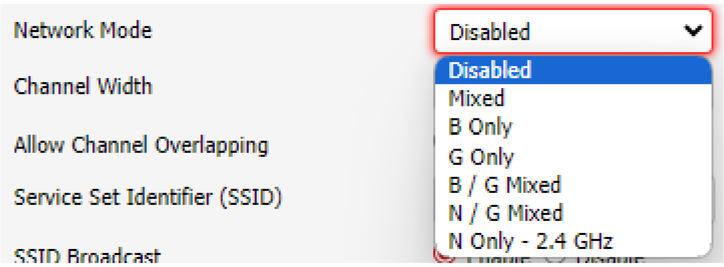
Radio Mode: AP

Basic Settings	Description
Wireless Mode	**AP:** The default settings. Access Point Mode will allow the router to act as a connection point for wireless client devices to connect with.

	Client: The radio interface is used to connect the Internet facing side of the router (the WAN) as a client to a remote access point. NAT or routing are performed between WAN and LAN. Use this mode if your Internet connection is provided by a remote access point and you want to attach a subnet of your own to it.
	Client Bridge (Routed): The radio interface is used to connect the LAN side of the router to an access point. The LAN and access point will be in the same subnet (bridging two network segments). The WAN side of the router is unused and can be disabled. Use this mode to make the router act as a WLAN adapter for a device connected to one of its LAN Ethernet ports.
	WDS Station: Used to connect with a WDS AP. WDS Station functions like a Client, but multiple layer 2 devices can be connected to the WDS Station device.
	WDS AP: Functions as an access point that only WDS Station devices can connect to.
	Mesh/802.11s: Connects wireless devices without having to set up infrastructure. All nodes see each other on a Layer 2 bridged network. Layer 3 infrastructure will work on top of this.

3.1.3 Wireless Network Mode

Wireless > Basic Settings > Wireless Network Mode



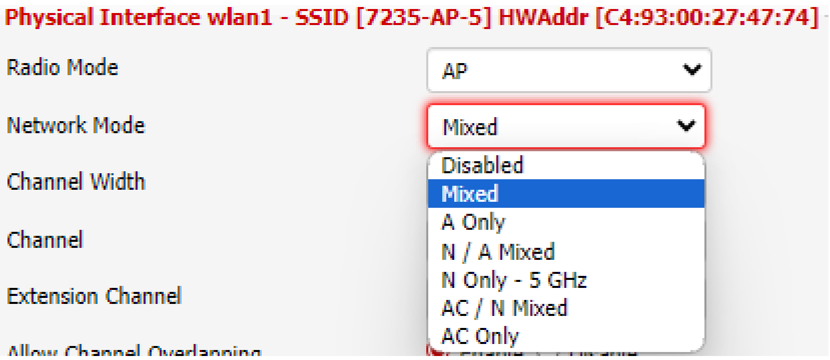
Network Mode: Disabled

Channel Width

Allow Channel Overlapping

Service Set Identifier (SSID)

SSID Broadcast



Physical Interface wlan1 - SSID [7235-AP-5] HWAddr [C4:93:00:27:47:74]

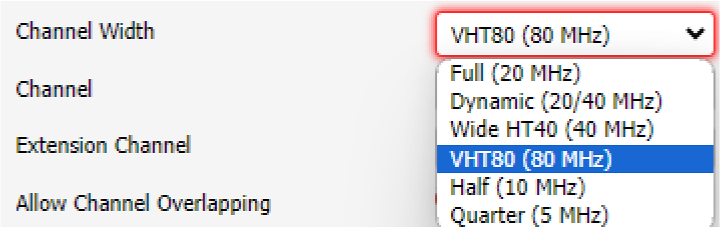
Radio Mode: AP

Network Mode: Mixed

Basic Settings	Description
Wireless Network Mode	**Disabled:** Disables the wireless network mode.
	Mixed: If you have mixed b/g/n devices on your network.
	B-Only: IEEE 802.11b allows a maximum data rate of11Mbits/s through 2.4GHz wireless connections. If only B type wireless devices are on the network, use this mode.
	G-Only: IEEE 802.11g allows a maximum data rate of 54Mbits/s through 2.4GHz wireless connections. If only G type wireless devices are on the network, use this mode.
	BG-Mixed: If B and G-type wireless devices are on the network, use this mode.
	NG-Mixed: Mix band of 802.11b/g/b modes.
	N-Only (2.4GHz): N-Only wireless network mode.
	NA-Mixed: Mix band of 802.11n/a modes.
	N-Only (5GHz): Improved throughput for 5GHz devices.
	AC/N-Mixed: Mix band of 802.11ac/n modes.
	AC-Only: AC-Only wireless network mode.

3.1.4 Channel Width

Wireless > Basic Settings > Channel Width


Channel Width: VHT80 (80 MHz)

Channel

Extension Channel

Allow Channel Overlapping

Basic Settings	Description
Channel Width	Choose between: Full (20MHz), Dynamic (20/40 MHz), Wide HT40 (40MHz), or VHT80 (80MHz).
Wireless Channel	Select the appropriate channel from the list provided to correspond with your network settings (in North America between channel 1 and 11, in Europe 1 and 13, in Japan all 14 channels). All devices in your wireless network must use the same channel in order to function correctly. Try to avoid conflicts with other wireless networks by choosing a channel where the upper and lower three channels are not in use.

TurboQAM Support: Non-standard 256-QAM support on 2.4GHz 802.11n enabling a data rate of up to 200Mbps per spatial stream instead of 150Mbps with the standard 64- QAM.

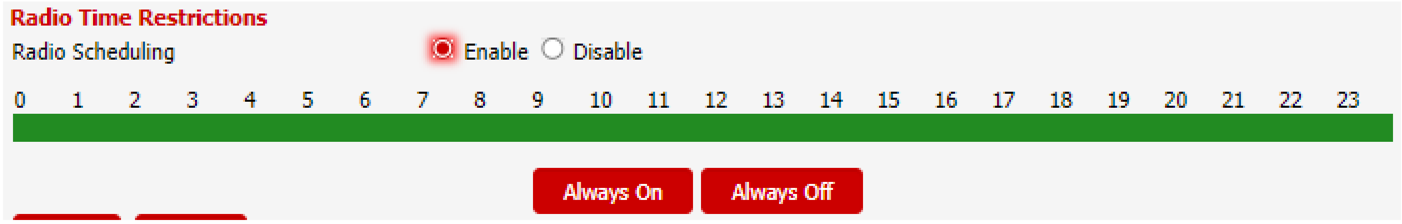
3.1.5 Wireless Network Name (SSID)

The SSID is the Service Set Identifier used to identify the operator's wireless LAN. The SSID is set by the user in Access Point or Access Point WDS Mode. All of the client devices within the range of the access point will receive the broadcasted SSID. The SSID is case-sensitive and must not exceed 32 alphanumeric characters. Make sure this setting is the same for all devices connected to your wireless network.

Wireless SSID Broadcast: When disabled, the SSID of the access point will no longer be broadcasted. This means client devices will not see the SSID of the unit even though they are within range. A user wishing to connect with a client device to a hidden SSID will need to directly input the SSID and password information. The hidden SSID acts as an additional layer of security, making it harder for unwanted users to connect to the network.

3.1.7 Radio Time Restrictions

Wireless > Basic Settings > Radio Time Restrictions

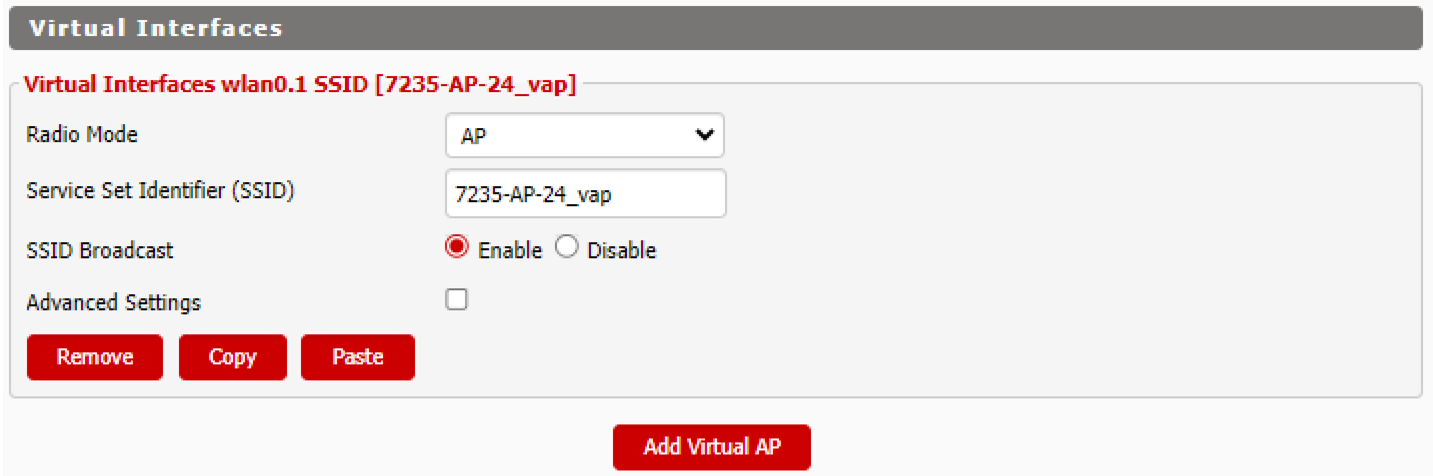


Radio Time Restrictions

Radio Scheduling ● Enable ○ Disable

3.1.8 Virtual Interfaces

Wireless > Basic Settings > Virtual Interfaces



Virtual Interfaces

Virtual Interfaces wlan0.1 SSID [7235-AP-24_vap]

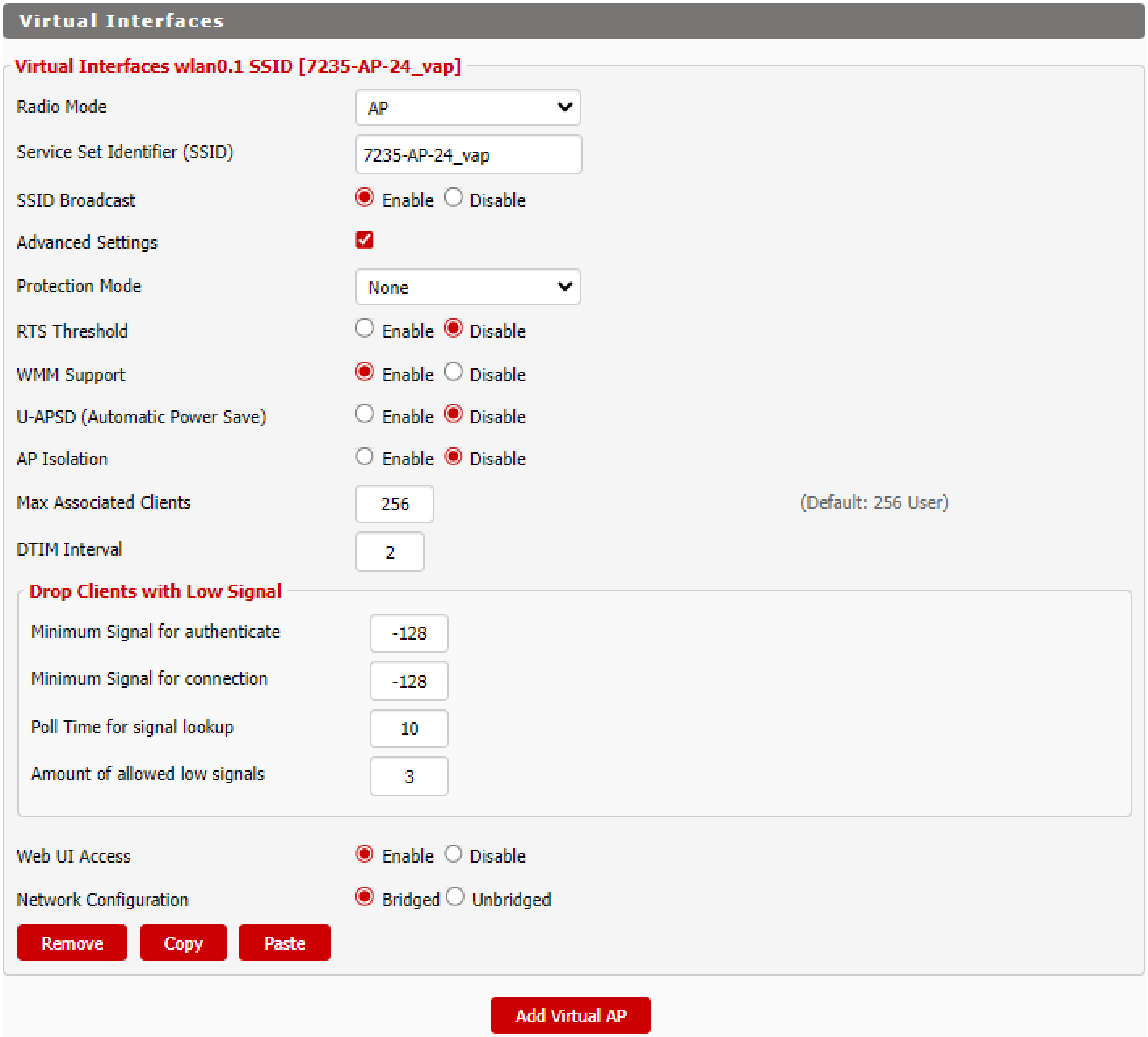
Radio Mode	AP
Service Set Identifier (SSID)	7235-AP-24_vap
SSID Broadcast	● Enable ○ Disable
Advanced Settings	□

Basic Settings	Description
Wireless Mode	Choose between Access Point or WDS Access Point for the wireless mode of the virtual interface.
Wireless Network Name (SSID)	Enter a SSID for the virtual interface.

Wireless SSID Broadcast	Enable or disable broadcasting of the SSID.

3.1.8.1 Advanced Settings

Wireless > Basic Settings > Virtual Interfaces > Advanced Settings



Virtual Interfaces

Virtual Interfaces wlan0.1 SSID [7235-AP-24_vap]

Radio Mode	AP
Service Set Identifier (SSID)	7235-AP-24_vap
SSID Broadcast	● Enable ○ Disable
Advanced Settings	☑
Protection Mode	None
RTS Threshold	○ Enable ● Disable
WMM Support	● Enable ○ Disable
U-APSD (Automatic Power Save)	○ Enable ● Disable
AP Isolation	○ Enable ● Disable
Max Associated Clients	256 (Default: 256 User)
DTIM Interval	2

Drop Clients with Low Signal

Minimum Signal for authenticate	-128
Minimum Signal for connection	-128
Poll Time for signal lookup	10
Amount of allowed low signals	3

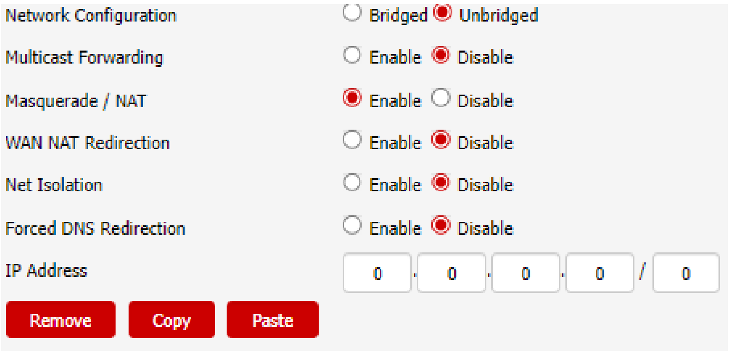
Web UI Access	● Enable ○ Disable
Network Configuration	● Bridged ○ Unbridged

Basic Settings	Description
Protection Mode	Choose between None, CTS, RTS/CTS

RTS Threshold	Specifies the maximum size for a packet before data is fragmented into multiple packets.
Frame Compression	Enable or disable this feature.
WMM Support	Enable or disable this feature.
AP Isolation	Disabled by default. If enabled, wireless clients are isolated and access to and from other wireless clients is stopped.
Max Associated Clients	Number of clients that can be connected to the access point. Default max is 256 users.
DTIM Interval	Set the DTIM interval.
Minimum Signal for Authenticate	Set the minimum signal for authentication.
Minimum Signal for Connection	Set the minimum signal for connections.
Poll Time for Signal Lookup	Set the poll time for signal lookup.
Amount of Allowed Low Signals	Set the amount of allowed low signals.

3.1.8.2 Network Configuration

Wireless > Basic Settings > Virtual Interfaces > Advanced Settings > Network Configuration



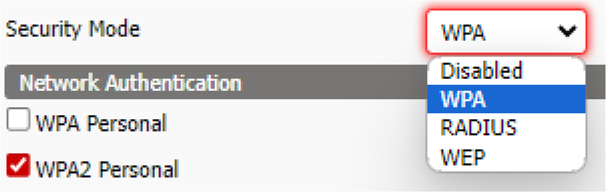
Network Configuration	○ Bridged ● Unbridged
Multicast Forwarding	○ Enable ● Disable
Masquerade / NAT	● Enable ○ Disable
WAN NAT Redirection	○ Enable ● Disable
Net Isolation	○ Enable ● Disable
Forced DNS Redirection	○ Enable ● Disable
IP Address	0 . 0 . 0 . 0 / 0

Basic Settings	Description
Network Configuration	**Bridged** shares the Wireless interface and LAN port (same network). **Unbridged** allows the separation between the Wireless interface and LAN.
Multicast Forwarding	Enable or disable Multicast forwarding.
Masquerade/NAT	Enable or disable NAT.
Net Isolation	Enable or disable Net Isolation.
Forced DNS Redirection	Enable or disable Forced-DNS-Redirection.
IP Address	Enter an IP Address.
Subnet Mask	Enter a Subnet Mask.

3.2 Wireless Security

The Antaira router supports different types of security settings for your network: WiFi Protected Access (WPA), WPA2, WPA3, Remote Access Dial In User Service (RADIUS), and Wires Equivalent Privacy (WEP), which can be selected from the list next to Security Mode. To disable security settings, select *Disabled*.

Wireless > Wireless Security > Security Mode

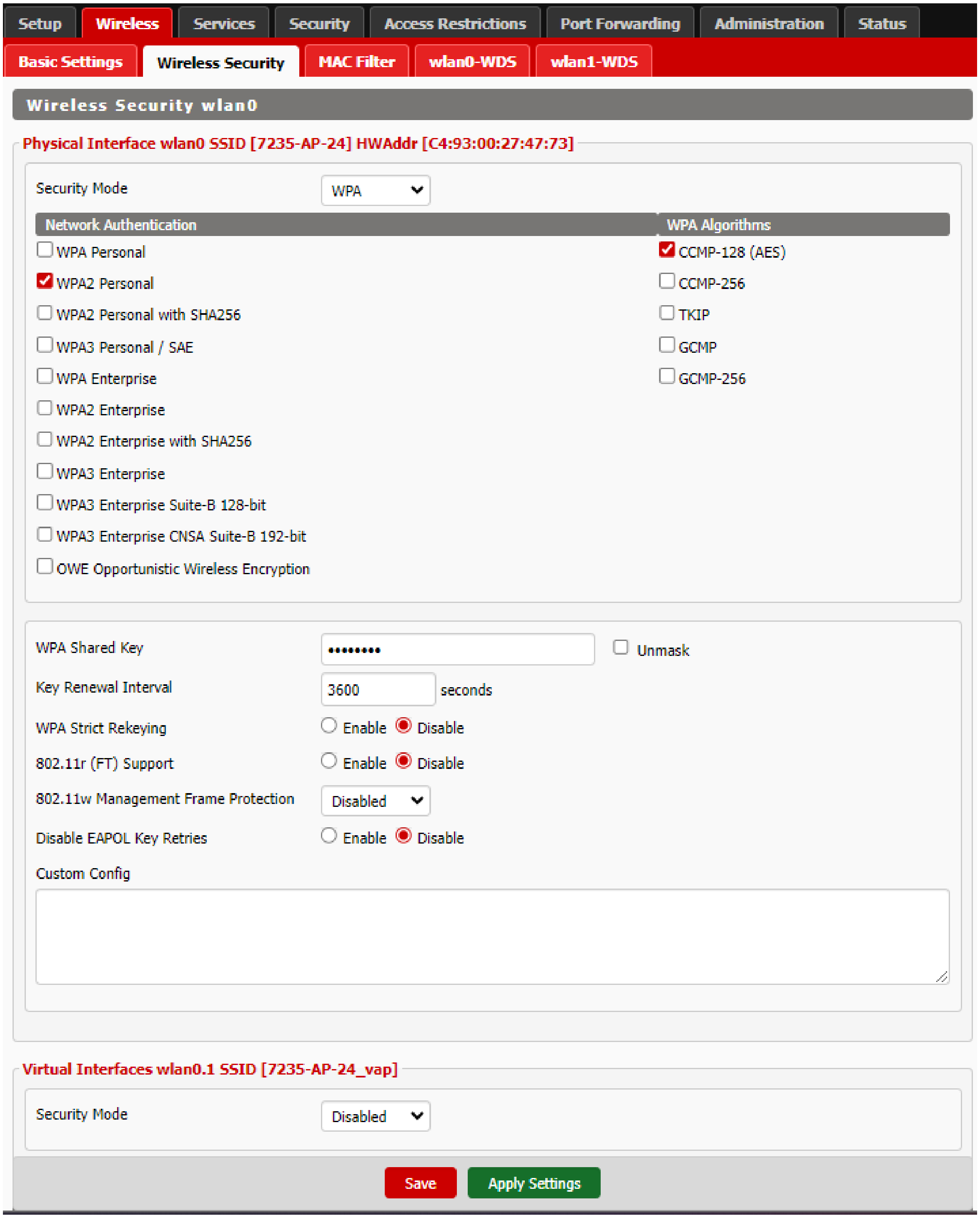


Security Mode: WPA

Network Authentication

☐ WPA Personal

☑ WPA2 Personal



Wireless Security wlan0

Physical Interface wlan0 SSID [7235-AP-24] HWAddr [C4:93:00:27:47:73]

Security Mode: WPA

Network Authentication	WPA Algorithms
□ WPA Personal	☑ CCMP-128 (AES)
☑ WPA2 Personal	□ CCMP-256
□ WPA2 Personal with SHA256	□ TKIP
□ WPA3 Personal / SAE	□ GCMP
□ WPA Enterprise	□ GCMP-256
□ WPA2 Enterprise	
□ WPA2 Enterprise with SHA256	
□ WPA3 Enterprise	
□ WPA3 Enterprise Suite-B 128-bit	
□ WPA3 Enterprise CNSA Suite-B 192-bit	
□ OWE Opportunistic Wireless Encryption	

WPA Shared Key: •••••••• □ Unmask

Key Renewal Interval: 3600 seconds

WPA Strict Rekeying: ○ Enable ● Disable

802.11r (FT) Support: ○ Enable ● Disable

802.11w Management Frame Protection: Disabled

Disable EAPOL Key Retries: ○ Enable ● Disable

Custom Config

Virtual Interfaces wlan0.1 SSID [7235-AP-24_vap]

Security Mode: Disabled

Wireless Security	Description
Security Mode	**Disabled:** Uses no wireless security.
	WPA: Uses WPA for wireless security. Additional

	options and settings will appear when selected.
	RADIUS: Uses RADIUS for wireless security. Additional options and settings will appear when selected.
	WEP: Uses WEP for wireless security. Additional options and settings will appear when selected.
	802.1x/EAP: (Only available when the Wireless Interface is in Client/Client Bridge/WDS Station mode) Uses 802.1x/EAP for wireless security. Additional options and settings will appear when selected.

3.2.1 WPA

Wireless > Wireless Security > Security Mode > WPA

Wireless Security	Description
Network Authentication	Choose the network authentication method.

WPA Algorithms

Wireless Security	Description
WPA Algorithms	**CCMP-128 (AES):** Advanced Encryption System (AES) utilizes a symmetric 128-Bit block data encryption and MIC.
	TKIP: Temporal Key Integrity Protocol (TKIP) which utilizes a stronger encryption method than WEP and incorporates Message Integrity Code (MIC) to provide protection against packet tampering

3.2.2 RADIUS

RADIUS utilizes either a RADIUS server for authentication or WEP for data encryption. To utilize RADIUS, enter the IP address of the RADIUS server and its shared secret. Select the desired encryption bit (64 or 128) for WEP and enter either a passphrase or a manual WEP key.

Wireless > Wireless Security > Security Mode > RADIUS

Wireless Security	Description
MAC Format	When sending the authentication request to the RADIUS server, the wireless client uses the MAC address as the username. This would be received by the RADIUS server in the following format: aabbcc-ddeeff , aabbccddeeff , aa bb-cc-dd-ee-ff.
Radius Auth Server Address	The RADIUS server IP address.
Radius Auth Server Port	The RADIUS server TCP port.
Radius Auth Shared Secret	The RADIUS shared secret.
Force Client IP	Enter a force client IP address if desired.

3.2.3 WEP

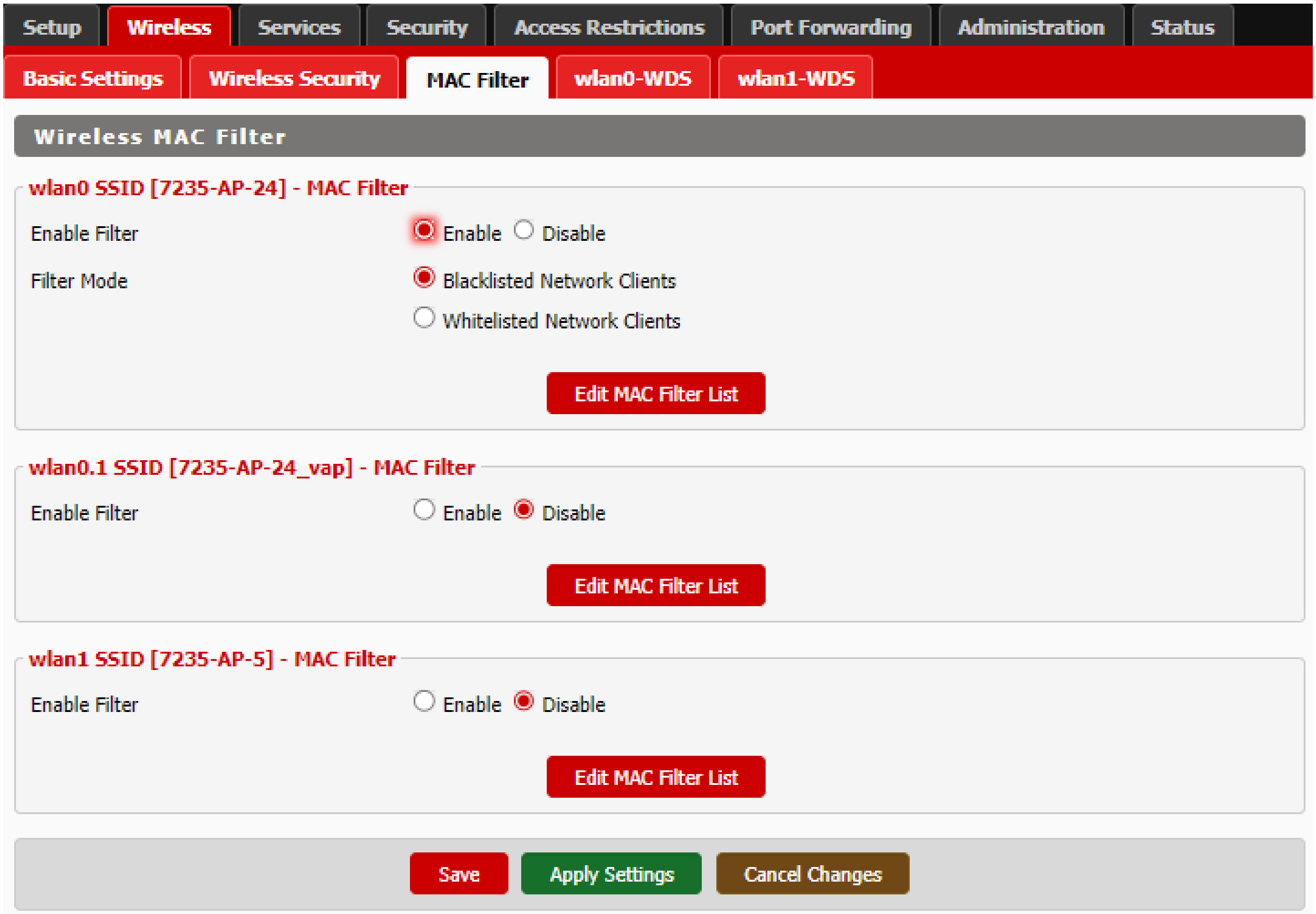
Wireless > Wireless Security > Security Mode > WEP

Wireless Security	Description
Authentication Type	Select Open or Shared Key for Authentication Type.
Default Transmit Key	Set the Default Transmit Key (1-4).
Encryption	Select the Encryption method.
Passphrase	Enter a Passphrase or generate one.
Key #	Enter key(s).

3.3 MAC Filter

The Wireless MAC Filter allows you to control which wireless-equipped PCs may or may not communicate with the router depending on their MAC addresses.

Wireless > MAC Filter



Wireless MAC Filter

wlan0 SSID [7235-AP-24] - MAC Filter

Enable Filter ● Enable ○ Disable

Filter Mode ● Blacklisted Network Clients ○ Whitelisted Network Clients

wlan0.1 SSID [7235-AP-24_vap] - MAC Filter

Enable Filter ○ Enable ● Disable

wlan1 SSID [7235-AP-5] - MAC Filter

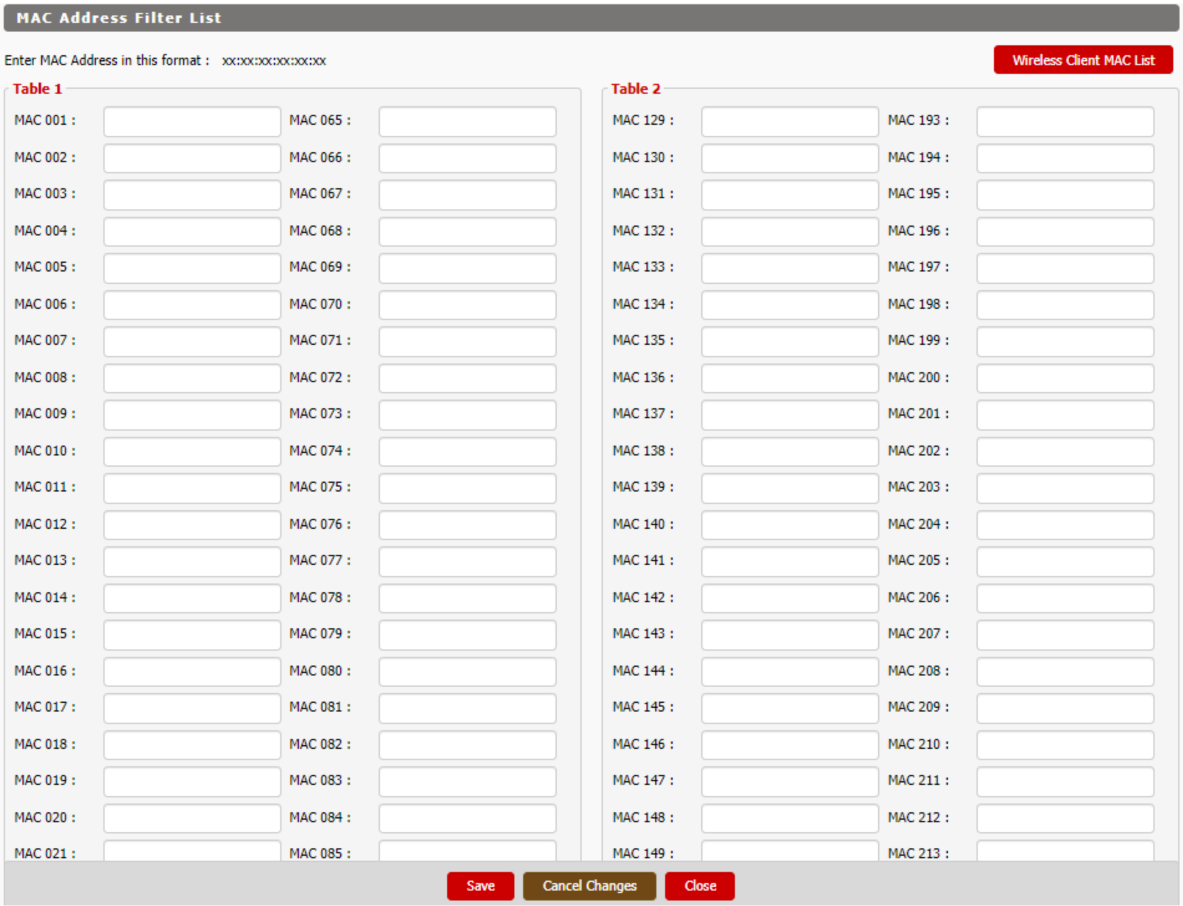
Enable Filter ○ Enable ● Disable

MAC Filter	Description
Use Filter	Enable or disable Wireless MAC Filter.
Filter Mode	**Prevent Clients Listed from Accessing the Wireless Network:** If you want to block specific wireless-equipped PCs from communicating with the router, use this setting.

	Permit Only Clients Listed to Access the Wireless Network: If you want to allow specific wireless-equipped PCs to communicate with the router, use this setting. Click the *Edit MAC Filter List* button and enter the appropriate MAC addresses into the MAC fields. **Note:** The MAC Address should be entered in this format: xxxxxxxxxxxx (the x's represent the actual characters of the MAC address). Click the *Save Settings* button to save your changes. Click the *Cancel Changes* button to cancel your unsaved changes. Click the *Close* button to return to the previous screen without saving changes.

3.3.1 Edit MAC Filter List

Wireless > MAC Filter > Edit MAC Filter List



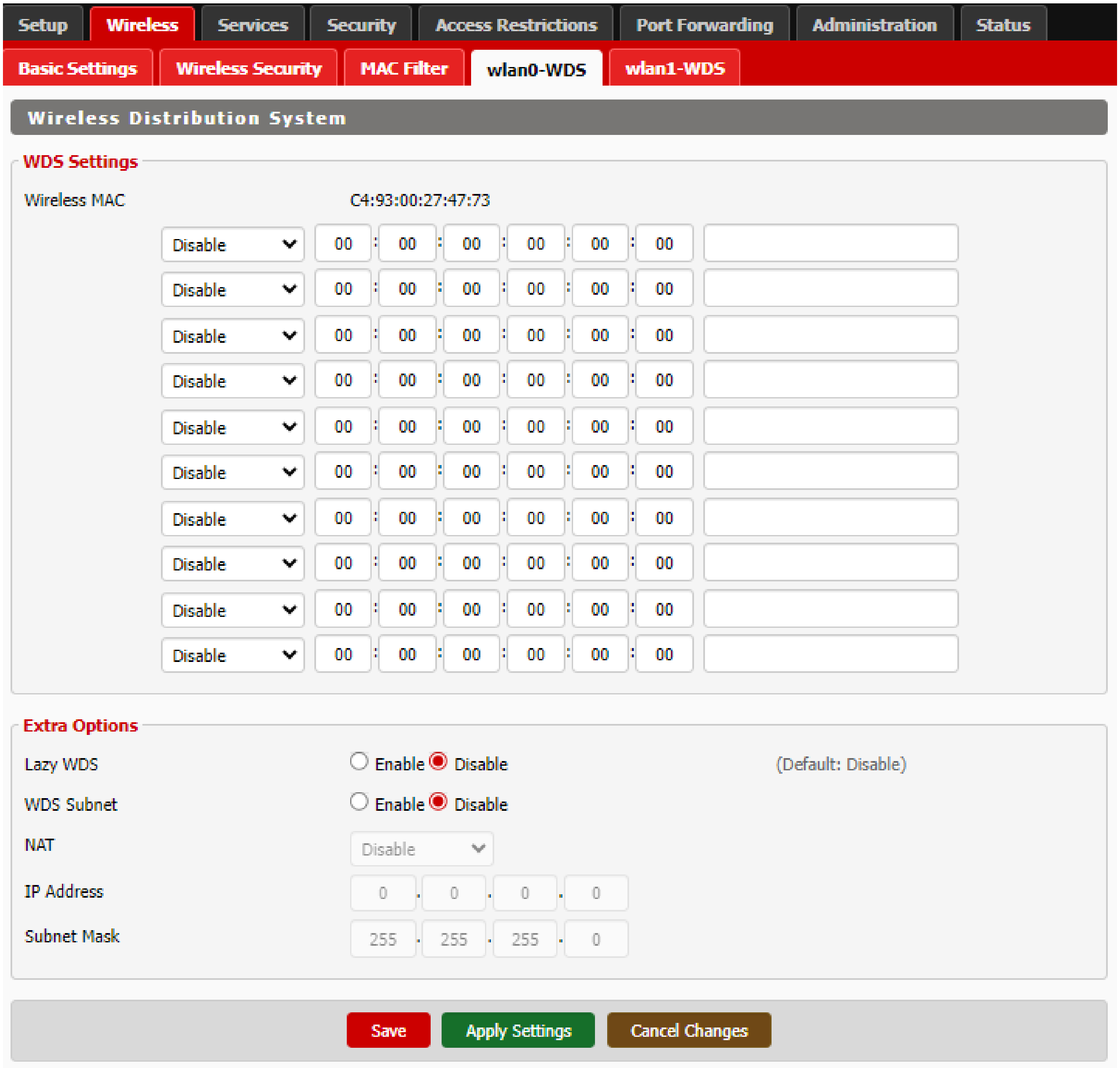
MAC Address Filter List

Enter MAC Address in this format : xx:xx:xx:xx:xx:xx

3.4 WDS

WDS (Wireless Distribution System) is a Wireless Access Point mode that enables wireless bridging in which WDS APs communicate only with each other (without allowing for wireless clients or stations to access them), and wireless repeating in which APs communicate with each other and with wireless stations (at the expense of halving the throughput). This mode supports two types of WDS: LAN and Point to Point.

Wireless > WDS



Wireless Distribution System

WDS Settings

Wireless MAC C4:93:00:27:47:73

Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	
Disable	00	00	00	00	00	00	

Extra Options

Lazy WDS ○ Enable ● Disable (Default: Disable)

WDS Subnet ○ Enable ● Disable

NAT Disable

IP Address 0 . 0 . 0 . 0

Subnet Mask 255 . 255 . 255 . 0

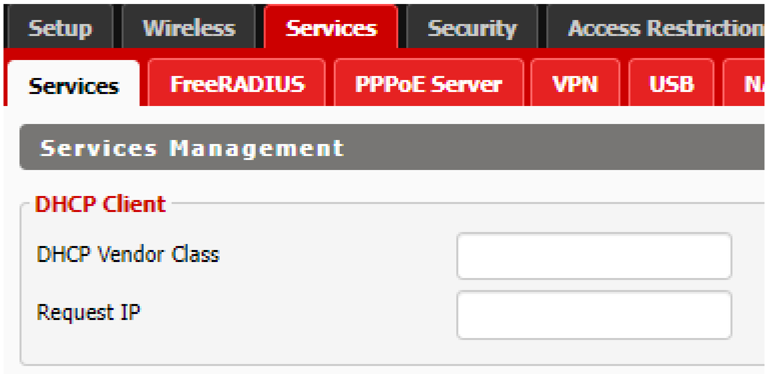
WDS	Description
Wireless MAC	Select between Disable, Point-to-Point, or LAN. Then enter a corresponding Wireless MAC address.
Lazy WDS	Enable or disable Lazy WDS.
WDS Subnet	Enable or disable WDS Subnet.
NAT	Enable or disable NAT.
IP Address	Enter an IP Address.
Subnet Mask	Enter a Subnet Mask.

4. Services

4.1 Services

4.1.1 DHCP Client

Services > Services > DHCP Client



Services Management

DHCP Client

DHCP Vendor Class

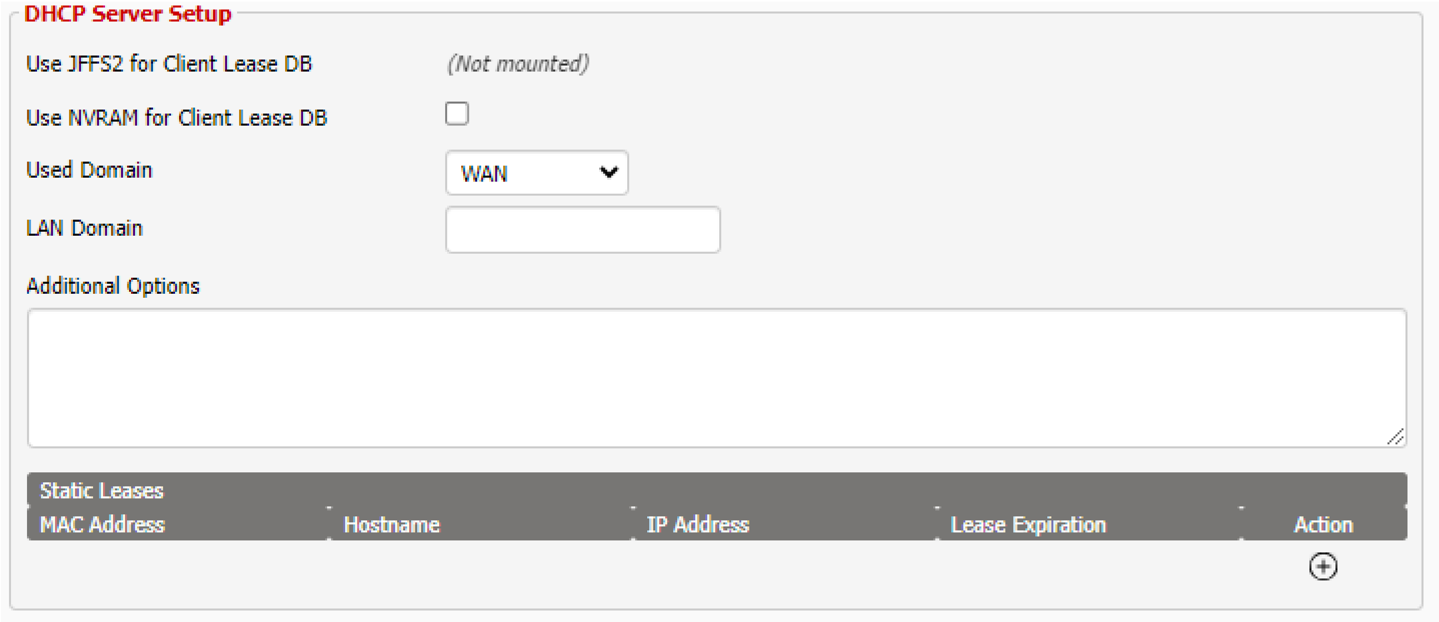
Request IP

DHCP Client	Description
Set Vendorclass	Enter a vendorclass.
Request IP	Enter a request IP.

4.1.2 DHCP Server

A DHCP server assigns IP addresses to your local devices.

Services > Services > DHCP Server



DHCP Server Setup

Use JFFS2 for Client Lease DB	*(Not mounted)*
Use NVRAM for Client Lease DB	□
Used Domain	WAN
LAN Domain	
Additional Options	

Static Leases

MAC Address	Hostname	IP Address	Lease Expiration	Action
				⊕

DHCP Server	Description
Use NVRAM for Client Lease DB	Enable or disable this feature.
Used Domain	Select which domain the DHCP clients should get as their local domain. This can be the WAN domain set on the Setup screen of the LAN domain which can be set here.
LAN Domain	Define your local LAN domain here. This is used as the local domain for dnsmasq and DHCP service if chosen above.
Additional DHCPd Options	Enter any additional DHCPd options here.
Static Leases	If you want to assign certain hosts a specific address then you can define them here. This is also the way to add hosts with a fixed address to the router's local

	DNS service (dnsmasq).

4.1.3 Dnsmasq

Dnsmasq is a local DNS server. It will resolve all host names known to the router from DHCP as well as forwarding and caching DNS entries from remote DNS servers.

Services > Services > Dnsmasq

Dnsmasq	Description
Dnsmasq	Enable or disable this feature.
Encrypt DNS	Enable or disable this feature.
DNSCrypt Reslover	
Cache DNSSEC data	Enable or disable this feature.
Validate DNS Replies (DNSSEC)	Enable or disable this feature.
Check Unsigned DNS Replies	Enable or disable this feature.
Local DNS	Enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.
No DNS Rebind	Enable or disable this feature.
Query DNS in Strict Order	Enable or disable this feature.
Add Requestor MAC to DNS Query	Enable or disable this feature.
Additional Dnsmasq Options	Enter any additional options here.

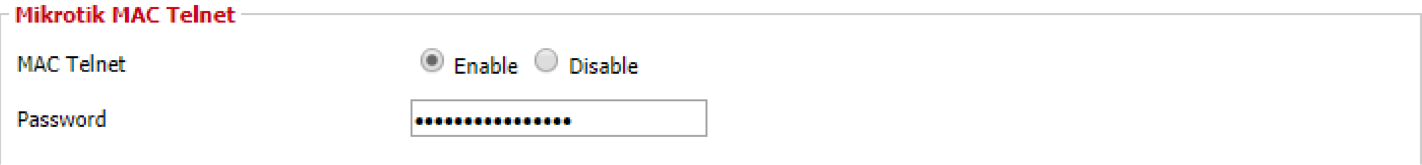
4.1.4 Lighttpd Webserver

Services > Services > Lighttpd Webserver

Lighttpd	Description
Lighttpd	Enable or disable this feature.
HTTPS Port	Set the HTTPS Port. Default is port 443.
HTTP Port	Set the HTTP Port. Default is port 8000.
WAN Access	Allow WAN Access.
URL	Displays the URL link.

4.1.5 Mikrotik MAC Telnet

Services > Services > Mikrotik MAC Telnet



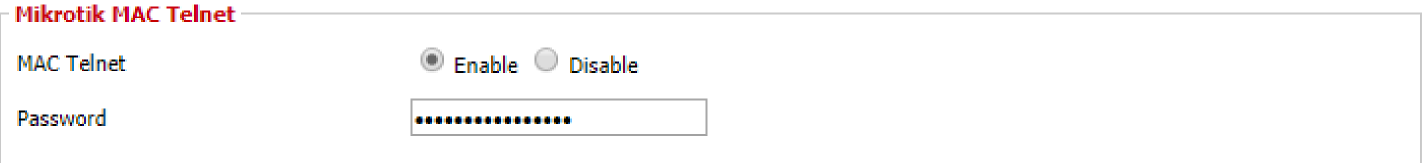
Mikrotik MAC Telnet

MAC Telnet ● Enable ○ Disable

Password ••••••••••••••••

4.1.6 PPPoE Relay

Services > Services > PPPoE Relay



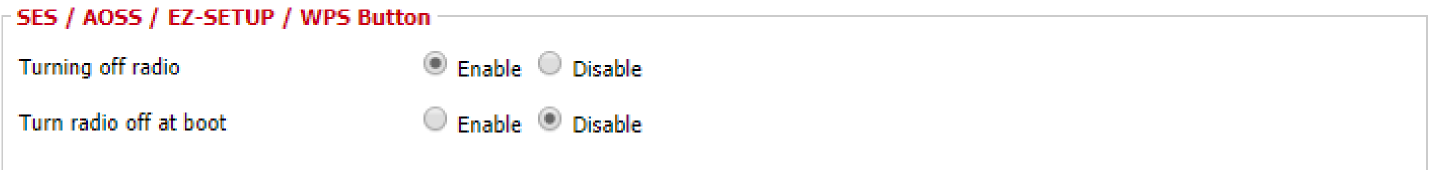
Mikrotik MAC Telnet

MAC Telnet ● Enable ○ Disable

Password ••••••••••••••••

4.1.7 SES/AOSS/EZ-SETUP/WPS Button

Services > Services > SES/AOSS/EZ-SETUP/WPS Button



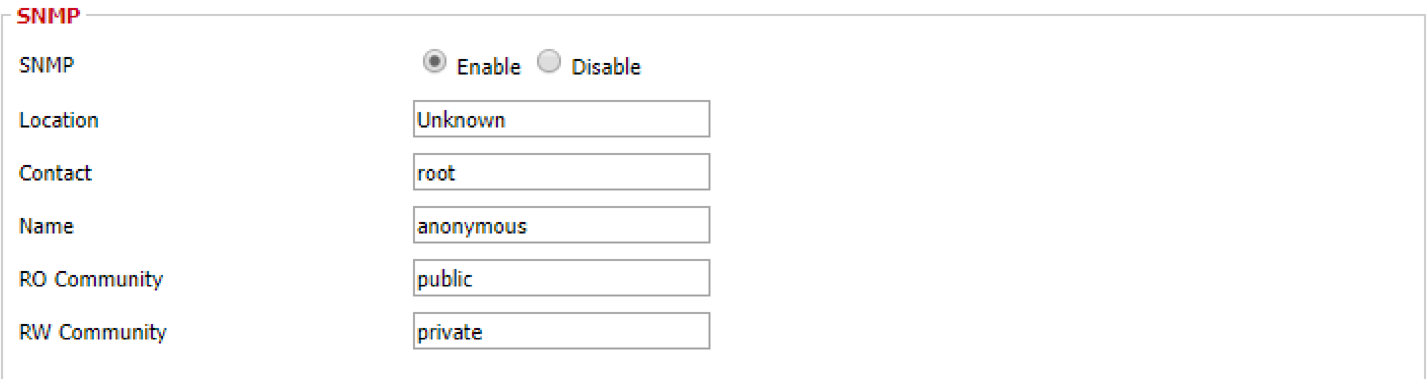
SES / AOSS / EZ-SETUP / WPS Button

Turning off radio	● Enable ○ Disable
Turn radio off at boot	○ Enable ● Disable

4.1.8 SNMP

The Simple Network Management Protocol (SNMP) is an application layer protocol that facilitates the exchange of management information between network devices. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

Services > Services > SNMP



SNMP

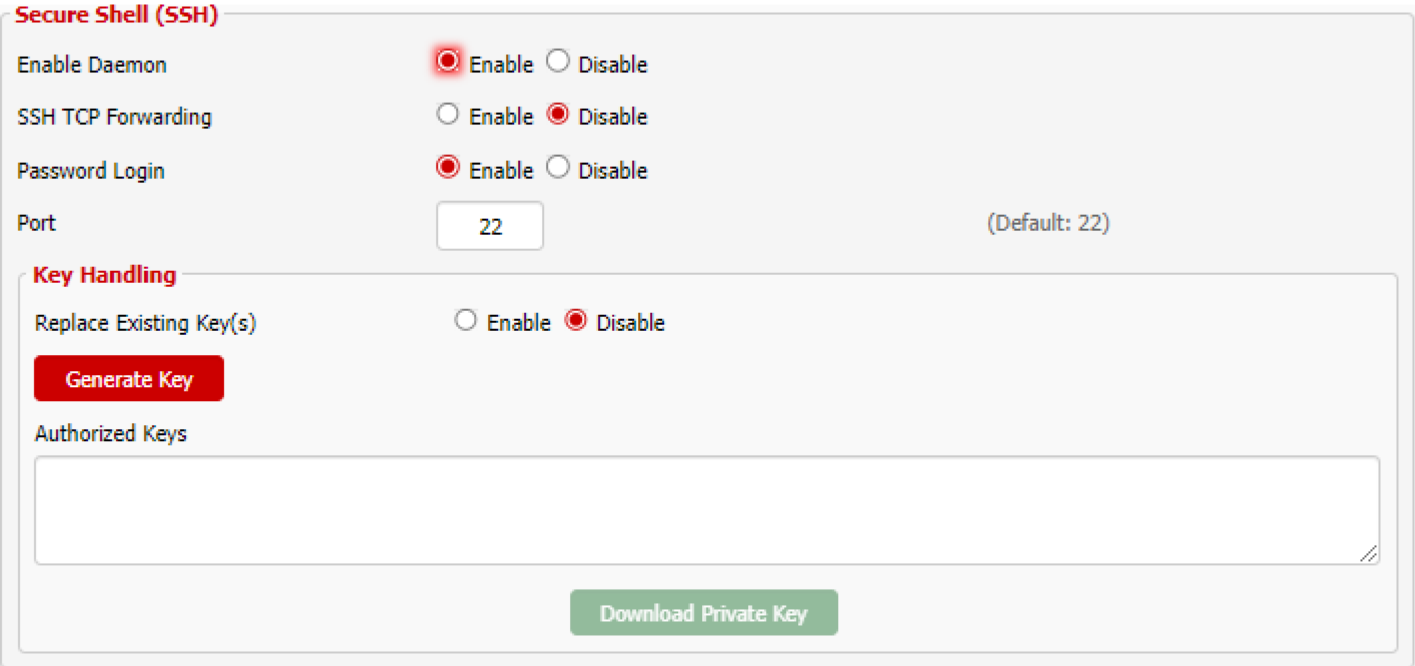
SNMP	● Enable ○ Disable
Location	Unknown
Contact	root
Name	anonymous
RO Community	public
RW Community	private

SNMP	Description
SNMP	Enable or disable SNMP.
Location	Enter location information.
Contact	Enter contact information.
Name	Enter a name.
RO Community	Enter a Read-Only Community string.
RW Community	Enter a Read/Write Community string.

4.1.9 Secure Shell

Enabling SSH allows you to access the Linux OS of your router with an SSH client (Putty for example).

Services > Services > Secure Shell



Secure Shell (SSH)

Enable Daemon ● Enable ○ Disable

SSH TCP Forwarding ○ Enable ● Disable

Password Login ● Enable ○ Disable

Port 22 (Default: 22)

Key Handling

Replace Existing Key(s) ○ Enable ● Disable

Generate Key

Authorized Keys

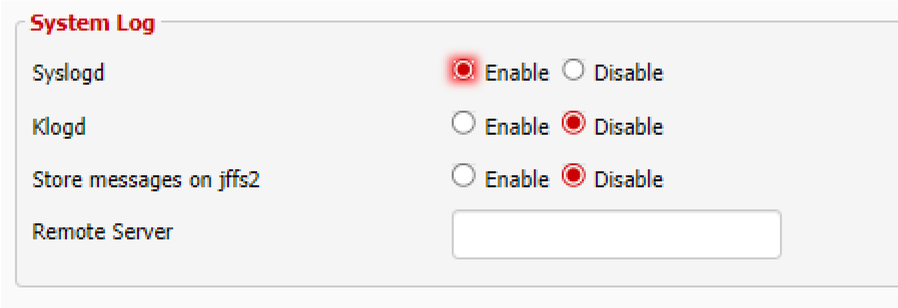
Download Private Key

Secure Shell	Description
SSHd	Enable or disable SSH.
SSH TCP Forwarding	Enable or disable this feature.
Password Login	Allow login with the router password (Username is *root*).
Port	Change the SSH port. Default is port 22.
Authorized Keys	Enter authorized keys is applicable.

4.1.10 System Log

System Logging is a messaging standard for logging on a network. Logging is useful to monitor the health of your network, help diagnose problems, intrusion detection, and intrusion forensics.

Services > Services > System Log



System Log

Syslogd ● Enable ○ Disable

Klogd ○ Enable ● Disable

Store messages on jffs2 ○ Enable ● Disable

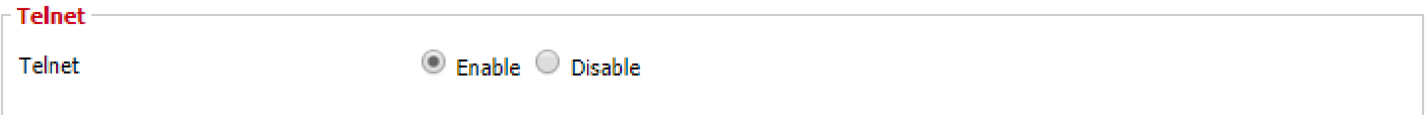
Remote Server

System Log	Description
Syslogd	Enable or disable syslogd.
Klogd	Enable or disable Klogd.
Remote Server	Enter the remote server IP address to receive syslogs.

4.1.11 Telnet

Enable or disable Telnet.

Services > Services > Telnet

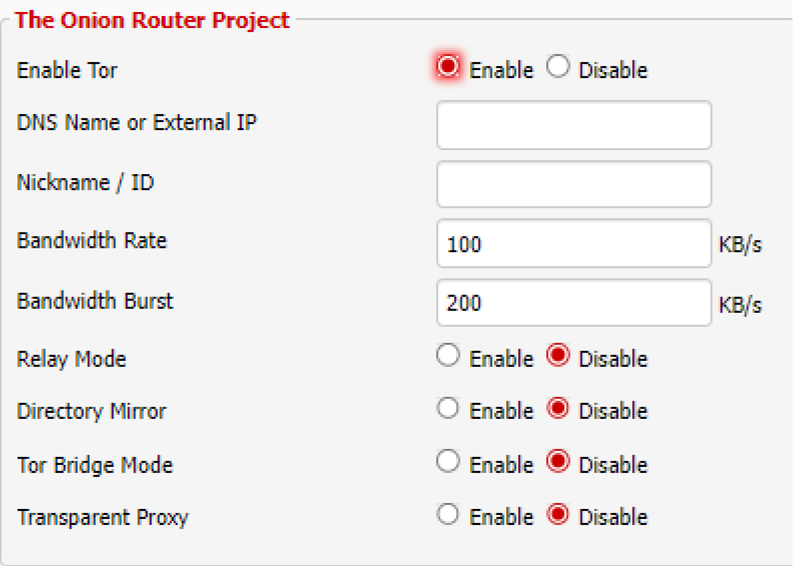


Telnet

Telnet ● Enable ○ Disable

4.1.12 The Onion Router Project

Services > Services > The Onion Router Project



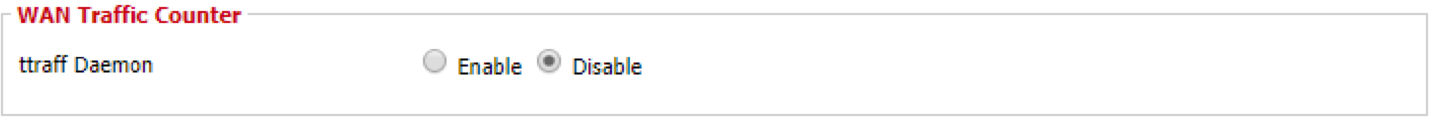
The Onion Router Project

Enable Tor	● Enable ○ Disable
DNS Name or External IP	
Nickname / ID	
Bandwidth Rate	100 KB/s
Bandwidth Burst	200 KB/s
Relay Mode	○ Enable ● Disable
Directory Mirror	○ Enable ● Disable
Tor Bridge Mode	○ Enable ● Disable
Transparent Proxy	○ Enable ● Disable

Onion Router Project	Description
Tor	Enable or disable this feature.
DNS Name or External IP	Enter the DNS name or external IP address.
Nickname/ID	Enter a nickname/ID.
Bandwidth Rate	Set the bandwidth rate.
Bandwidth Burst	Set the bandwidth burst.
Relay Mode	Enable or disable this feature.
Directory Mirror	Enable or disable this feature.
Tor Bridge Mode	Enable or disable this feature.
Transparent Proxy	Enable or disable this feature.

4.1.13 WAN Traffic Counter

Services > Services > WAN Traffic Counter

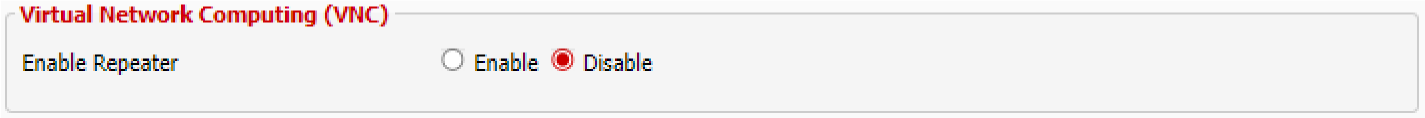


WAN Traffic Counter

ttraff Daemon ○ Enable ● Disable

4.1.14 VNC

Services > Services > VNC

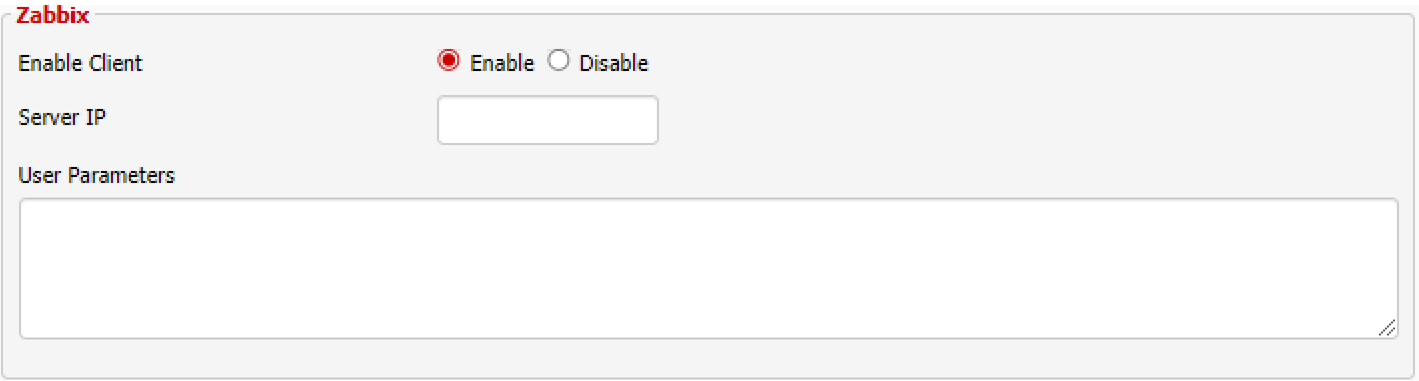


Virtual Network Computing (VNC)

Enable Repeater ○ Enable ● Disable

4.1.15 Zabbix

Services > Services > Zabbix



Zabbix

Enable Client ● Enable ○ Disable

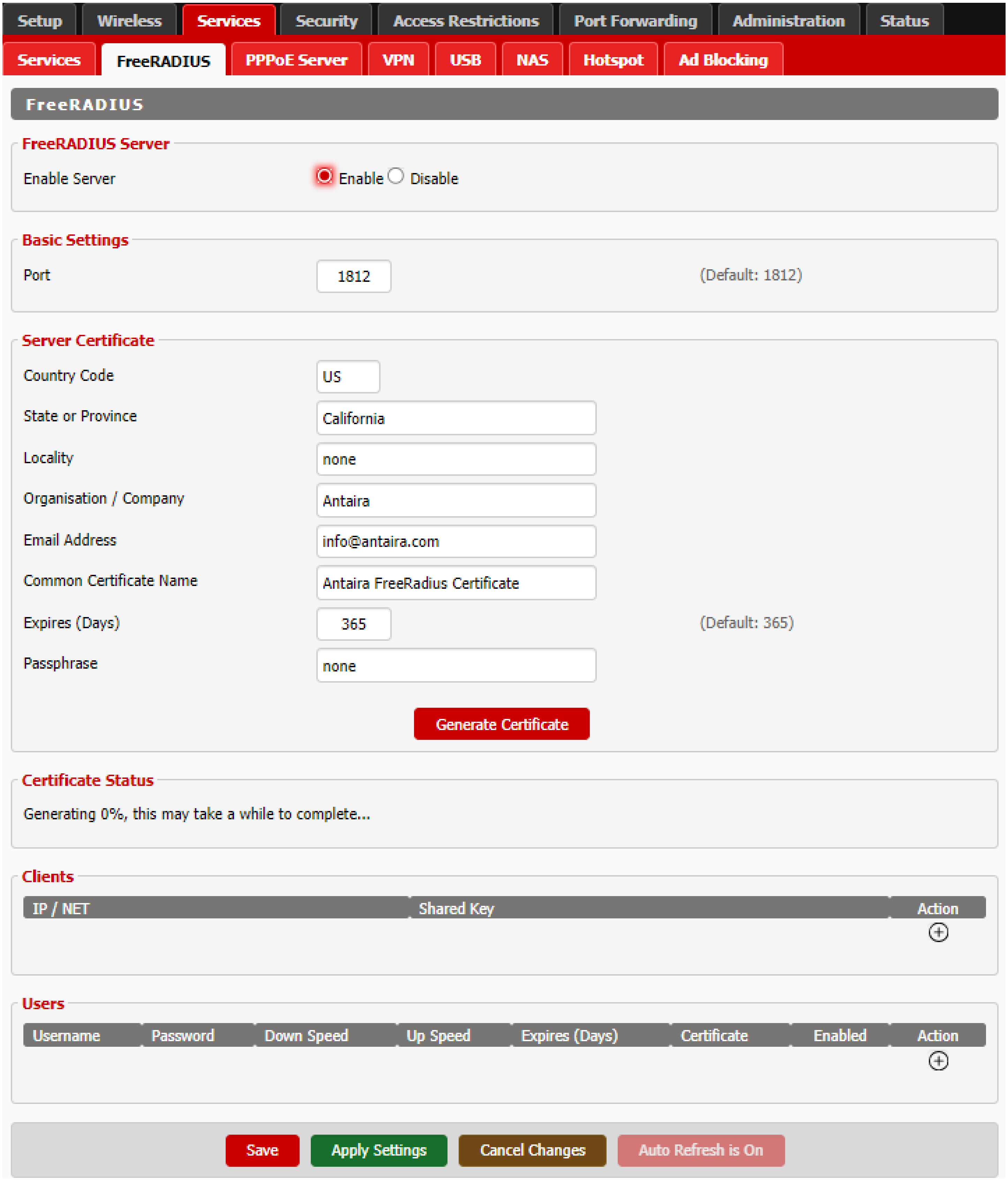
Server IP

User Parameters

4.2 FreeRadius

FreeRADIUS is widely deployed RADIUS. FreeRADIUS can be used to authenticate WLAN clinets using WPA/WPA2 Enterpirse.

Services > FreeRadius



FreeRADIUS

FreeRADIUS Server

Enable Server ● Enable ○ Disable

Basic Settings

Port 1812 (Default: 1812)

Server Certificate

Country Code	US
State or Province	California
Locality	none
Organisation / Company	Antaira
Email Address	info@antaira.com
Common Certificate Name	Antaira FreeRadius Certificate
Expires (Days)	365 (Default: 365)
Passphrase	none

Generate Certificate

Certificate Status

Generating 0%, this may take a while to complete...

Clients

IP / NET	Shared Key	Action
		⊕

Users

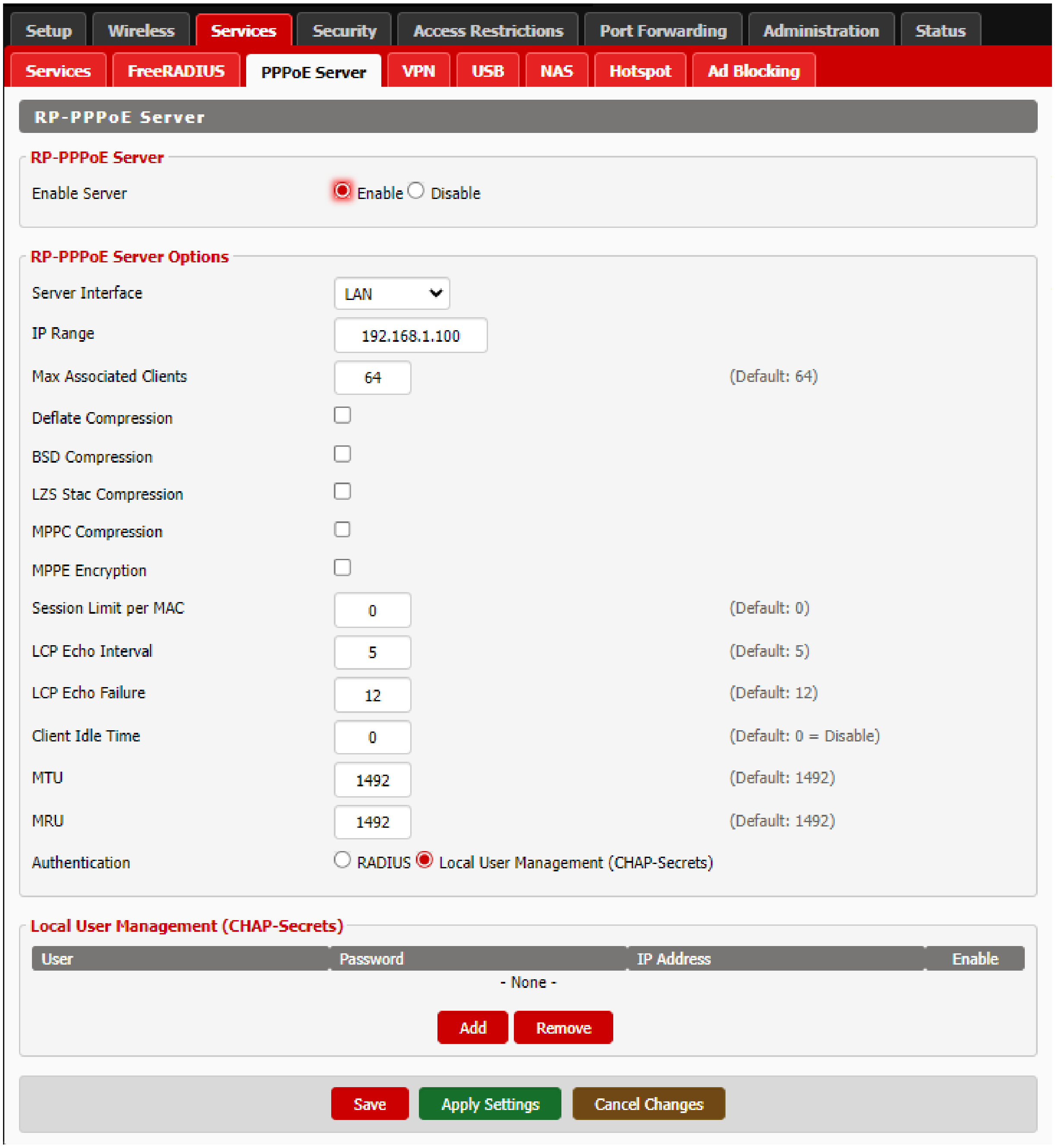
Username	Password	Down Speed	Up Speed	Expires (Days)	Certificate	Enabled	Action
							⊕

FreeRadius	Description
FreeRadius	Enable or disable FreeRadius.
Country Code	Enter a Country Code.
State or Province	Enter a State or Province.
Locality	Enter a Locality.
Organization/Company	Enter an Organization or Company.
Email Address	Enter an email address.
Common Certificate Name	Enter a Common Certificate Name.
Expires (Days)	Set the expiration date for the certificate. Default is 365 days.
Passphrase	Enter a passphrase.
Radius Port	Set the Radius port. Default is port 1812.
Clients	Add clients.
Users	Add users.

4.3 PPPoE Server

The Point-to-Point Protocol over Ethernet (PPPoE) is a networking protocol for encapsulating PPP frames inside Ethernet frames.

Services > PPPoE Server



RP-PPPoE Server

RP-PPPoE Server

Enable Server ● Enable ○ Disable

RP-PPPoE Server Options

Server Interface	LAN	
IP Range	192.168.1.100	
Max Associated Clients	64	(Default: 64)
Deflate Compression	□	
BSD Compression	□	
LZS Stac Compression	□	
MPPC Compression	□	
MPPE Encryption	□	
Session Limit per MAC	0	(Default: 0)
LCP Echo Interval	5	(Default: 5)
LCP Echo Failure	12	(Default: 12)
Client Idle Time	0	(Default: 0 = Disable)
MTU	1492	(Default: 1492)
MRU	1492	(Default: 1492)
Authentication	○ RADIUS ● Local User Management (CHAP-Secrets)	

Local User Management (CHAP-Secrets)

User	Password	IP Address	Enable
- None -			

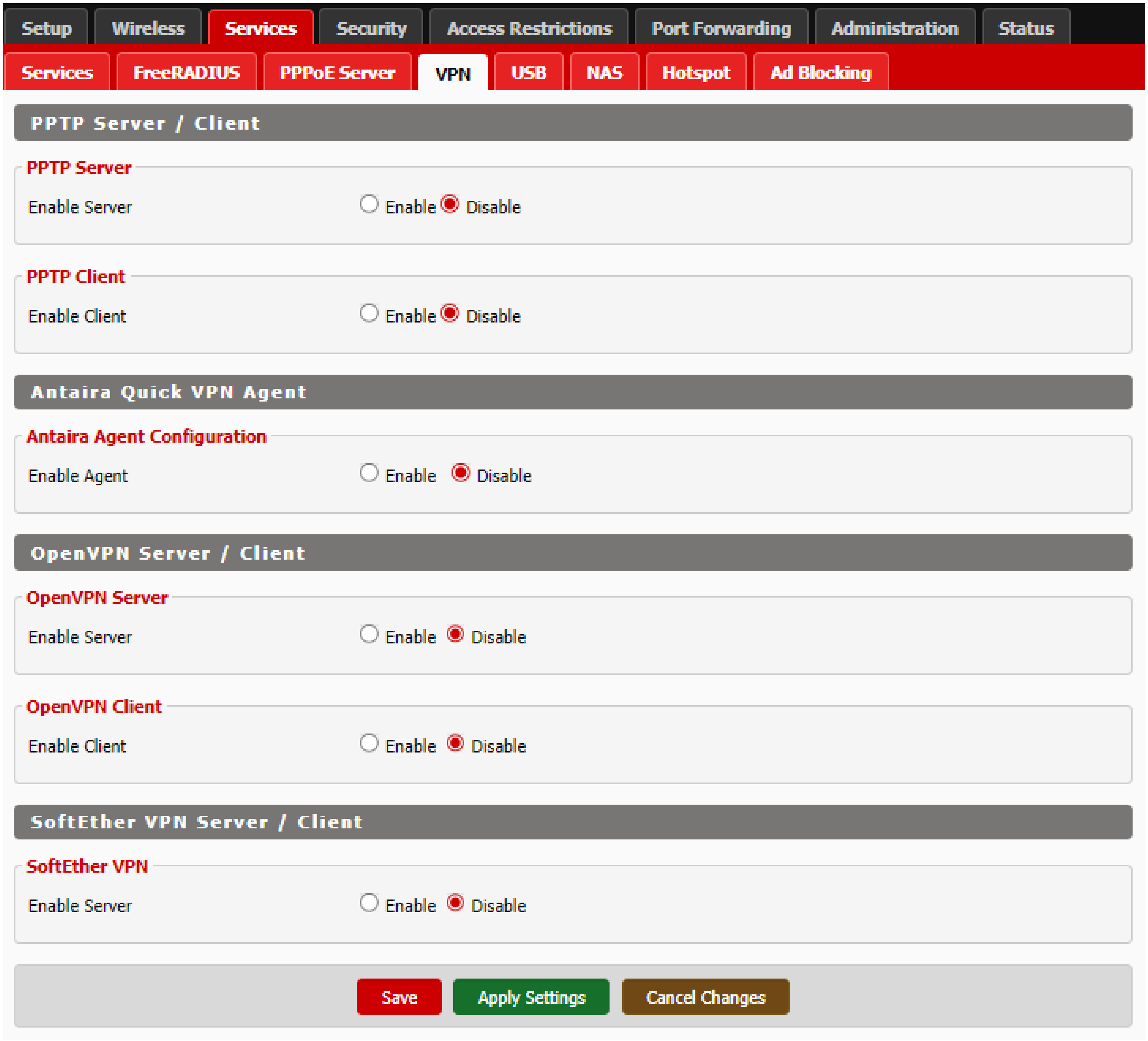
PPPoE Server	Description
RP-PPPoE Server Daemon	Enable or disable this feature.
RP-PPPoE Server Interface	Select the interface.

IP Range	Set the IP range.
Max Associated Clients	Set the maximum associated clients allowed.
Deflate Compression	Enable or disable this feature.
BSD Compression	Enable or disable this feature.
LZS Stac Compression	Enable or disable this feature.
MPPC Compression	Enable or disable this feature.
MPPE Encryption	Enable or disable this feature.
Session Limit per MAC	Set a session limit per MAC address. Default is 0.
LCP Echo Interval	Set the LCP Echo Interval. Default is 5.
LCP Echo Failure	Set the LCP Echo Failure. Default is 12.
Client Idle Time	
MTU/MRU	MTU/MRU should be set to equal. The default values are valid for Ethernet packet networks with an MTU of 1500Bytes. If you would like to use PPTP on other (WAN) connections, e.g. DSL, coax, fiber, etc, you will have to adjust the values to the correct settings. Default is 1436.
Authentication	Select an Authentication method.

4.4 VPN

Virtual Private Network (VPN) allows two LANs to create a secured virutal tunnel connection between each other over the Internet. Typically used to extend a private network across a public network.

Services > VPN



PPTP Server / Client

PPTP Server

Enable Server ○ Enable ● Disable

PPTP Client

Enable Client ○ Enable ● Disable

Antaira Quick VPN Agent

Antaira Agent Configuration

Enable Agent ○ Enable ● Disable

OpenVPN Server / Client

OpenVPN Server

Enable Server ○ Enable ● Disable

OpenVPN Client

Enable Client ○ Enable ● Disable

SoftEther VPN Server / Client

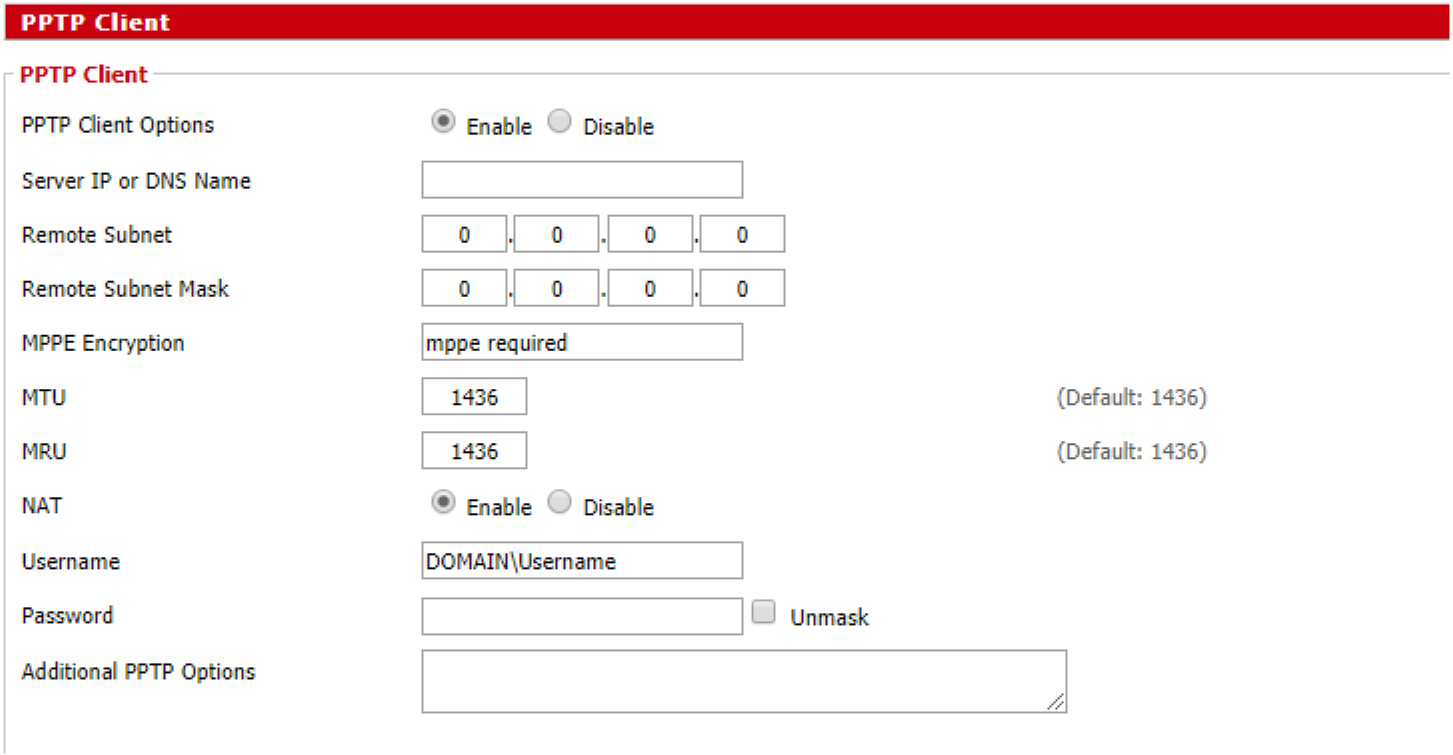
SoftEther VPN

Enable Server ○ Enable ● Disable

4.4.1 PPTP Server

A Point-To-Point Tunneling Protocol allows you to connect securely from a remote location (such as your home) to a LAN located in another location (workplace, business office, etc).

Services > VPN > PPTP Server



PPTP Client

PPTP Client

PPTP Client Options	● Enable ○ Disable
Server IP or DNS Name	
Remote Subnet	0 . 0 . 0 . 0
Remote Subnet Mask	0 . 0 . 0 . 0
MPPE Encryption	mppe required
MTU	1436 (Default: 1436)
MRU	1436 (Default: 1436)
NAT	● Enable ○ Disable
Username	DOMAIN\Username
Password	□ Unmask
Additional PPTP Options	

PPTP Server	Description
PPTP Server	Enable or disable PPTP Server option.
Broadcast Support	When **Disabled**, PPTP-Server does set *proxy-arp* which works for broadcasting in most cases. When **Enabled**, *bcrelay* will relay all broadcast messages to the default bridge network. This will increase cpu load. Disabled by default.
MPPE Encryption	Forces clients to use encryption with 128bit. When encryption is disabled, encryption to clients is allowed, but not forced.
DNS1 & 2	Add your local/WAN DNS Server. Setting DNS2 is optional.
WINS1 & 2	Add your local WINS server. This setting is optional.

MTU/MRU	MTU/MRU should be set to equal. The default values are valid for Ethernet packet networks with an MTU of 1500Bytes. If you would like to use PPTP on other (WAN) connections, e.g. DSL, coax, fiber, etc, you will have to adjust the values to the correct settings. Default is 1436.
Server IP	Enter a LAN IP Address *(An IP from your network that is not used by any device or the router)*. Example: *(Assuming the router's LAN address is 192.168.1.1)* Server IP = 192.168.1.2. The default port for pptp is 1723.
Client IP(s)	The client IP range. Leaving it blank will not work. *(Input in format like: 192.168.1.100-199)*. IPs in this range are given to clients trying to connect. This should be a valid IP address on the LAN segment of the network, and outside of the DHCP address range**.**
Max Associated Clients	Max allowed concurrent clients**.**
Authentication	RADIUS or CHAP Secrets.

4.4.2 PPTP Client

The PPTP Client configuration. These settings allow you to connect the router to a PPTP Server.

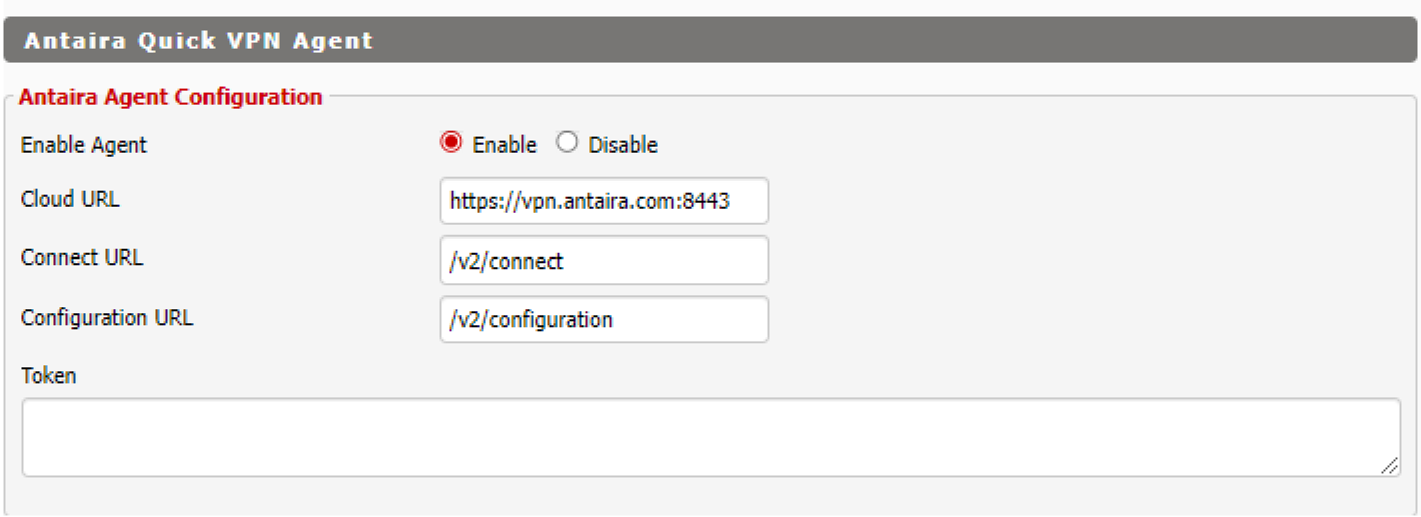
Services > VPN > PPTP Client

PPTP Client	**Description**
PPTP Client Options	Enable or disable PPTP Client options.
Server IP or DNS Name	The IP address of the VPN server.
Remote Subnet	Use the Network Address for the Remote Network *(10.20.1.0 for example)*.
Remote Subnet	Use the Subnet Mask appropriate for the

Mask	Remote Network *(255.255.255.0 for example)*.
MPPE Encryption	The type of security to use for the connection. If you are connecting to another router, you need *(Example: mppe required)*. But if you are connecting to a Windows VPN server you need *(Example: mppe required, no40, no56, stateless)* or *(Example: mppe required, no40, no56, stateful)*.
MTU/MRU	Needs to match the server's MTU/MRU settings.
NAT	Recommended to leave enabled.
Username	Your Remote PPTP Network Domain/Username. *(Example: YOURCOMPANY\\johndoe*)
Password	Your Remote PPTP Network Password.
Additional PPTP Options	Additional options for PPTP connections.

4.4.3 Antaira Quick VPN Agent

Antaira Technologies introduces Antaira ConnectVPN, a cloud-based VPN system designed to seamlessly connect remote devices using Antaira's wireless routers. This system streamlines configuration, monitoring, and data collection processes.



Antaira Quick VPN Agent

Antaira Agent Configuration

Enable Agent ● Enable ○ Disable

Cloud URL https://vpn.antaira.com:8443

Connect URL /v2/connect

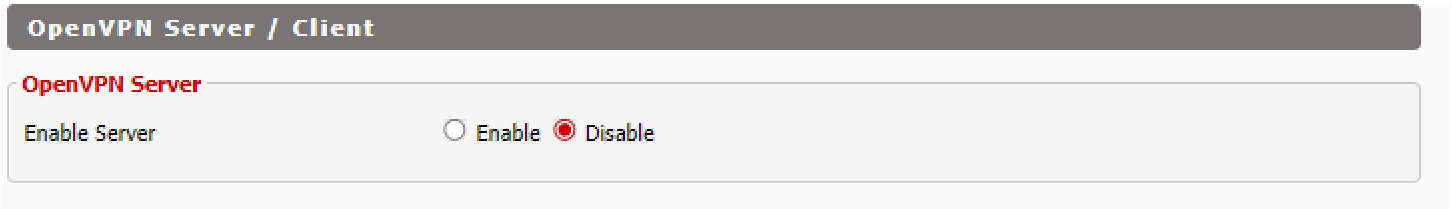
Configuration URL /v2/configuration

Token

4.4.4 OpenVPN Server

OpenVPN is a full-features SSL VPN solution which can accommodate a wide range of configurations. This page allows you to setup an OpenVPN Server.

Services > VPN > OpenVPN Server



OpenVPN Server / Client

OpenVPN Server

Enable Server ○ Enable ● Disable

OpenVPN	Description
OpenVPN	Start OpenVPN server/daemon service.
Start Type	Select System for start type.
Config as	Choose to configure via GUI or config file.
Server Mode	The mode of tunneling. **TUN**: Routing (layer 3) **TAP**: Bridging networks (Layer 2, can be used for routing, but not common)
Network	Network to use for the tunnel (Only in routing mode).
Netmask	Netmask of the network for the tunnel.
Port	The port which OpenVPN server listens on. Default is port 1194.
Tunnel Protocol	The sub-protocol the connection will use. Default is UDP.
Encryption Cipher	The encryption algorithm that will be used for the tunnel. Blowfish: fastest to AES512: safest.
Hash Algorithm	The hash algorithm that will be used. MD4: fastest to SHA512.
Advanced Options	Refer to the Advanced Options table below.
Public Server Cert	Server certificate issued by CA for this particular router (usually server.crt). Only part between 'BEGIN' and 'END' is required.

CA Cert	Certificate of OpenVPN CA in pem form (usually ca.crt). Only part between (and including) -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- is necessary.
Private Server Key	Key associated with Public Server Cert (usually server.key). This should be kept secret as anyone with this key can successfully authenticate client certificates.
DH PEM	Diffie Hellman parameters generated for the OpenVPN server (usually dh1024.pem).
Additional Config	Any additional configurations you want to define for the VPN connection.
TLS Auth Key	The static key OpenVPN should use for generating HMAC send/receive Keys.
Certificate Revoke List	Enter certificates to be revoked, if desired.

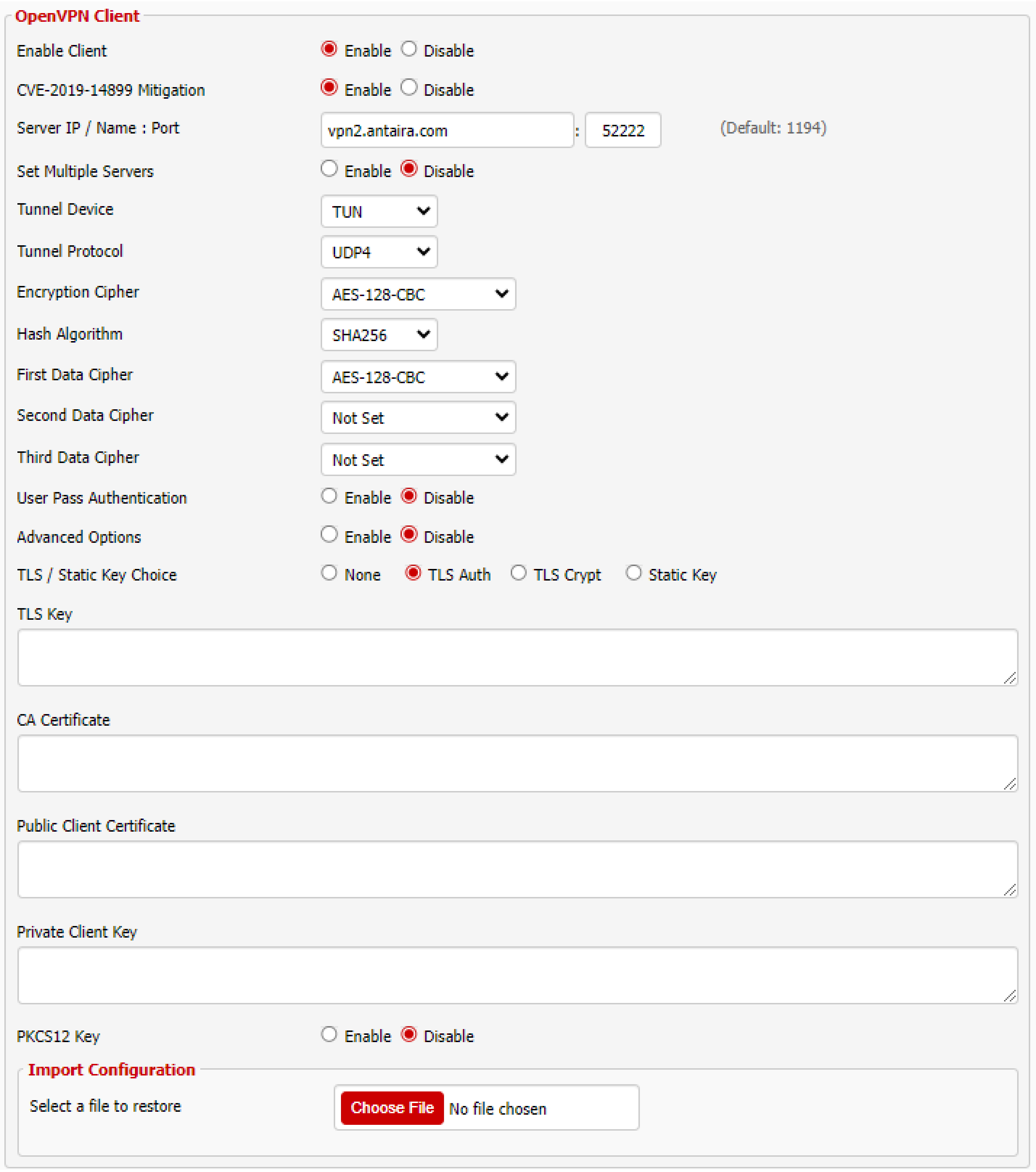
Advanced Options (Server Side)	**Description**
TLS Cipher	What encryption algorithm OpenVPN should use for encrypting its control channel. Default is disabled.
LZO Compression	Enables compression over VPN. This may speed up the connection.
Redirect Default Gateway	Force the clients to use the tunnel as the default gateway. Default is disabled.
Allow Client to Client	Allows clients to see each other. Default is disabled.
Allow Duplicate cn	Allow the use of one client certification for multiple clients. (This poses a security risk of sharing certifications). Default is disabled.
Tunnel MTU	Set the mtu of the tunnel. Default is 1500.

Setting	
Tunnel UDP Fragment	Set mss-fix and fragmentation across the tunnel.
Tunnel UDP MSS-Fix	Equal to value of Fragment. Only used with udp. Should be set on one side of the connection only.
CCD-Dir DEFAULT File	Enter CCD-dir default file here.
Client Connect Script	Enter a client connect script here.
Static Key	Enter the static key here.
PKCS12 Key	Used for peer-to-peer links. No pki needed.

4.4.5 OpenVPN Client

OpenVPN is a full-features SSL VPN solution which can accommodate a wide range of configurations. This page allows you to setup the router as an OpenVPN Client.

Services > VPN > OpenVPN Client



OpenVPN Client

Enable Client	● Enable ○ Disable
CVE-2019-14899 Mitigation	● Enable ○ Disable
Server IP / Name : Port	vpn2.antaira.com : 52222 (Default: 1194)
Set Multiple Servers	○ Enable ● Disable
Tunnel Device	TUN
Tunnel Protocol	UDP4
Encryption Cipher	AES-128-CBC
Hash Algorithm	SHA256
First Data Cipher	AES-128-CBC
Second Data Cipher	Not Set
Third Data Cipher	Not Set
User Pass Authentication	○ Enable ● Disable
Advanced Options	○ Enable ● Disable
TLS / Static Key Choice	○ None ● TLS Auth ○ TLS Crypt ○ Static Key

TLS Key

CA Certificate

Public Client Certificate

Private Client Key

PKCS12 Key	○ Enable ● Disable

Import Configuration

Select a file to restore	Choose File No file chosen

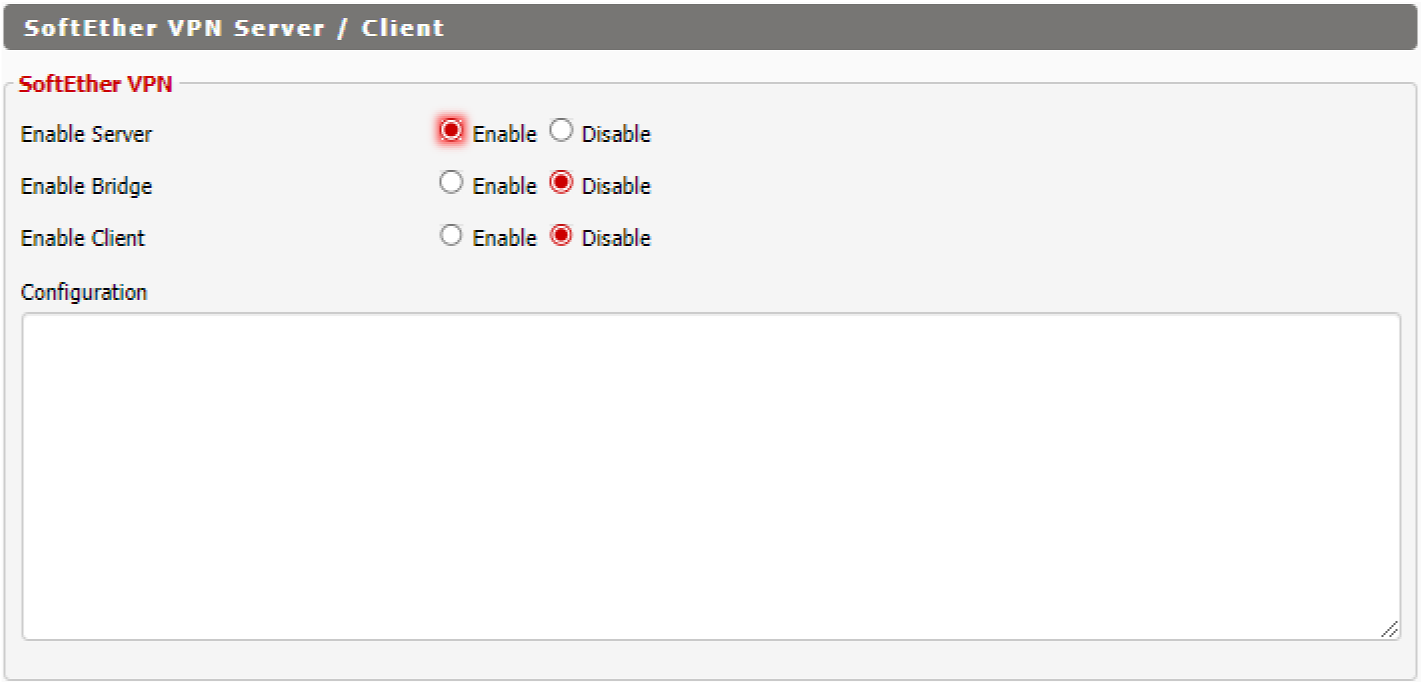
OpenVPN	Description
Start OpenVPN Client	Enable or disable OpenVPN client options.
Server IP/Name	IP address/hostname of the OpenVPN server you wish to connect to.
Port	The port which OpenVPN server is listening on. Default is port 1194.
Tunnel Device	The mode of tunneling. **TUN**: Routing (layer 3). **TAP**: Bridging (layer 2, can be used for routing, but not common).
Tunnel Protocol	The sub-protocol the connection will use. Default is UDP.
Encryption Cipher	The encryption algorithm that will be used for the tunnel. Blowfish is fastest, while AES512 is safest.
Hash Algorithm	The hash algorithm that will be used. MD4: fastest to SHA512.
User Pass Authentication	Enable or Disable this feature.
Advanced Options	Refer to the Advanced Options table below.
CA Cert	CA certificate. Only part between ‘BEGIN’ and ‘END’ is required.
Public Client Cert	Client certificate issued by CA.
Private Client Key	Key associated with the Public Client Cert. This should be kept secret because anyone with this key can successfully authenticate as this client.

Advanced Options (Client Side)	Description
TLS Cipher	What encryption algorithm OpenVPN should use for encrypting its control channel. Default is disabled.
LZO Compression	Enables compression over VPN. This may speed up the connection. Must be the same value as the server.
NAT	Enables network address translation on the client side of the connection. Enabling it gives you the Firewall Protection option. Default is disabled.
IP Address	Enter an IP address in case you do not get an IP address from the server. Not very common.
Subnet Mask	Subnet mask for the IP address above.
Tunnel MTU Setting	Set the mtu of the tunnel. Default is 1500.
Tunnel UDP Fragment	Set mss-fix and fragmentation across the tunnel.
Tunnel UDP MSS-Fix	Equal to value of Fragment. Only used with udp. Should be set on one side of the connection only.
neCertType Verification	Checks to see if the remote server is using a valid type of certificate meant for OpenVPN connections.
TLS Auth Key	The static key OpenVPN should use for generating HMAC send/receive keys.
Additional Config	Any additional configurations you want to define for the VPN connection.
Policy Based Routing	Allow only special clients to use the tunnel. Add IP address in the form of: 0.0.0.0/0 to force clients to use the tunnel as the default gateway. Type one IP per line.
PKCS12 Key	Enter the PKCS12 key here.
Static Key	Used for peer-to-peer links. No pki needed.

4.4.5 SoftEther VPN

An alternative VPN service to OpenVPN.

Services > VPN > SoftEther VPN



SoftEther VPN Server / Client

SoftEther VPN

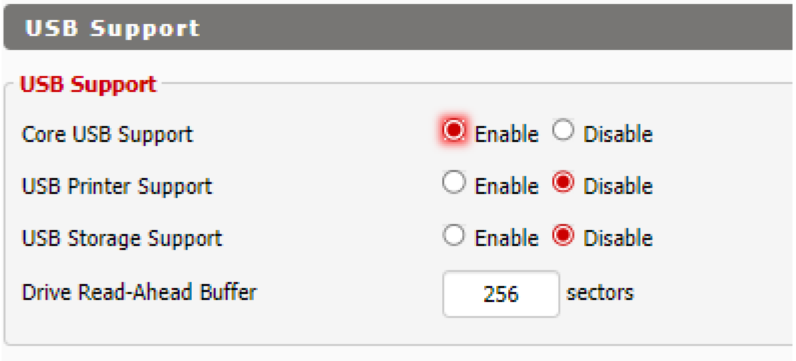
Enable Server ● Enable ○ Disable

Enable Bridge ○ Enable ● Disable

Enable Client ○ Enable ● Disable

Configuration

4.5 USB



USB Support

USB Support

Core USB Support ● Enable ○ Disable

USB Printer Support ○ Enable ● Disable

USB Storage Support ○ Enable ● Disable

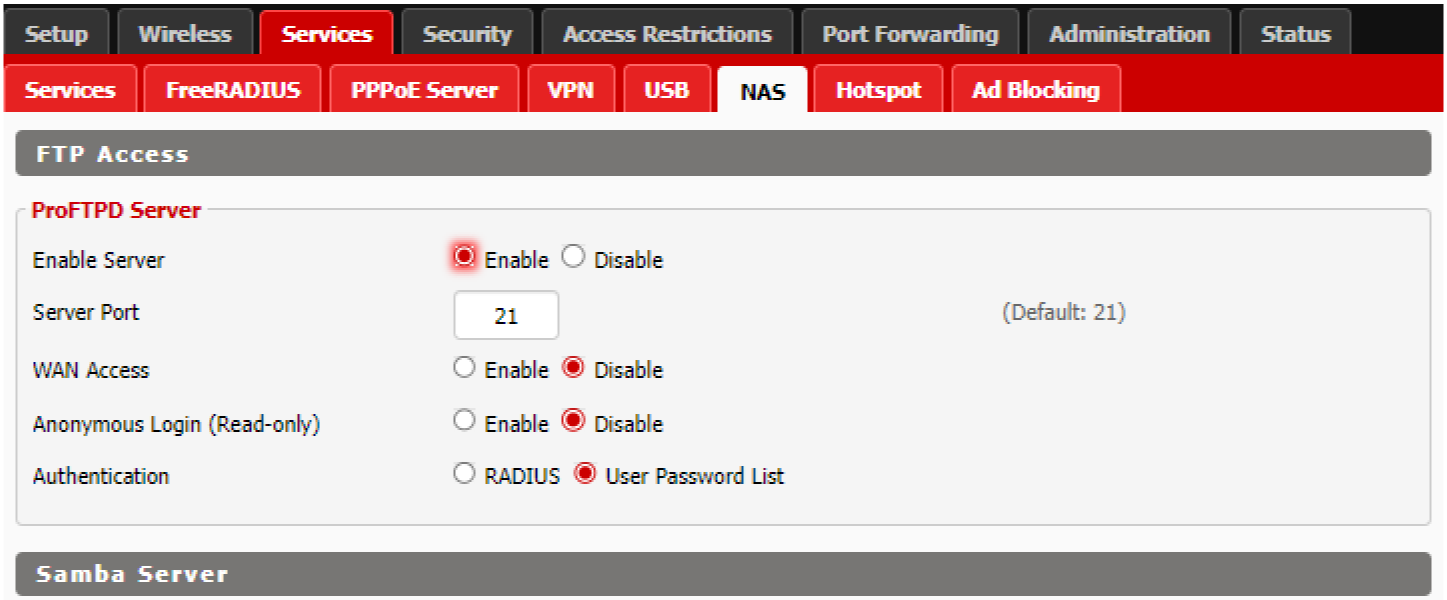
Drive Read-Ahead Buffer 256 sectors

USB	Description
Core USB Support	Enable or disable USB support.
USB Printer	Enable or disable printer support.

Support	
USB Storage Support	Enable or disable support for external drives.
USB Over IP	Enable or disable USB over IP.
Automatic Drive Mount	Auto mount connected drives.
Use SES Button to Remove drives	Use SES Button to un-mount drives before disconnecting them.
Disk Info	Displays disk info e.g. partition size, volume name if set, as well as UUID for all connected drives.

4.6 NAS

4.6.1 FTP Server



FTP Access

ProFTPD Server

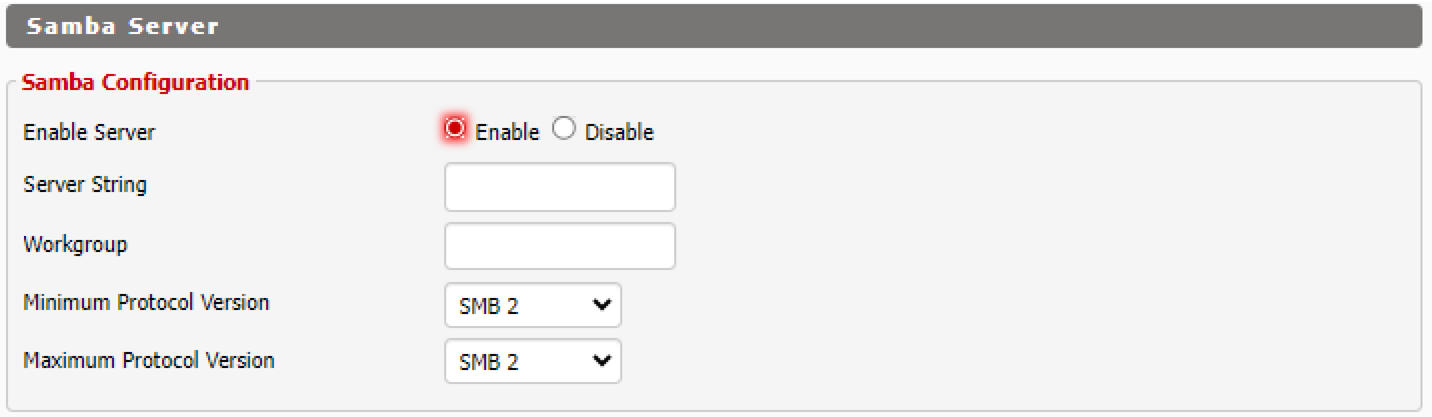
Enable Server	● Enable ○ Disable
Server Port	21 (Default: 21)
WAN Access	○ Enable ● Disable
Anonymous Login (Read-only)	○ Enable ● Disable
Authentication	○ RADIUS ● User Password List

Samba Server

FTP	Description
ProFTPD	Enable or disable ProFTPD services.
Server Port	Enter a server port number.
WAN Access	Enable or disable WAN access.
Anonymous Login	Enable or disable anonymous login.
Anonymous Home Directory	Enter a home directory.

Authentication	Select between Radius or User Password List for authentication.

4.6.2 Samba Server



Samba Server

Samba Configuration

Enable Server ● Enable ○ Disable

Server String

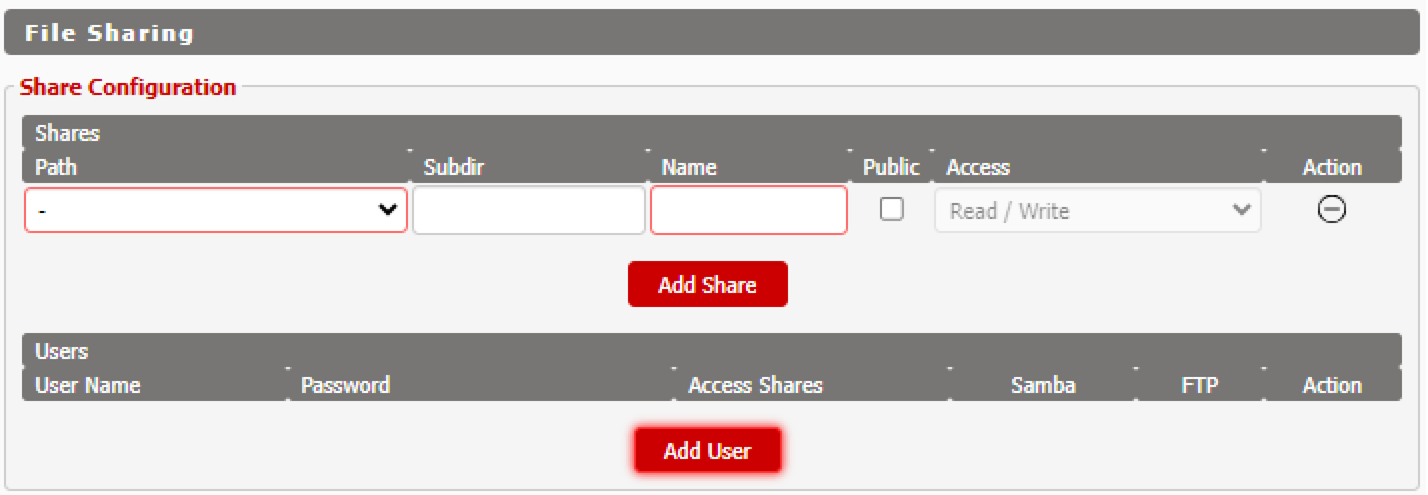
Workgroup

Minimum Protocol Version SMB 2

Maximum Protocol Version SMB 2

Samba	Description
Samba	Enable or disable Samba server services.
Server String	Enter a server string.
Workgroup	Enable a workgroup.
Minimum Protocol Version	Select a minimum protocol version.
Maximum Protocol Version	Select a maximum protocol version.

4.6.3 File Sharing



File Sharing

Share Configuration

Shares

Path	Subdir	Name	Public	Access	Action
-			□	Read / Write	⊖

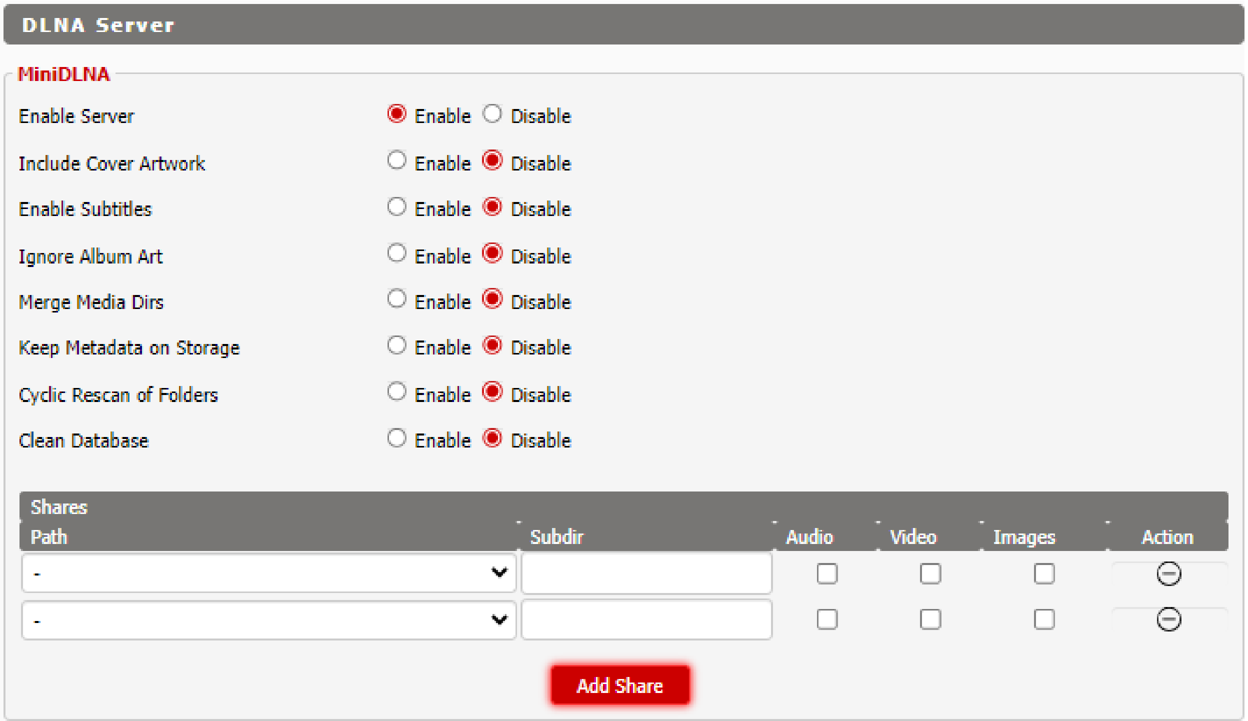
Add Share

Users

User Name	Password	Access Shares	Samba	FTP	Action

Add User

4.6.4 DLNA Server



DLNA Server

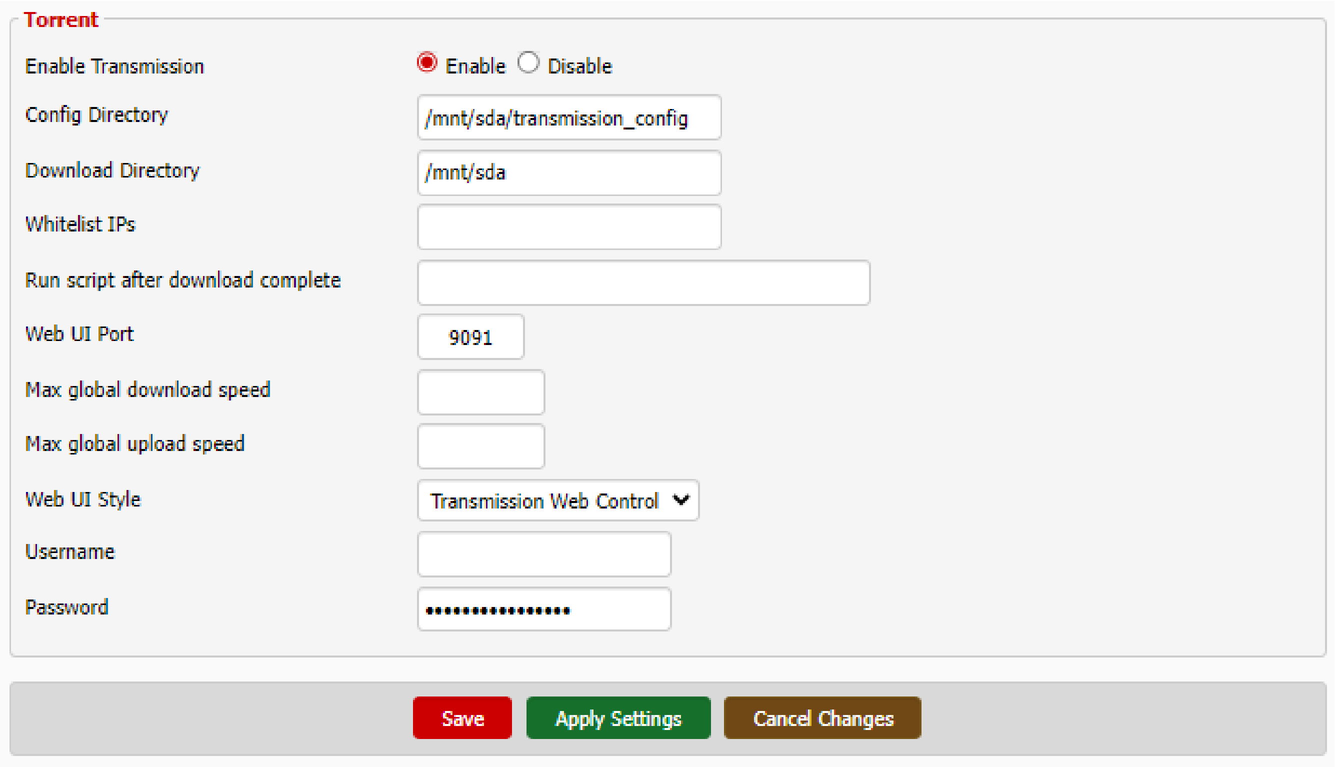
MiniDLNA

Enable Server	● Enable ○ Disable
Include Cover Artwork	○ Enable ● Disable
Enable Subtitles	○ Enable ● Disable
Ignore Album Art	○ Enable ● Disable
Merge Media Dirs	○ Enable ● Disable
Keep Metadata on Storage	○ Enable ● Disable
Cyclic Rescan of Folders	○ Enable ● Disable
Clean Database	○ Enable ● Disable

Shares

Path	Subdir	Audio	Video	Images	Action
-		□	□	□	⊖
-		□	□	□	⊖

4.6.5 Torrent

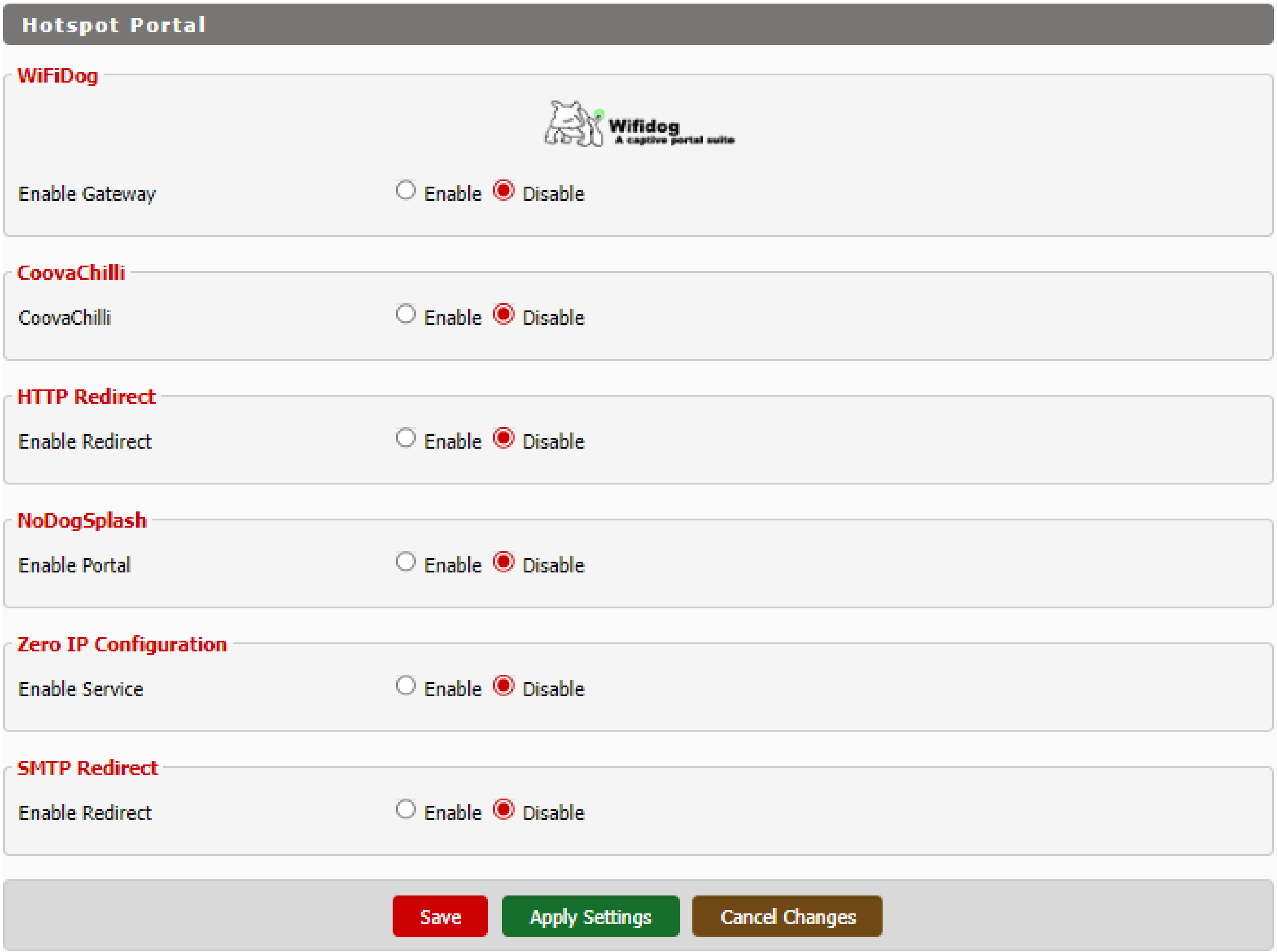


Torrent

Enable Transmission	● Enable ○ Disable
Config Directory	/mnt/sda/transmission_config
Download Directory	/mnt/sda
Whitelist IPs	
Run script after download complete	
Web UI Port	9091
Max global download speed	
Max global upload speed	
Web UI Style	Transmission Web Control
Username	
Password	•••••••••••••••

4.7 Hotspot

You can use the router as a Hotspot gateway with authentication and accounting. (Radius). ChilliSpot is an open source captive portal or wireless LAN access point controller. It is used for authenticating users of a wireless LAN. It supports web-based login which is today's standard for public hotspots and it supports WPA.



Hotspot Portal

WiFiDog

Enable Gateway ○ Enable ● Disable

CoovaChilli

CoovaChilli ○ Enable ● Disable

HTTP Redirect

Enable Redirect ○ Enable ● Disable

NoDogSplash

Enable Portal ○ Enable ● Disable

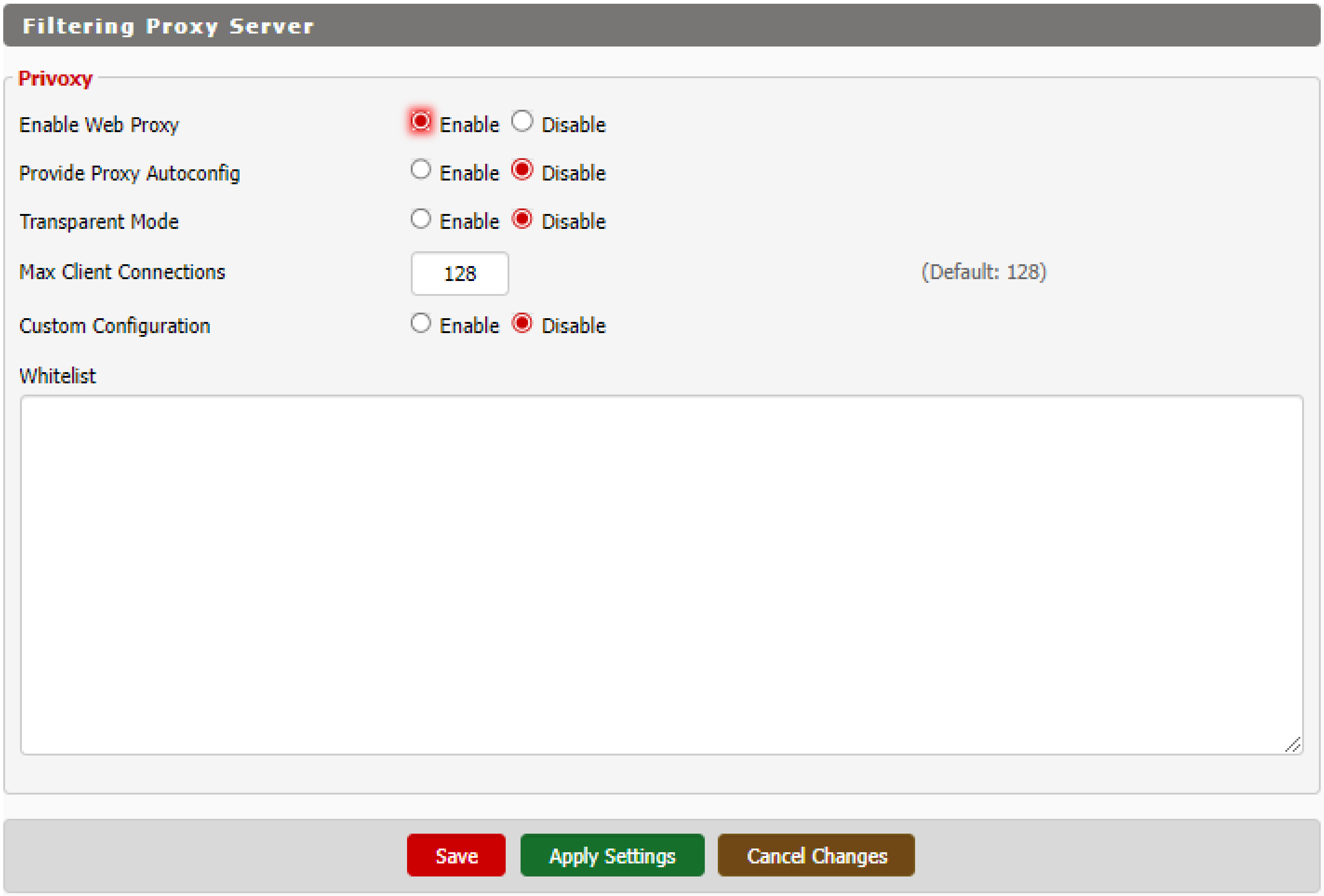
Zero IP Configuration

Enable Service ○ Enable ● Disable

SMTP Redirect

Enable Redirect ○ Enable ● Disable

4.8 Adblocking



Filtering Proxy Server

Privoxy

Enable Web Proxy	● Enable ○ Disable
Provide Proxy Autoconfig	○ Enable ● Disable
Transparent Mode	○ Enable ● Disable
Max Client Connections	128 (Default: 128)
Custom Configuration	○ Enable ● Disable

Whitelist

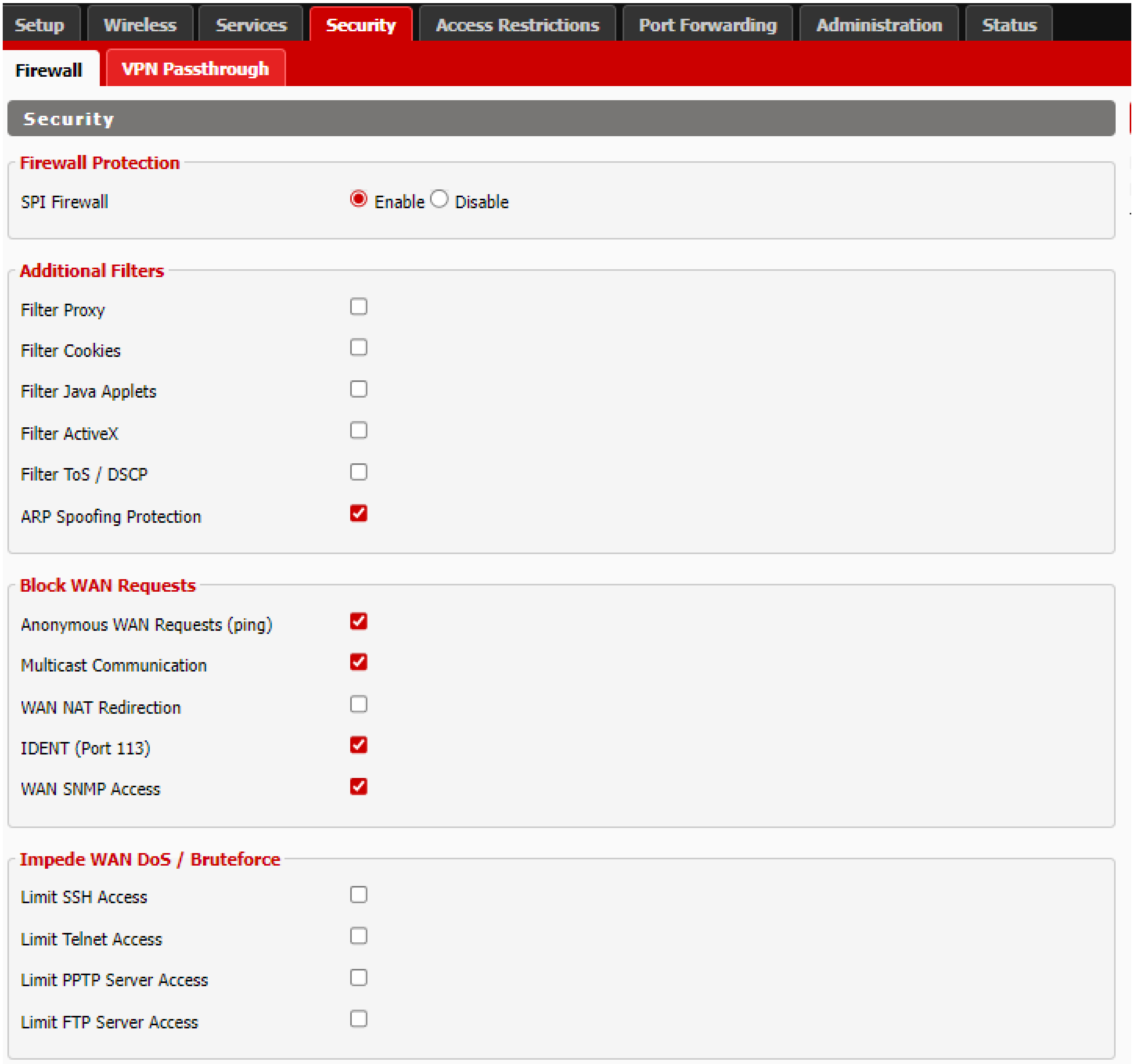
Adblocking	Description
Privoxy	Enables you to filter common ads.
Provide Proxy Autoconfig	Publishes a WPAD/PAC file that clients use to automatically setup proxy details.
Transparent Mode	Traffic to port 80 is intercepted by Privoxy even if the client did not configure any proxy settings, thus allowing you to enforce filtering. Transparent mode cannot intercept HTTPS connections. All HTTPS traffic will not be filtered by Privoxy unless added to the autconfig.
Exclude IP	Exclude an IP address.
Custom Configuration	Allows you to specify custom settings and paths to custom filters on external media. e.g. A USB.
Whitelist	Enter items to be whitelisted from the filter.

5. Security

5.1 Firewall

5.1.1 Security

The purpose of the Firewall is to moderate traffic and/or log it.



Security

Firewall Protection

SPI Firewall ● Enable ○ Disable

Additional Filters

Filter Proxy □
Filter Cookies □
Filter Java Applets □
Filter ActiveX □
Filter ToS / DSCP □
ARP Spoofing Protection ☑

Block WAN Requests

Anonymous WAN Requests (ping) ☑
Multicast Communication ☑
WAN NAT Redirection □
IDENT (Port 113) ☑
WAN SNMP Access ☑

Impede WAN DoS / Bruteforce

Limit SSH Access □
Limit Telnet Access □
Limit PPTP Server Access □
Limit FTP Server Access □

Additional Filters	Description
SPI Firewall	Enable or disable the SPI Firewall.
Filter Proxy	Blocks HTTP requests containing the “Host:” string.
Filter Cookies	Identifies HTTP requests that contain the “Cookie:” string and mangle the cookie. Attempts to stop cookies from being used.
Filter Java Applets	Blocks HTTP requests containing a URL ending in “.js” or “.class”.
Filter ActiveX	Blocks HTTP requests containing a URL ending in “.ocx” or “.cab”.
ARP Spoofing Protection	Enable protection against ARP spoofing.

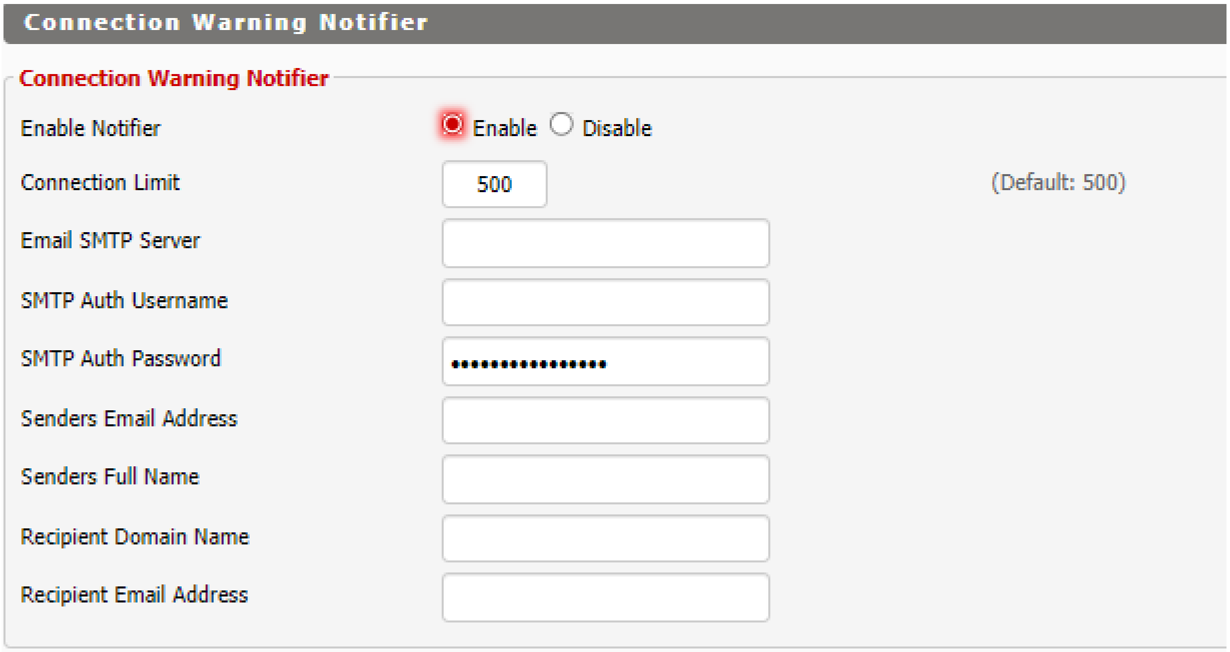
Block WAN Requests	Description
Anonymous WAN Requests (ping)	Stops the router from responding to pings from the WAN.
Multicast Communication	Prevents multicast packets from reaching the LAN.
WAN NAT Redirection	Prevents hosts on the LAN from using WAN address of the router to contact servers on the LAN which may have been configured using port redirection.
IDENT (port 113)	Prevents WAN access to port 113.
WAN SNMP Access	Prevents the WAN from reaching SNMP.

Impede WAN DoS/Bruteforce	Description
Limit SSH Access	Enable or disable this feature.
Limit Telnet Access	Enable or disable this feature.
Limit PPTP Server Access	Enable or disable this feature.

Limit FTP Server Access	Enable or disable this feature.

5.1.2 Connection Warning Notifier

Set a connection limit to the router. If the limit is exceeded, you can configure an SMTP alert to be sent.



Connection Warning Notifier

Connection Warning Notifier

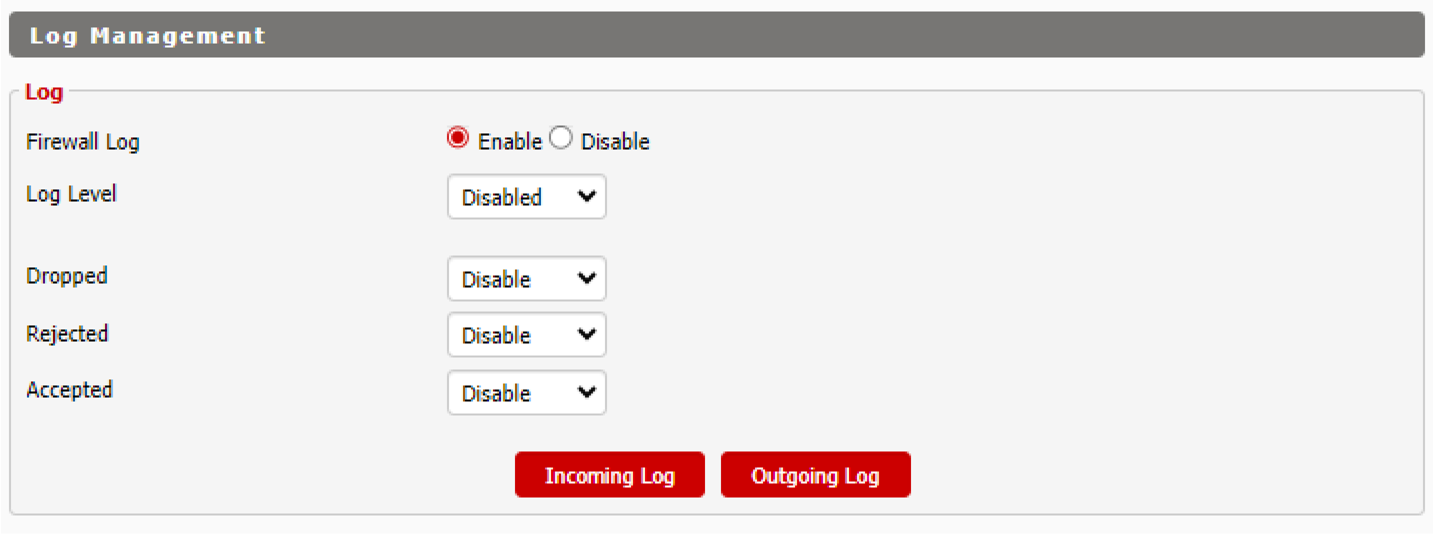
Enable Notifier	● Enable ○ Disable	
Connection Limit	500	(Default: 500)
Email SMTP Server		
SMTP Auth Username		
SMTP Auth Password	••••••••••••••••	
Senders Email Address		
Senders Full Name		
Recipient Domain Name		
Recipient Email Address		

Connection Warning Notifier	Description
Warning Notifier	Enable or disable the Warning Notifier feature.
Connection Limit	Limit amount of connections. Default is 500.
Email SMTP Server	Email SMTP server.
SMTP Auth Username	The SMTP username.
SMTP Auth Password	The SMTP password.
Senders Email Address	The sender’s email address.
Senders Full Name	The sender’s name.
Recipient Domain Name	Enter recipient’s domain name.

Recipient Email Address	Enter recipient's email address.

5.1.3 Log Management

The router can keep logs of all incoming or outgoing traffic for Internet connections.



Firewall Log ● Enable ○ Disable

Log Level: Disabled

Dropped: Disable

Rejected: Disable

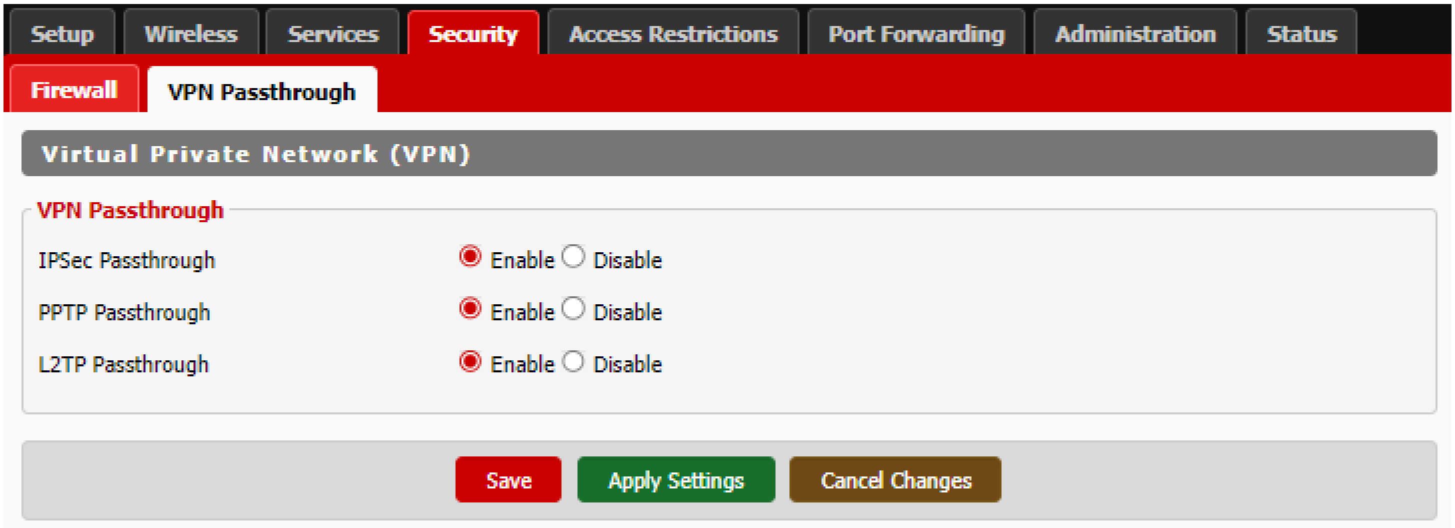
Accepted: Disable

Log Management	Description
Log	To keep activity logs, select Enable.
Log Level	Set this to the required amount of information. Set Log Level higher to log more actions.
Dropped	Log Dropped items
Rejected	Log Rejected items
Accepted	Log Accepted items.

Incoming Log:
To see a temporary log of the router's most recent incoming traffic, click the Incoming Log button.
Outgoing Log:
To see a temporary log of the router's most recent outgoing traffic, click the Outgoing Log button.

5.2 VPN Passthrough

The router allows you to run VPN services on your network.



VPN Passthrough

IPSec Passthrough ● Enable ○ Disable

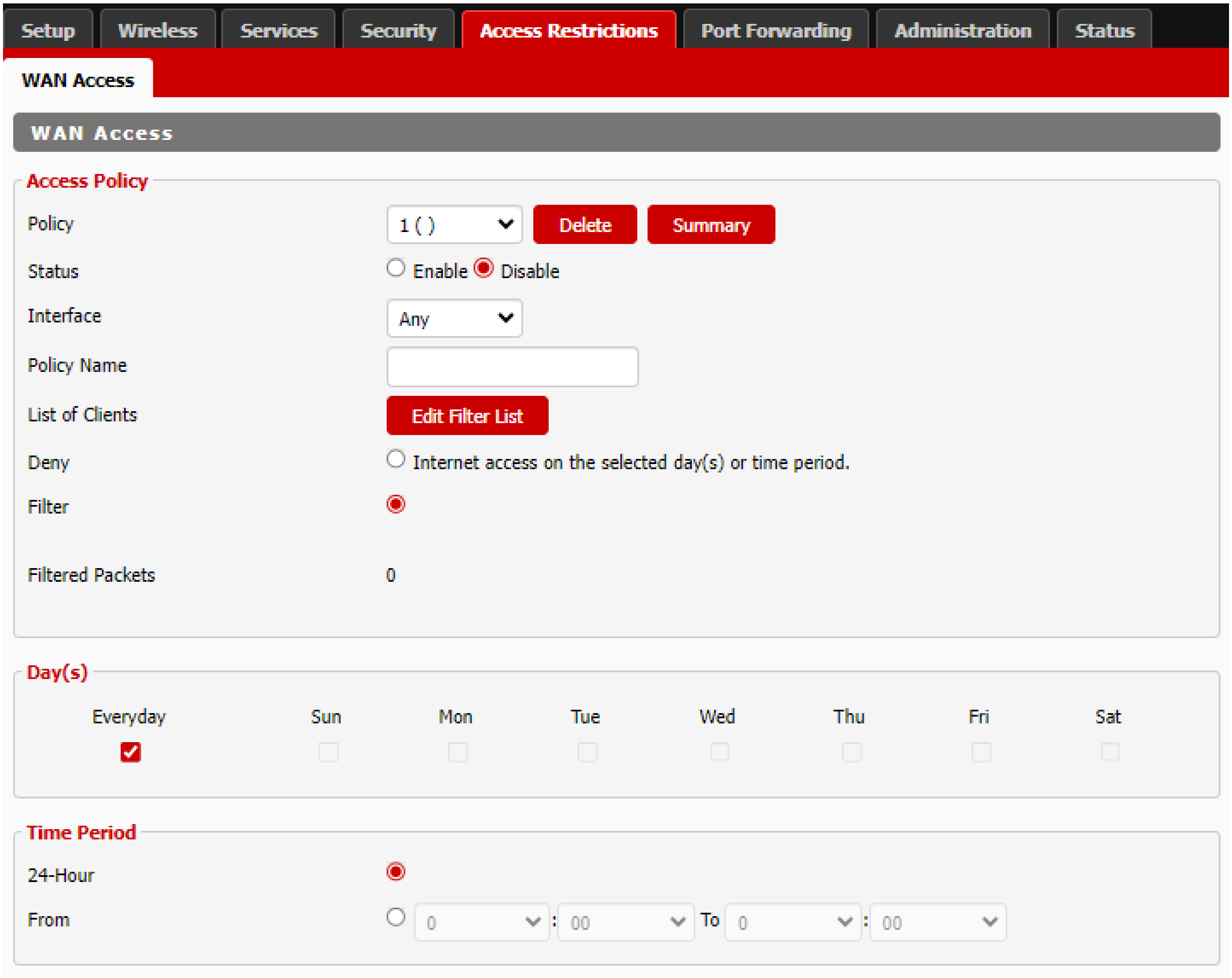
PPTP Passthrough ● Enable ○ Disable

L2TP Passthrough ● Enable ○ Disable

VPN Passthrough	Description
IPSec Passthrough	Allow IPSec.
PPTP Passthrough	Allow PPTP.
L2TP Passthrough	Allow P2TP.

6. Access Restrictions

6.1 WAN Access



WAN Access

Access Policy

Policy: 1 ( )

Status: ○ Enable ● Disable

Interface: Any

Policy Name:

List of Clients

Deny: ○ Internet access on the selected day(s) or time period.

Filter: ●

Filtered Packets: 0

Day(s)

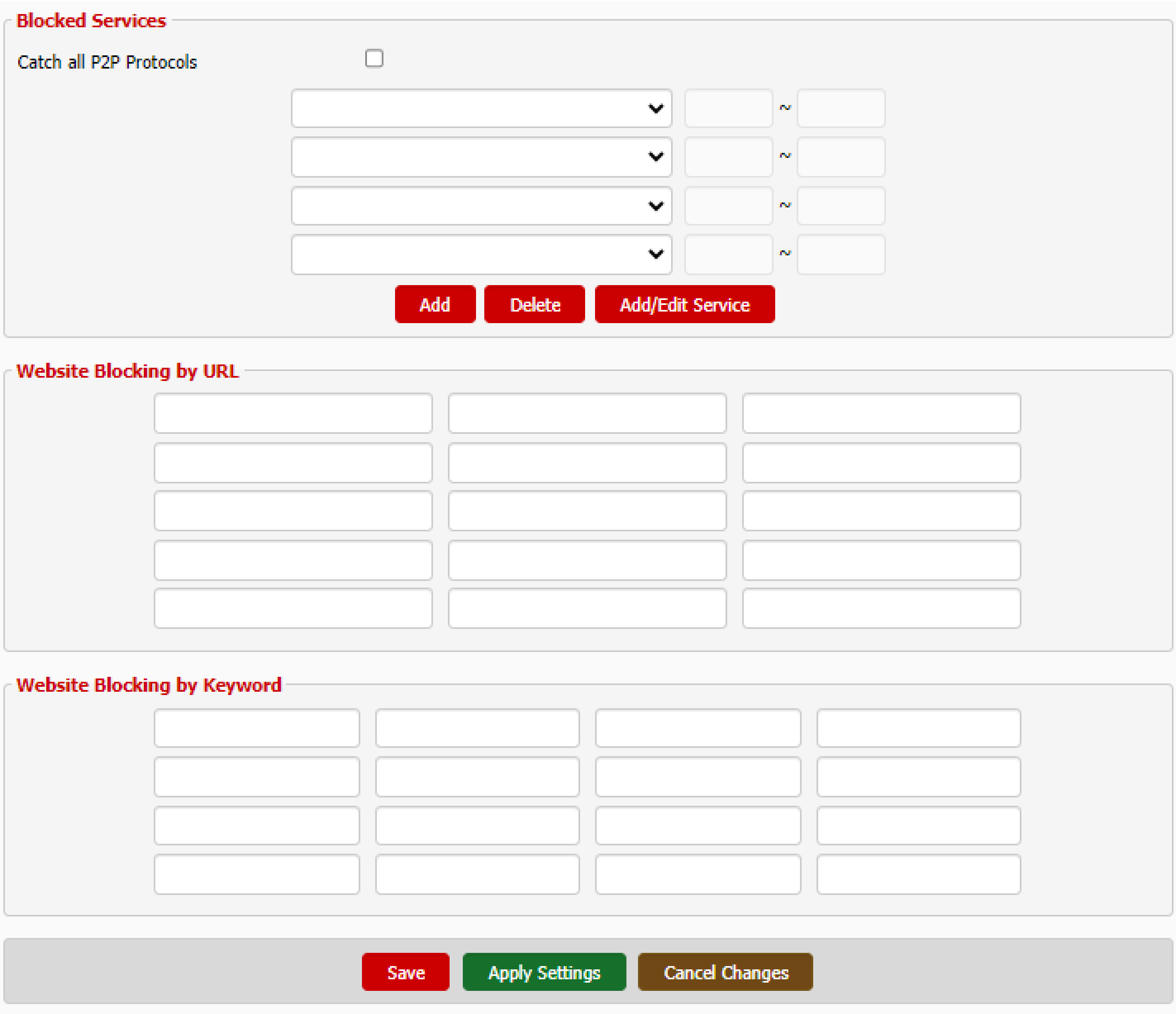
Everyday	Sun	Mon	Tue	Wed	Thu	Fri	Sat
☑	□	□	□	□	□	□	□

Time Period

24-Hour: ●

From: ○ 0 : 00 To 0 : 00

Access Policy	Description
Policy	Select a policy number to use.
Status	Enable or disable this particular policy.
Interface	Select an interface that this policy will affect.
Policy Name	Enter a name for the policy.
PC's	Specify clients by IP address or MAC address to Filter or Deny.

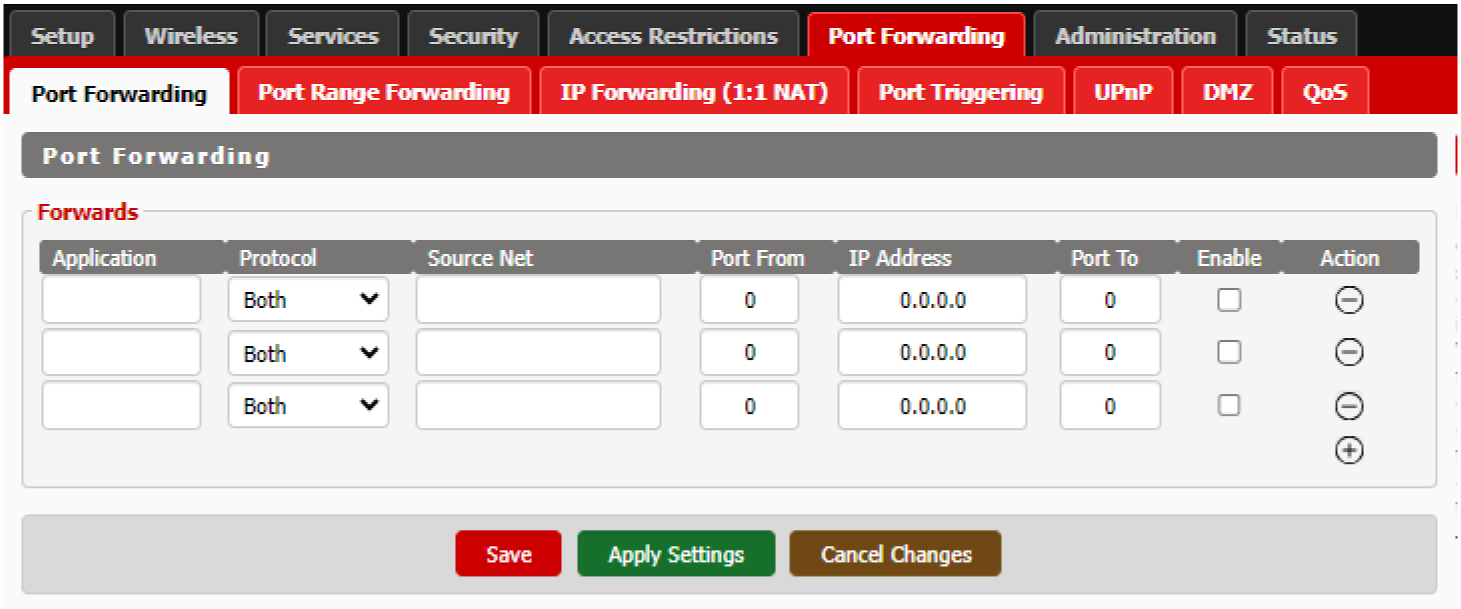


Catch all P2P Protocols □

7. Port Forwarding

7.1 Port Forwarding

Port Forwarding allows you to set up public services on your network, such as a web server, FTP server, or other specialized Internet applications. Any PC whose port is being forwarded must have a static IP address assigned.



Port Forwarding

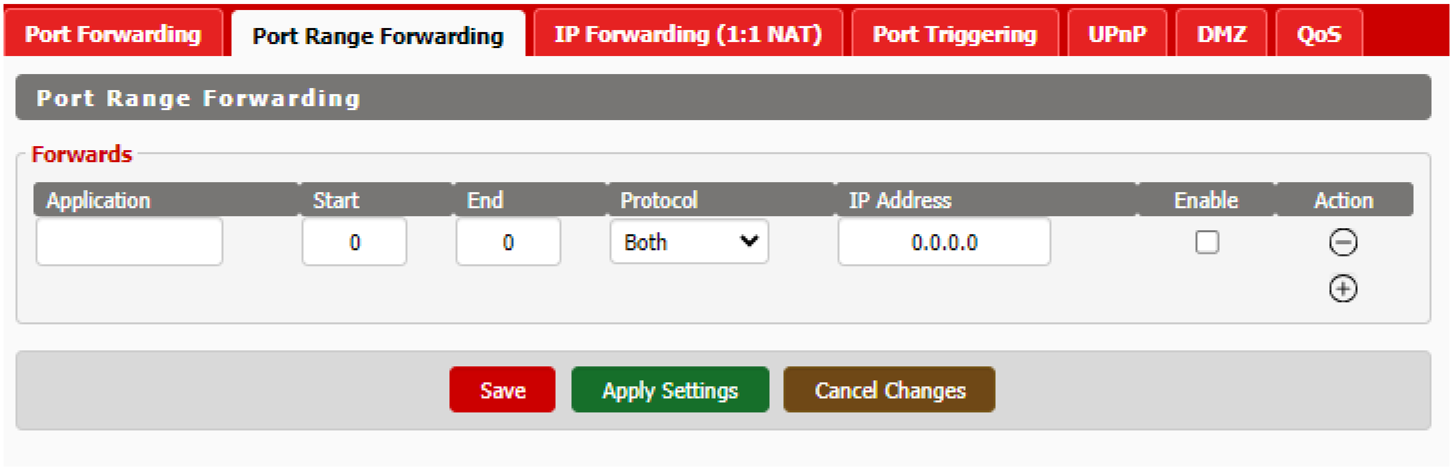
Forwards

Application	Protocol	Source Net	Port From	IP Address	Port To	Enable	Action
	Both		0	0.0.0.0	0	□	⊖
	Both		0	0.0.0.0	0	□	⊖
	Both		0	0.0.0.0	0	□	⊖
							⊕

Port Forwarding	Description
Application	Enter the name of the application in the file provided.
Protocol	Choose the right protocol TCP, UDP, or Both. Set this to what the application requires.
Source Net	Forward only if sender matches this IP/Net (example: 192.168.1.0/24).
Port From	Enter the number of the external port (the port number seen by users on the Internet).
IP Address	Enter the IP address of the PC running the application.
Port To	Enter the number of the internal port (the port number used by the application).
Enable	Enable port forwarding for the application.

7.2 Port Range Forwarding

Port Range Forwarding allows you to set up public services on your network, such as a web server, FTP server, or other specialized Internet applications. Any PC whose port is being forwarded must have a static IP address assigned.

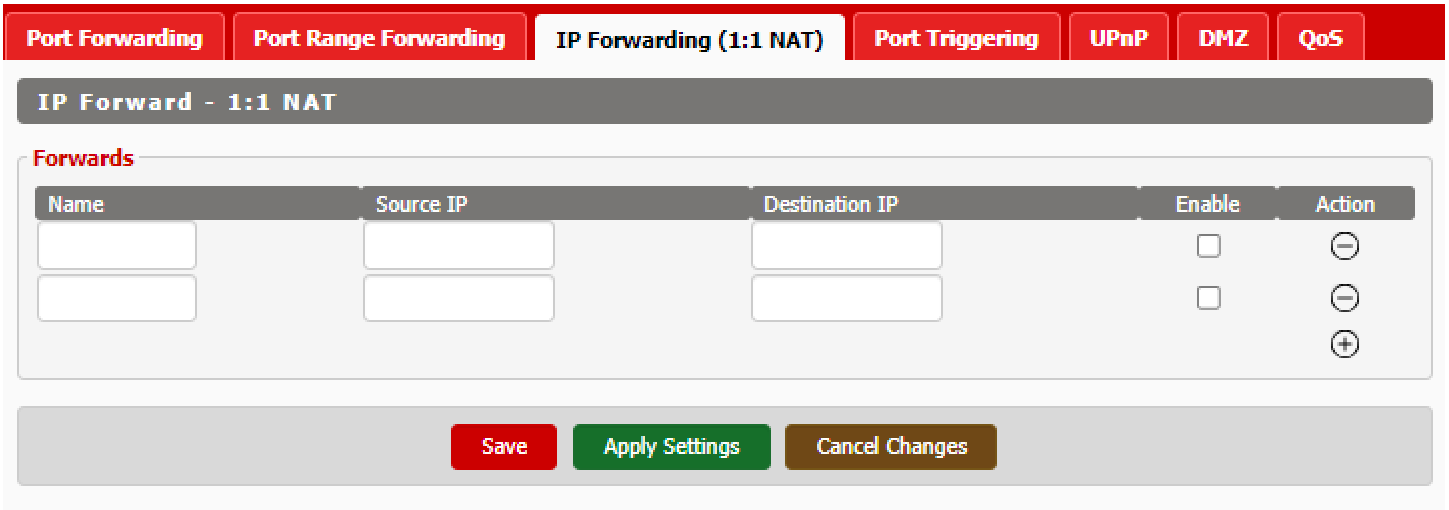


Application	Start	End	Protocol	IP Address	Enable	Action
	0	0	Both	0.0.0.0	□	⊖ ⊕

Port Range Forwarding	Description
Application	Enter the name of the application in the field provided.
Start	Enter the number of the first port of the range you want to be seen by users on the Internet and forwarded.
End	Enter the number of the last port of the range you want forwarded.
Protocol	Choose the right protocol TCP, UDP, or Both. Set this to what the application requires.
IP Address	Enter the IP address of the PC running the application.
Enable	Enable port forwarding for the application.

7.3 IP Forwarding (1:1 NAT)

Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the router will route the data to the device you specify. Due to security concerns, you may want to limit port forwarding to only those ports you are using, and uncheck the Enable checkbox after you are finished.



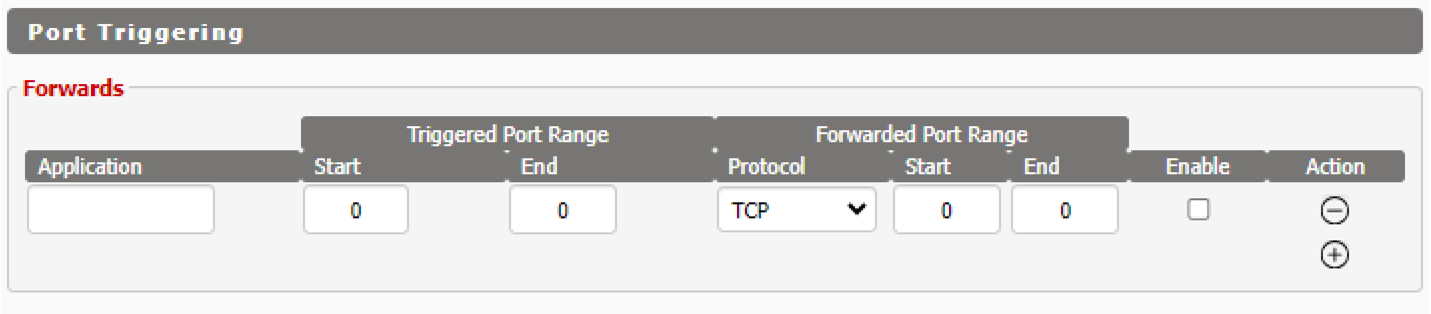
IP Forward - 1:1 NAT

Forwards

Name	Source IP	Destination IP	Enable	Action
			□	⊖
			□	⊖
				⊕

7.4 Port Triggering

Port triggering is a configuration option on a NAT-enabled router which allows a host machine to dynamically and automatically forward a specific port back to itself. Port triggering opens an incoming port when your computer is using a specifed outgoing port for specific traffic.



Port Triggering

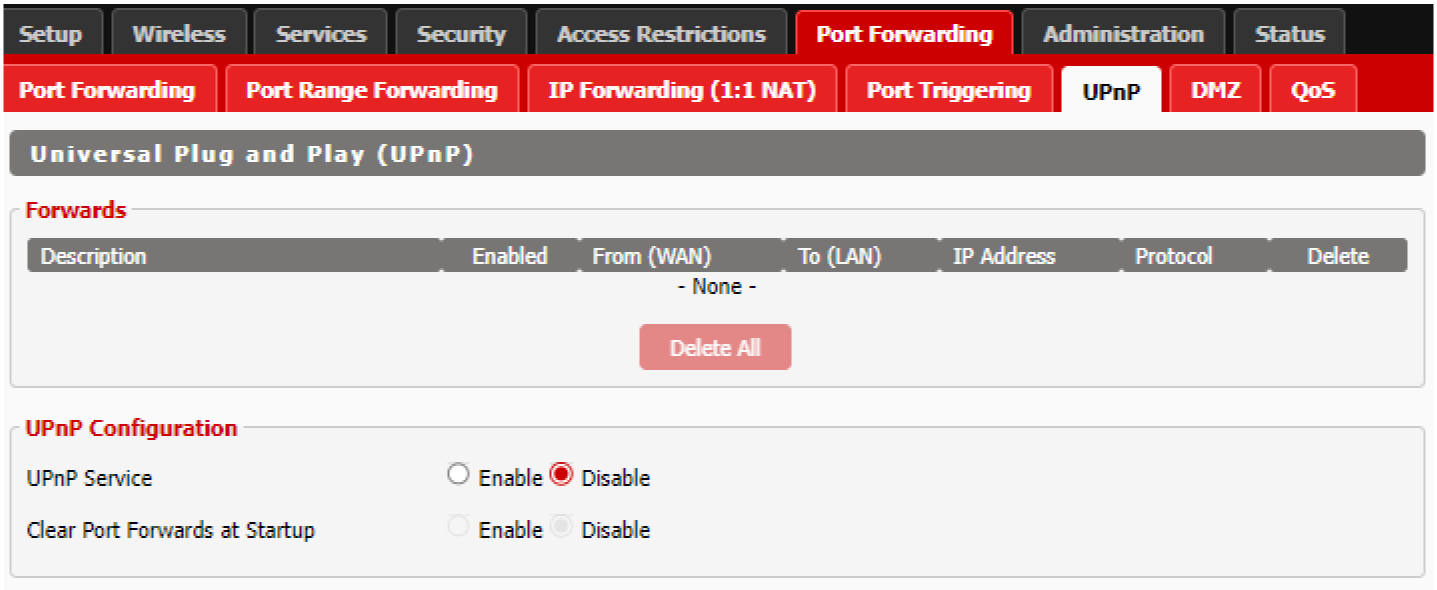
Forwards

	Triggered Port Range		Forwarded Port Range				
Application	Start	End	Protocol	Start	End	Enable	Action
	0	0	TCP	0	0	□	⊖
							⊕

Port Triggering	Description
Application	Enter the name of the application in the field provided.
Triggered Port Range	Enter the number of the first and the last port of the range which should be triggered. If a PC sends outbound traffic from those ports, incoming traffic on the Forwarded Port Range will be forwarded to that PC.
Protocol	Choose the right protocol TCP, UDP, or Both. Set this to what the application requires.
Forwarded Port Range	Enter the number of the first and last port of the range which should be forwarded from the Internet to the PC and has triggered the Triggered Port Range.
Enable	Enable port triggering for the application.

7.5 UPnP

Universal Plug and Play (UPnP) is a set of computer network protocols. This allows devices to connect seamlessly and to simplify the implementation of networks. UPnP achieves this by defining and publishing UPnP device control protocols built upon open, Internet-based communication standards.



Universal Plug and Play (UPnP)

Forwards

Description	Enabled	From (WAN)	To (LAN)	IP Address	Protocol	Delete
- None -						

UPnP Configuration

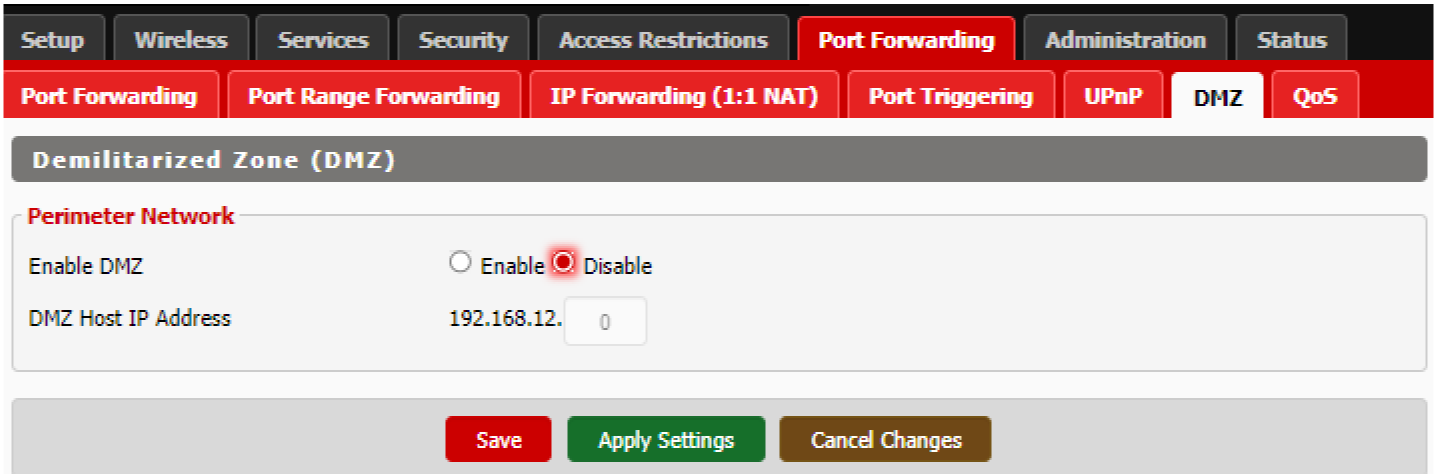
UPnP Service ○ Enable ● Disable

Clear Port Forwards at Startup ○ Enable ○ Disable

Universal Plug and Play (UPnP)	Description
Forwards	The UPnP forwards table shows all open ports forwarded automatically by the UPnP process.
UPnP Service	Enables UPnP service.
Clear Port Forwards at Startup	If enabled, a presentation URL tag is sent with the device description. This allows the router to show up in Window's My Network Places. You may need to reboot your PC when enabling this option.

7.6 DMZ

The Demilitarized Zone (DMZ) hosting feature allows one local user to be exposed to the Internet for use of a service. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure since it only opens a designated port.



Demilitarized Zone (DMZ)

Perimeter Network

Enable DMZ ○ Enable ● Disable

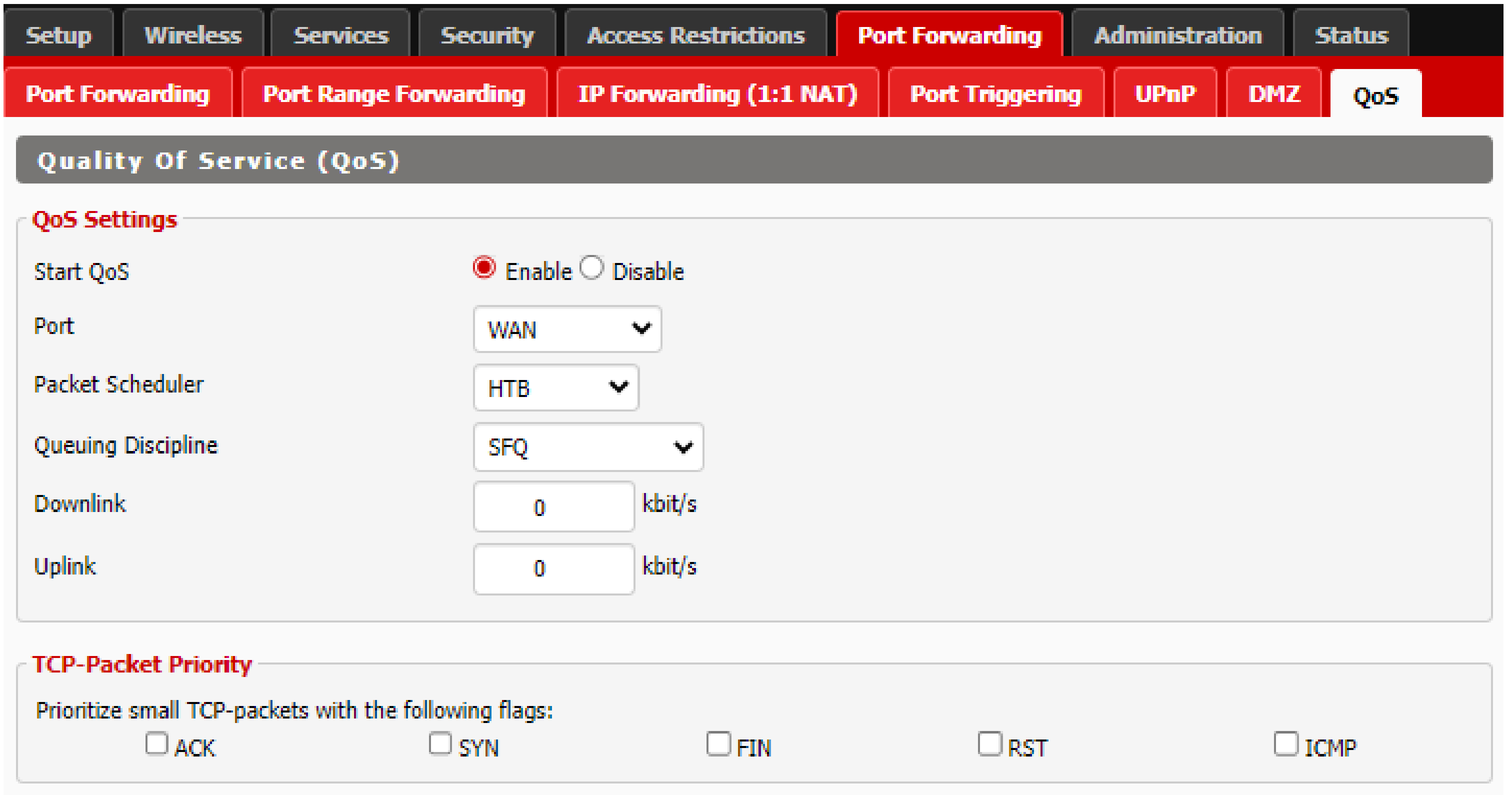
DMZ Host IP Address 192.168.12. 0

Demilitarized Zone (DMZ)	Description
Use DMZ	Enable or disable DMZ.
DMZ Host IP Address	Enter the IP address of the PC you wish to expose.

7.7 QoS

7.7.1 QoS Settings

Bandwidth management prioritizes the traffic on your router. Interactive traffic (telephony, browsing, telent, etc) gets priority and bulk traffic (file tranfers, P2P) gets low priority. The main goal is to allow both types to live side-by-side without unimportant traffic disturbing more ciritical things. Quality of Service (QoS) allows control of the bandwidth allocation to different services, netmasks, MAC addresses, and the ports. QoS is divided into five bandwidth classes: Maximum, Premium, Express, Standard, and Bulk. Unclassified services will use the Standard bandwidth class.



Quality Of Service (QoS)

QoS Settings

Start QoS	● Enable ○ Disable
Port	WAN
Packet Scheduler	HTB
Queuing Discipline	SFQ
Downlink	0 kbit/s
Uplink	0 kbit/s

TCP-Packet Priority

Prioritize small TCP-packets with the following flags:

□ ACK □ SYN □ FIN □ RST □ ICMP

Quality of Service (QoS)	Description
Start QoS	Enable or disable QoS services.
Port	You must choose whether to apply QoS to the WAN or LAN & WLAN port (LAN and WLAN are bonded internally into a single virtual device).
Packet Scheduler	HFSC: Hierarchical Fair Service Curve. Queues attached to an interface build a tree, thus each queue can have further child queues. Each queue can have a priority and bandwidth assigned. Priority controls the how long time packets take to get sent out, while bandwidth effects throughput. HTB is a little more resource demanding than HFSC. HTB: Hierarchical Token Bucket. HTB helps in controlling the use of the outbound bandwidth on a given link. HTB allows you to use one physical link to simulate several slower links and to send different kinds of traffic on different simulated links. HTB is useful for limiting a client’s download/upload rates, preventing their monopolization of the available bandwidth.

Queuing Discipline	Choose between SFQ or FQ_CODEL as the queuing discipline method.
Downlink (kbps)	In order to use QoS, you must enter bandwidth values for your uplink and downlink. These are generally 85% to 95% of your maximum bandwidth. If you only want QoS to apply to uplink bandwidth, enter 0 (no limit) for downlink. Do not enter 0 for uplink.
Uplink (kbps)	In order to use QoS, you must enter bandwidth values for your uplink and downlink. These are generally 85% to 95% of your maximum bandwidth. If you only want QoS to apply to uplink bandwidth, enter 0 (no limit) for downlink. Do not enter 0 for uplink.
TCP Packet Priority	Prioritize small TCP-packets with the following flags: ACK, STN, FIN, RST.

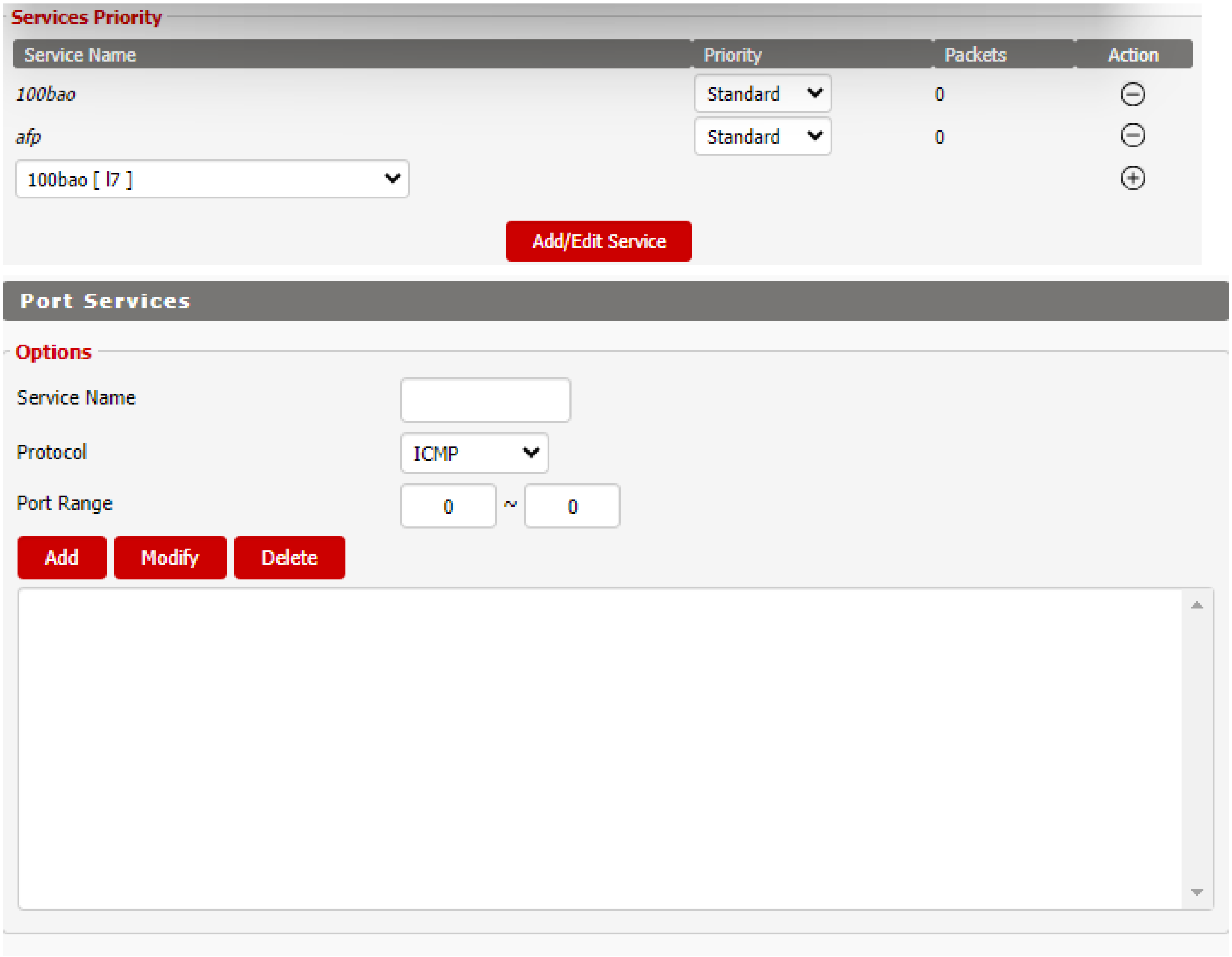
Priority: Bandwidth classification based on the four categories will be enabled first on the hardware ports, then on MAC addresses, then netmasks and finally services. For example, if you enable classification based on a MAC address, this will override netmask and service classifications. However, the LAN port-based classification will work together with MAC, netmask and service classifications, and will not override them.

- Maximum – (75% - 100%) This class offers maximum priority and should be used sparingly.
- Premium – (50% - 100%) Second highest bandwidth class. By default, handshaking and ICMP packets fall into this class. Most VoIP and video services will function well in this class if Express is not sufficient.
- Express – (25% - 100%) The Express class is for interactive applications that require bandwidth above standard services so that interactive apps run smoothly. • Standard – (15% - 100%) All services that are not specifically classed will fall under standard class.
- Bulk – (5% - 100%) The bulk class is only allocated remaining bandwidth when the remaining classes are idle. If the line is full of traffic from other classes, bulk will only be allocated 1% of total set limit. Use this class for P2P and downloading services like FTP

Uplink:
Set this to 85% - 95% (max) of your total upload limit.
Downlink:
Set this to 85% - 100% (max) of your total download limit.

7.7.2 Services Priority

You may control your data rate with respect to the application that is consuming bandwidth.



Services Priority

Service Name	Priority	Packets	Action
100bao	Standard	0	⊖
afp	Standard	0	⊖
100bao [l7]			⊕

Port Services

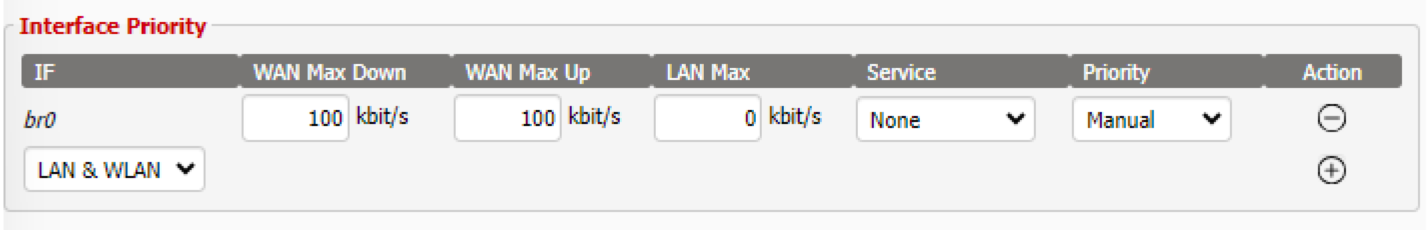
Options

Service Name	
Protocol	ICMP
Port Range	0 ~ 0

Services Priority	Description
Service Name	Enter a service name.
Protocol	Select the appropriate protocol.
Port Range	Enter a port range.

7.7.3 Interface Priority

You may specify the priority for all traffic from an interface on the router.

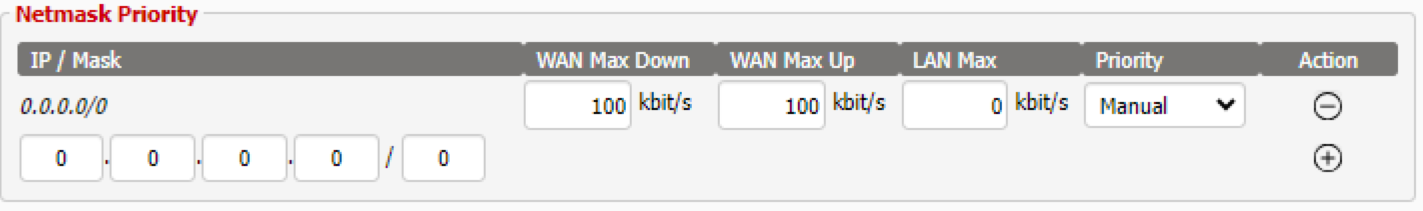


Interface Priority

IF	WAN Max Down	WAN Max Up	LAN Max	Service	Priority	Action
br0	100 kbit/s	100 kbit/s	0 kbit/s	None	Manual	⊖
LAN & WLAN						⊕

7.7.4 Netmask Priority

You may control your data rate with respect to the application that is consuming bandwidth

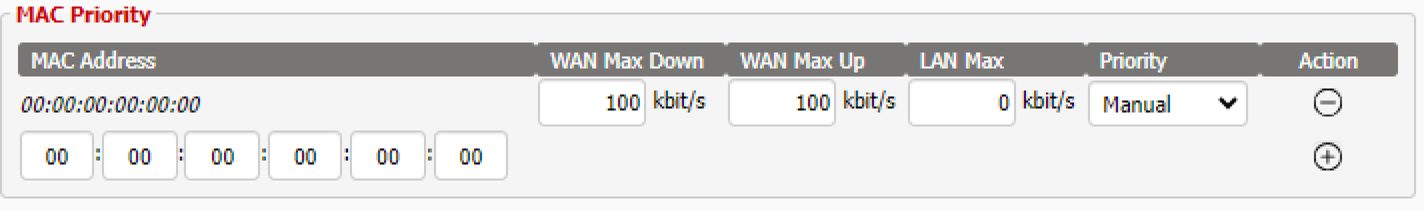


Netmask Priority

IP / Mask	WAN Max Down	WAN Max Up	LAN Max	Priority	Action
0.0.0.0/0	100 kbit/s	100 kbit/s	0 kbit/s	Manual	⊖
0 . 0 . 0 . 0 / 0					⊕

7.7.5 MAC Priority

You may specify priority for all traffic from a device on your network by assigning it a name, specifying priority and entering the device MAC address.

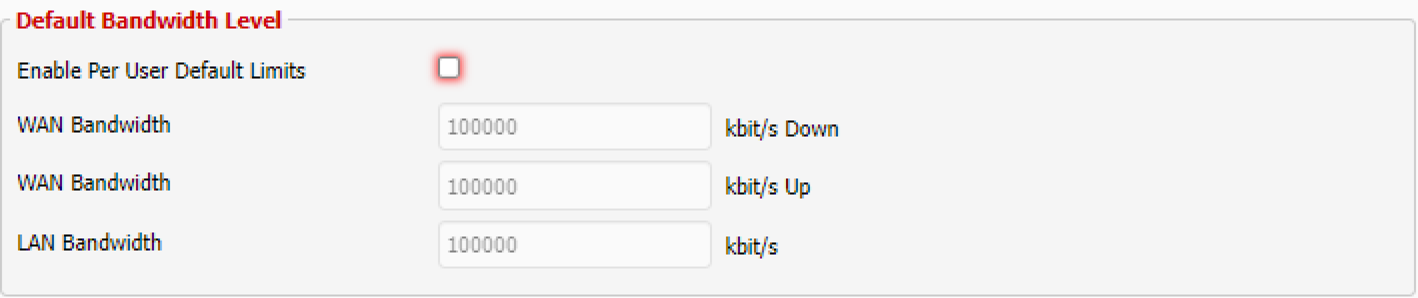


MAC Priority

MAC Address	WAN Max Down	WAN Max Up	LAN Max	Priority	Action
00:00:00:00:00:00	100 kbit/s	100 kbit/s	0 kbit/s	Manual	⊖
00 : 00 : 00 : 00 : 00 : 00					⊕

7.7.6 Default Bandwidth Level

Enable Per User Default Limits: Enable the default level per user or set the level for all users.

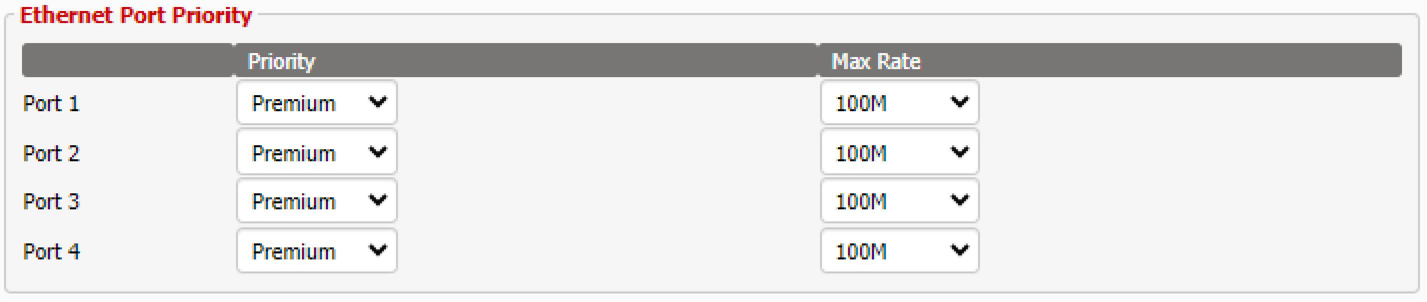


Default Bandwidth Level

Enable Per User Default Limits	□	
WAN Bandwidth	100000	kbit/s Down
WAN Bandwidth	100000	kbit/s Up
LAN Bandwidth	100000	kbit/s

7.7.7 Ethernet Port Priority

You may specify priority for all traffic from a device on your network by assigning priority level, specifying priority and entering the max rate per port.



Ethernet Port Priority

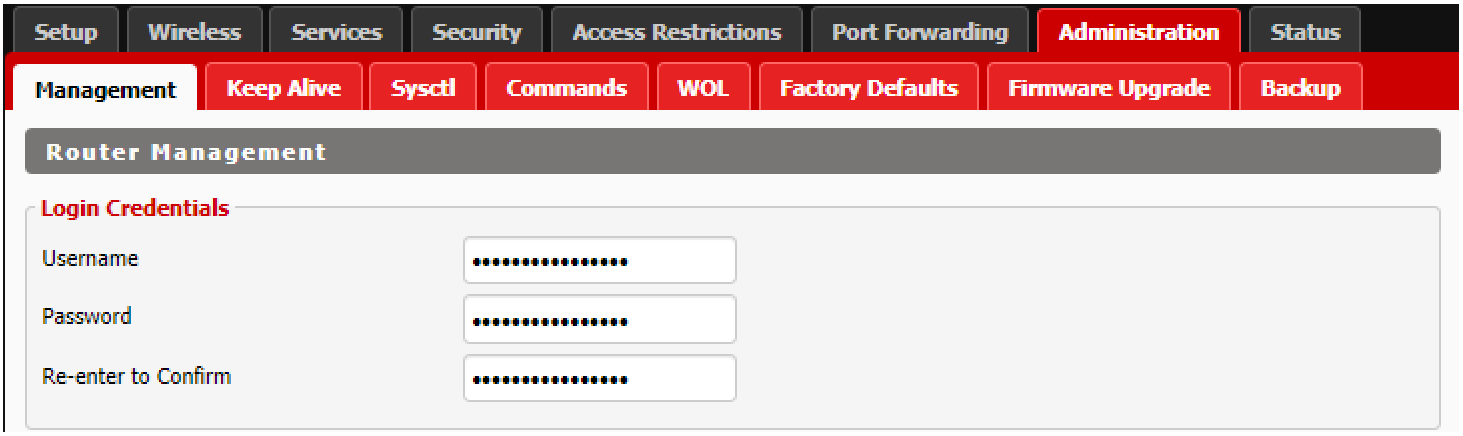
	Priority	Max Rate
Port 1	Premium	100M
Port 2	Premium	100M
Port 3	Premium	100M
Port 4	Premium	100M

8. Administration

The Administration tab allows you to change the router's settings. On this page you will find most of the configurable items of the router code.

8.1 Management

8.1.1 Router Password



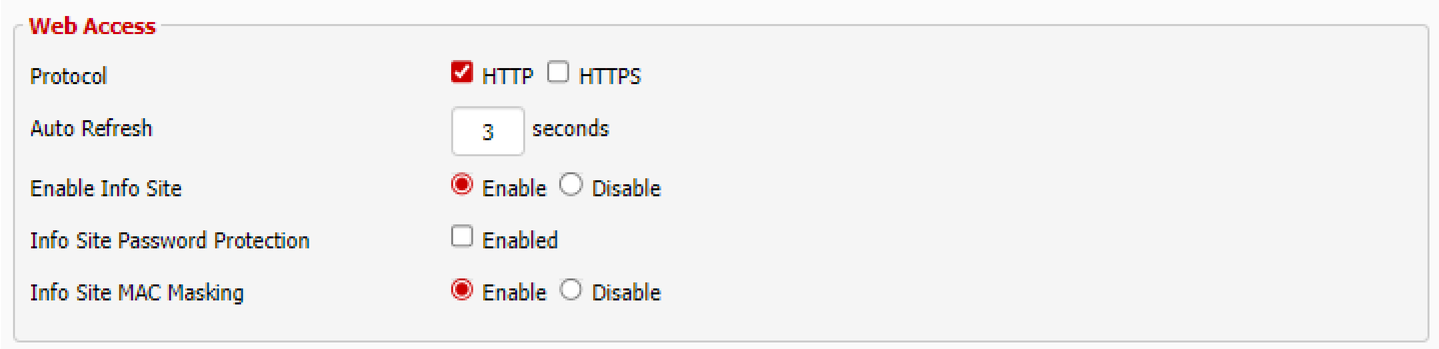
Router Management

Login Credentials

Username	••••••••••••••••
Password	••••••••••••••••
Re-enter to Confirm	••••••••••••••••

Router Password	Description
Router Username	Enter the router's username.
Router Password	Enter the router's password. New password must not exceed 32 characters in length and must not include any spaces.
Re-enter to Confirm	Enter the new password to confirm it.

8.1.2 Web Access



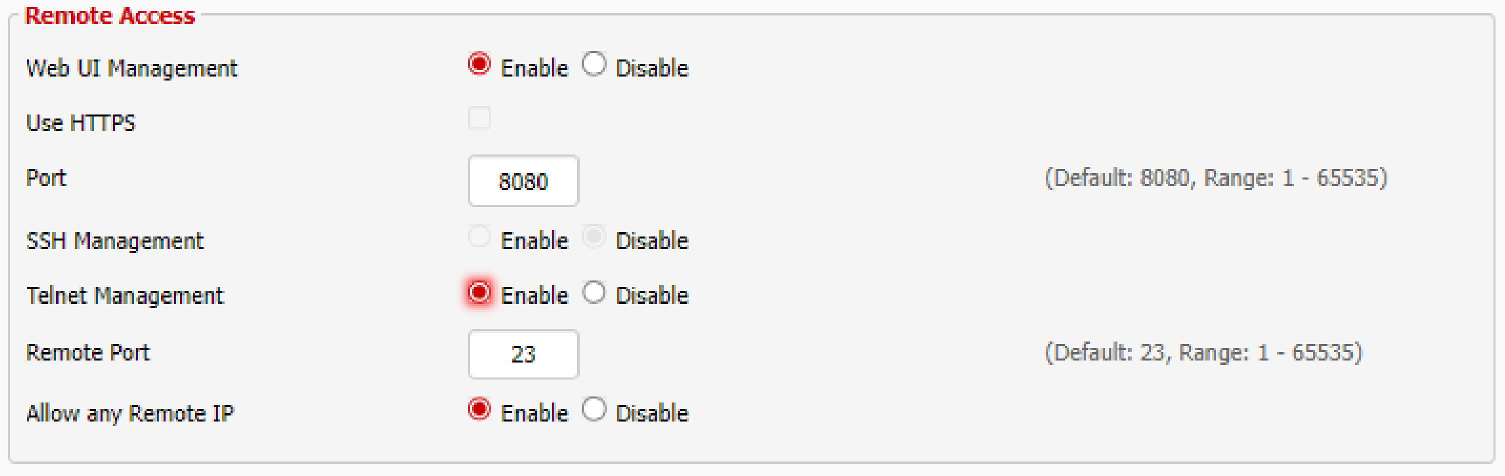
Web Access

Protocol	☑ HTTP ☐ HTTPS
Auto Refresh	3 seconds
Enable Info Site	● Enable ○ Disable
Info Site Password Protection	☐ Enabled
Info Site MAC Masking	● Enable ○ Disable

Web Access	Description
Protocol	Manage the router using either HTTP protocol or HTTPS protocol. If you choose to disable this feature, a manual reboot will be required.
Auto-Refresh (seconds)	Set the auto-refresh time of the web page.
Enable Info Site	Activate the router information web page.
Info Sie Password Protection	Password protect the router information web page.
Info site MAC Masking	Allows you to truncate MAC addresses in the web interface.

8.1.3 Remote Access

This feature allows you to manage the router from a remote location, via the Internet. When enabled, use the specified port (default is 8080).



Remote Access

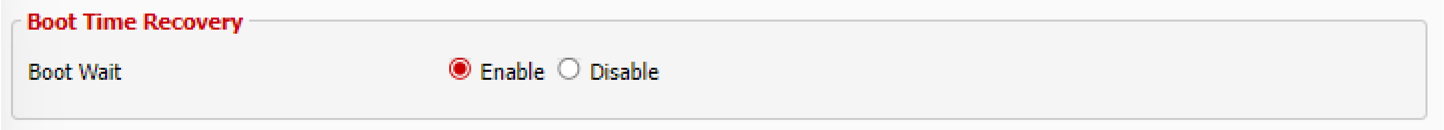
Web UI Management	● Enable ○ Disable	
Use HTTPS	□	
Port	8080	(Default: 8080, Range: 1 - 65535)
SSH Management	○ Enable ● Disable	
Telnet Management	● Enable ○ Disable	
Remote Port	23	(Default: 23, Range: 1 - 65535)
Allow any Remote IP	● Enable ○ Disable	

Remote Access	Description
Web GUI Management	Enable or disable remote access the web interface.
Use HTTPS	Use HTTPS, otherwise default is HTTP.
Web GUI Port	To remotely manage the router, enter http://xxxx.xxxx.xxxx.xxxx:8080 (the 's represents the router's IP address, and 8080 represents the specified port) in your web browser's address field.
SSH Management	Enable SSH remote access. Note that the SSH daemon needs to be enabled in the Services page.

Telnet Management	Enable Telent remote access.
Telnet Remote Port	Telnet port. Default is port 23.
Allow Any Remote IP	Allow any remote IP access or specify a range or IPs.

8.1.4 Boot Time Recovery

Boot Wait is a feature that introduces a short delay while booting (5 seconds). During this delay you can initiate the download of a new firmware if the one in flash rom is not broken. This is only necessary if you can no longer reflash using the web interface because the installed firmware will not boot.

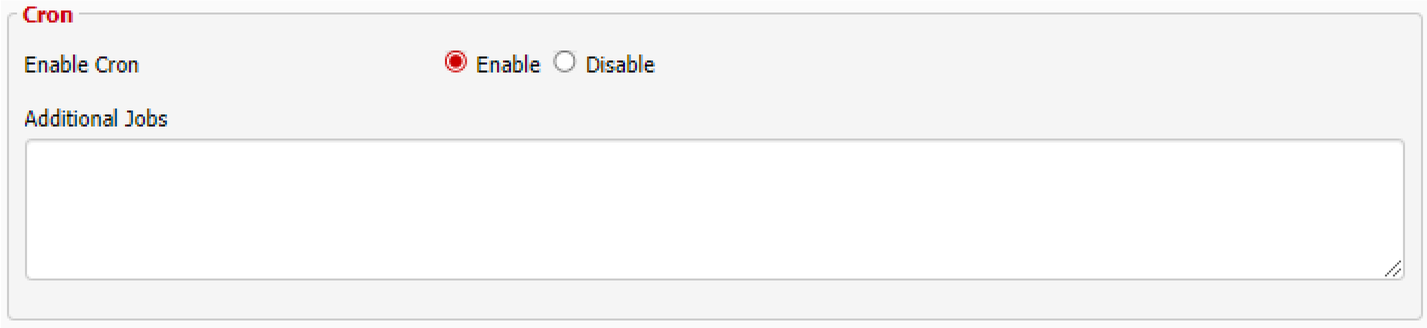


Boot Time Recovery

Boot Wait ● Enable ○ Disable

8.1.5 Cron

The cron subsystem schedules execution of Linux commands. You will need to use the command line or startup scripts to do this.



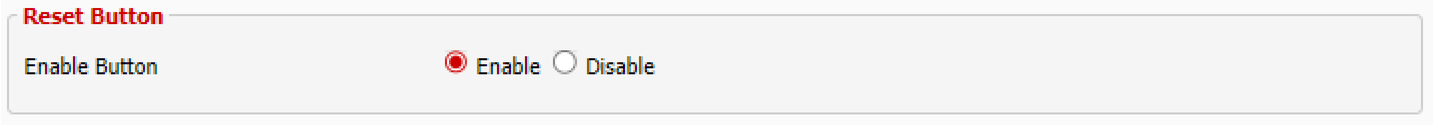
Cron

Enable Cron ● Enable ○ Disable

Additional Jobs

8.1.6 Reset Button

This feature controls the reset buttton process. The reset button initiates actions depending on how long you press it.



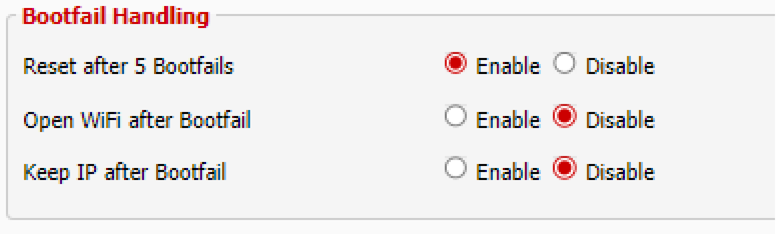
Reset Button

Enable Button ● Enable ○ Disable

On Device:

- Short press – Reset the router (reboot)
- Long press (>30s) – Reboot and restore the factory default configuration. You should hear beep and that will hard reset the unit to factory default.

8.1.7 Bootfail Handling

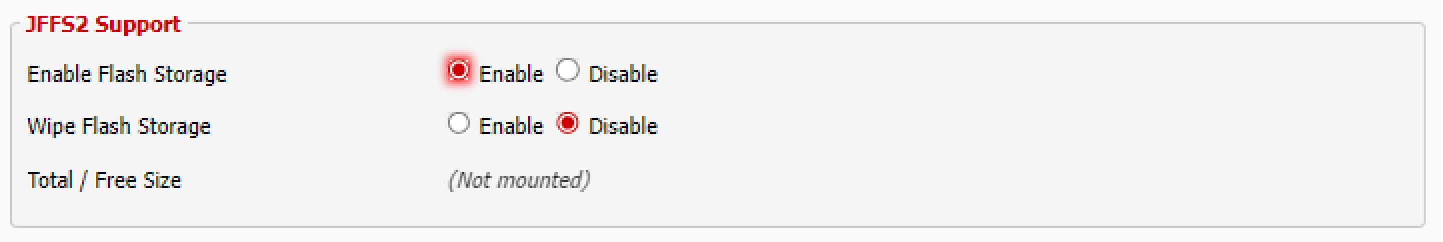


Bootfail Handling

Reset after 5 Bootfails	● Enable ○ Disable
Open WiFi after Bootfail	○ Enable ● Disable
Keep IP after Bootfail	○ Enable ● Disable

8.1.8 JFFS2 Support

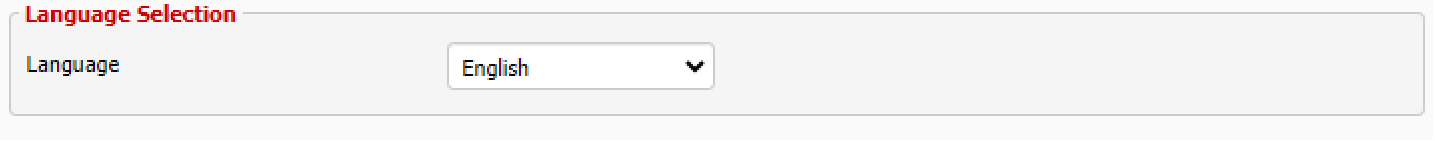
When you first Enable Flash Storage, it is necessary to enable Wipe Flash Storage in order to prepare the flash file system for usage.



JFFS2 Support

Enable Flash Storage	● Enable ○ Disable
Wipe Flash Storage	○ Enable ● Disable
Total / Free Size	*(Not mounted)*

8.1.9 Language Selection

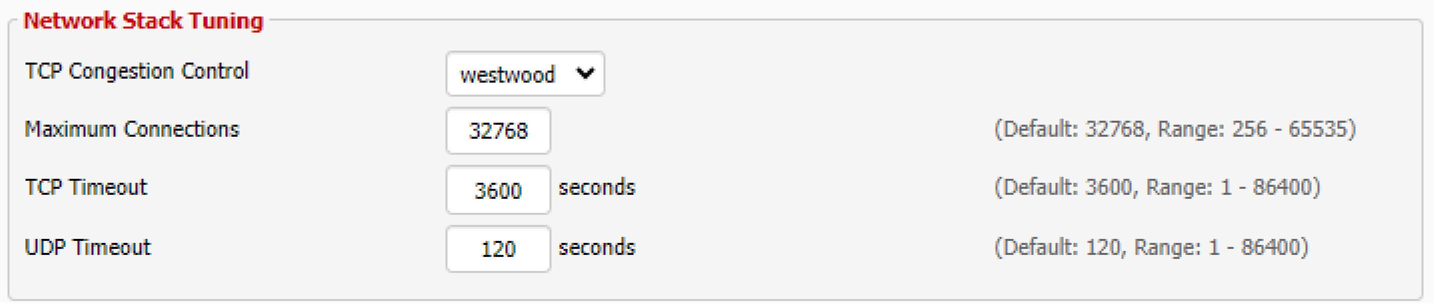


Language Selection

Language	English

8.1.10 Network Stack Tuning

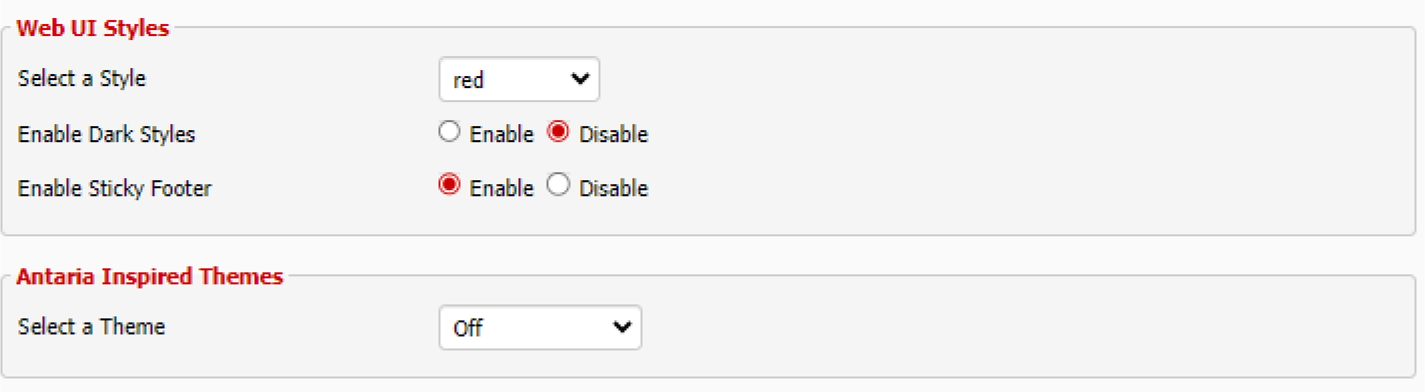
Advanced users can use the sysctl tab to further tune the network stack beyond the limited set of options available here. Any settings available on sysctl should be handled with caution, ensure you have a current backup before proceeding in case changes have undesired results.



Network Stack Tuning

TCP Congestion Control	westwood	
Maximum Connections	32768	(Default: 32768, Range: 256 - 65535)
TCP Timeout	3600 seconds	(Default: 3600, Range: 1 - 86400)
UDP Timeout	120 seconds	(Default: 120, Range: 1 - 86400)

8.1.11 Web UI and Theme



Web UI Styles

Select a Style: red

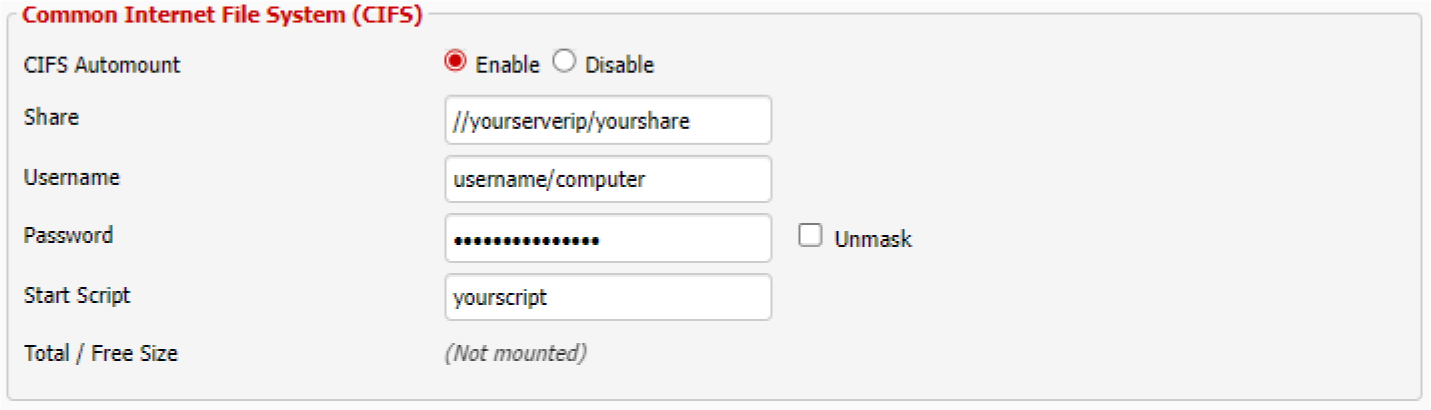
Enable Dark Styles: ○ Enable ● Disable

Enable Sticky Footer: ● Enable ○ Disable

Antaria Inspired Themes

Select a Theme: Off

8.1.12 Common Internet File System (CIFS)



Common Internet File System (CIFS)

CIFS Automount: ● Enable ○ Disable

Share: //yourserverip/yourshare

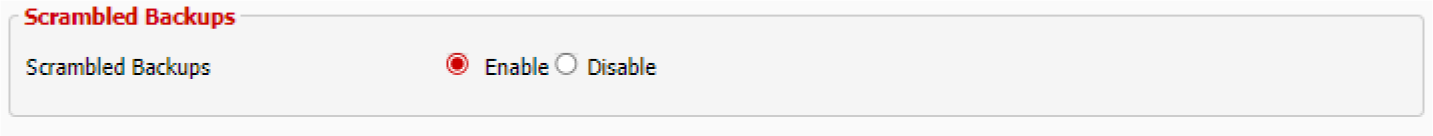
Username: username/computer

Password: ••••••••••••••• □ Unmask

Start Script: yourscript

Total / Free Size: *(Not mounted)*

8.1.13 Scrambled Backups

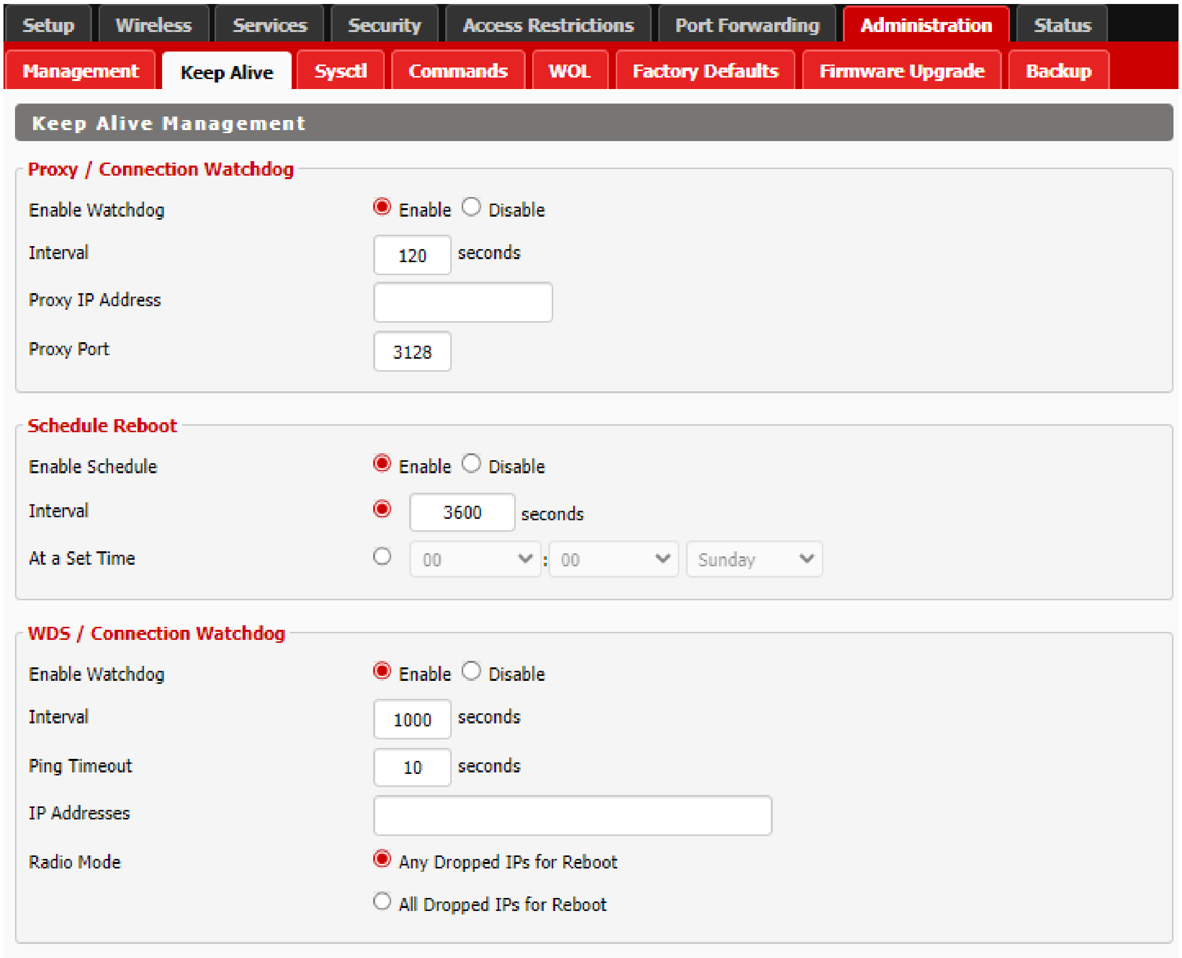


Scrambled Backups

Scrambled Backups: ● Enable ○ Disable

8.2 Keep Alive

Configure Keep Alive Management within Proxy or WDS, Watchdog, and scheduling Reboot



Keep Alive Management

Proxy / Connection Watchdog

Enable Watchdog ● Enable ○ Disable

Interval 120 seconds

Proxy IP Address

Proxy Port 3128

Schedule Reboot

Enable Schedule ● Enable ○ Disable

Interval ● 3600 seconds

At a Set Time ○ 00 : 00 Sunday

WDS / Connection Watchdog

Enable Watchdog ● Enable ○ Disable

Interval 1000 seconds

Ping Timeout 10 seconds

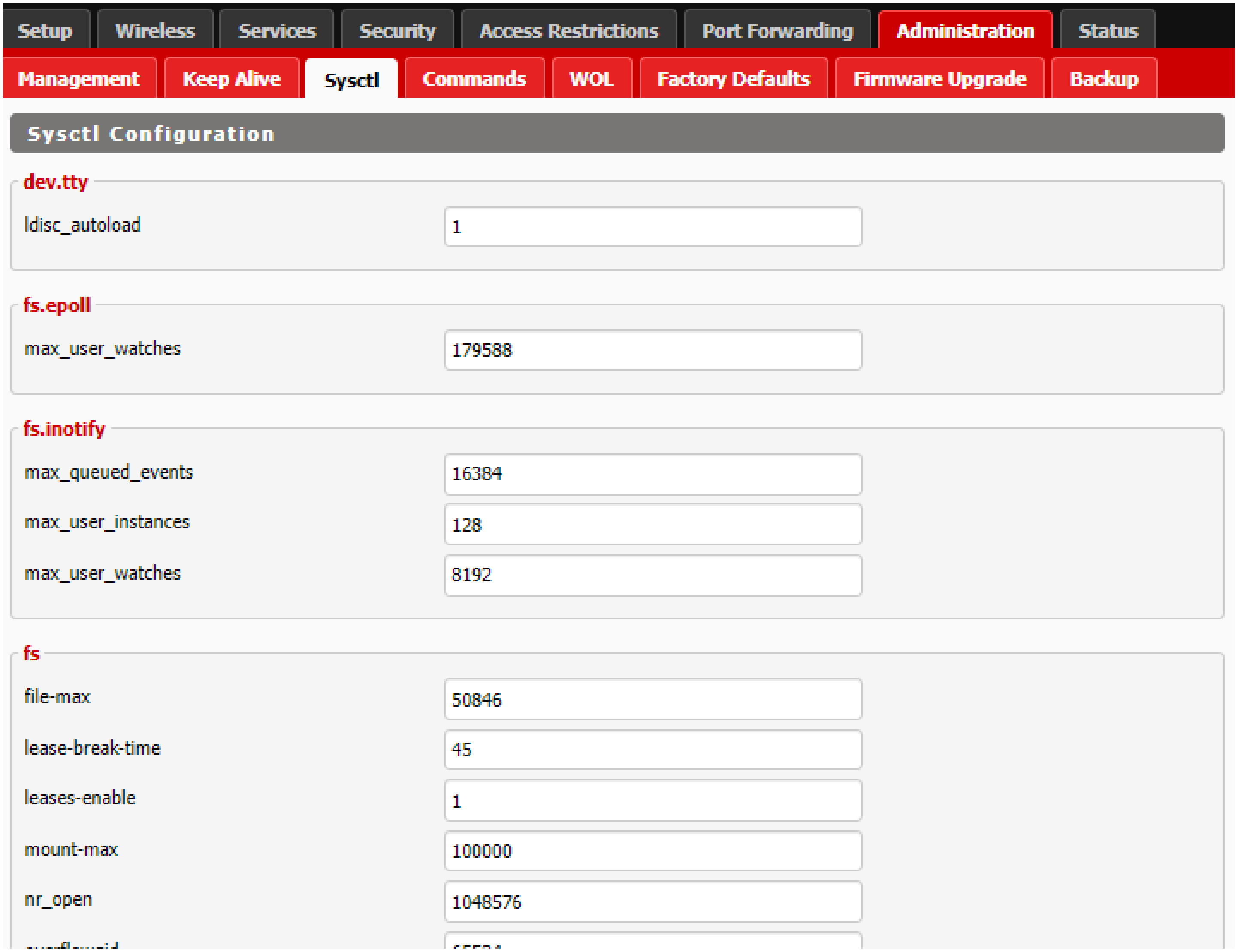
IP Addresses

Radio Mode ● Any Dropped IPs for Reboot
○ All Dropped IPs for Reboot

Schedule Reboot At a Set Time:
Choose a schedule when to reboot the router. Cron must be enabled in the management tab.
WDS / Connection Watchdog:
IP Addresses: Only a maximum of three IP addresses separated by a SPACE are allowed.

8.3 Sysctl

sysctl is used to modify kernel parameters at runtime



Sysctl Configuration

dev.tty

ldisc_autoload	1

fs.epoll

max_user_watches	179588

fs.inotify

max_queued_events	16384
max_user_instances	128
max_user_watches	8192

fs

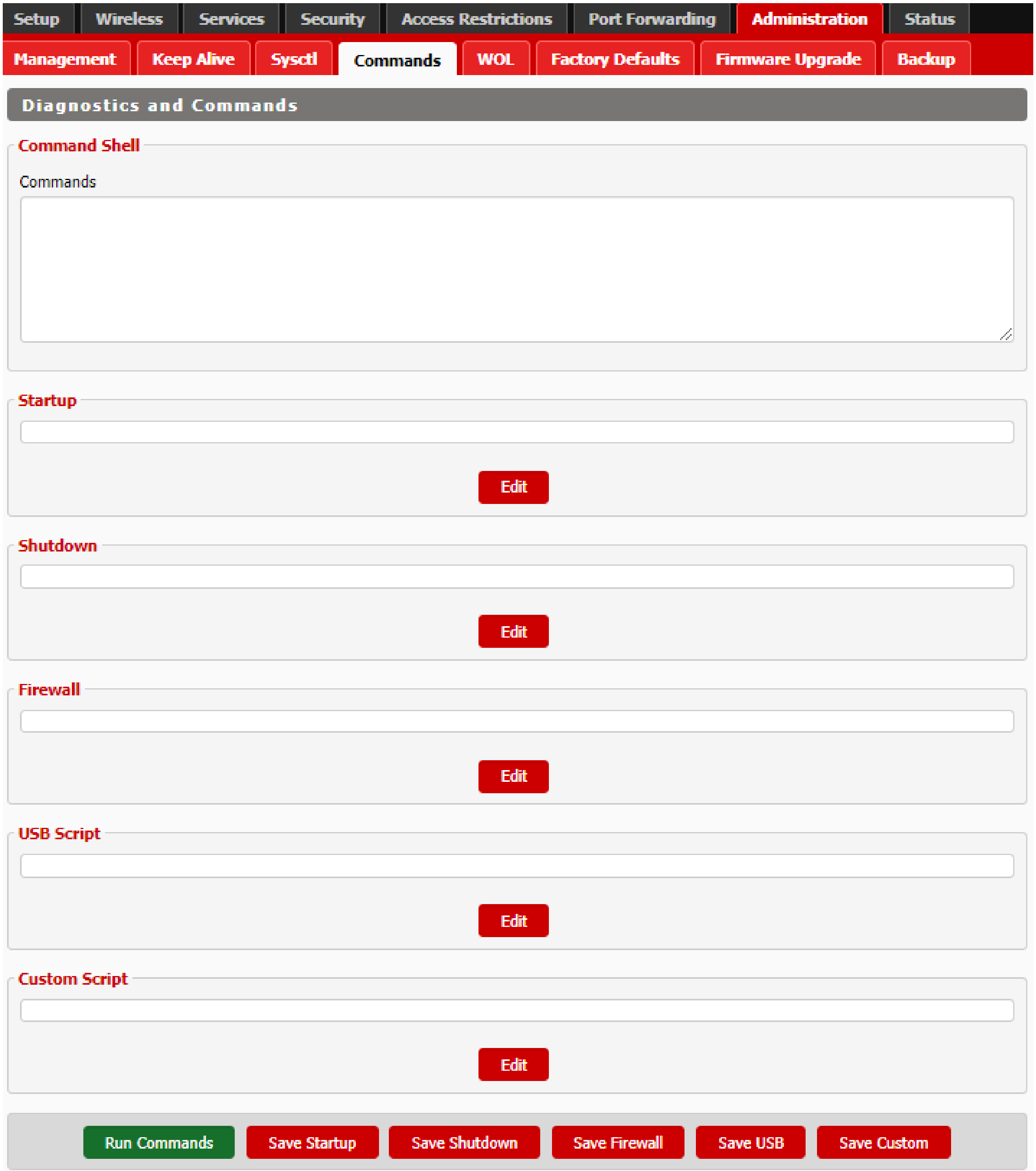
file-max	50846
lease-break-time	45
leases-enable	1
mount-max	100000
nr_open	1048576
overflowuid	65534

NOTE:

It is recommended to save a config file before any modification to the sysctl

8.4 Commands

You can run commands directly via the web interface. Fill the text area with your commands and click Run Commands to run them. You can also specifiy commands to be executed during the router startup. Fill the text area with commands (only one command per row) and click Save Startup.

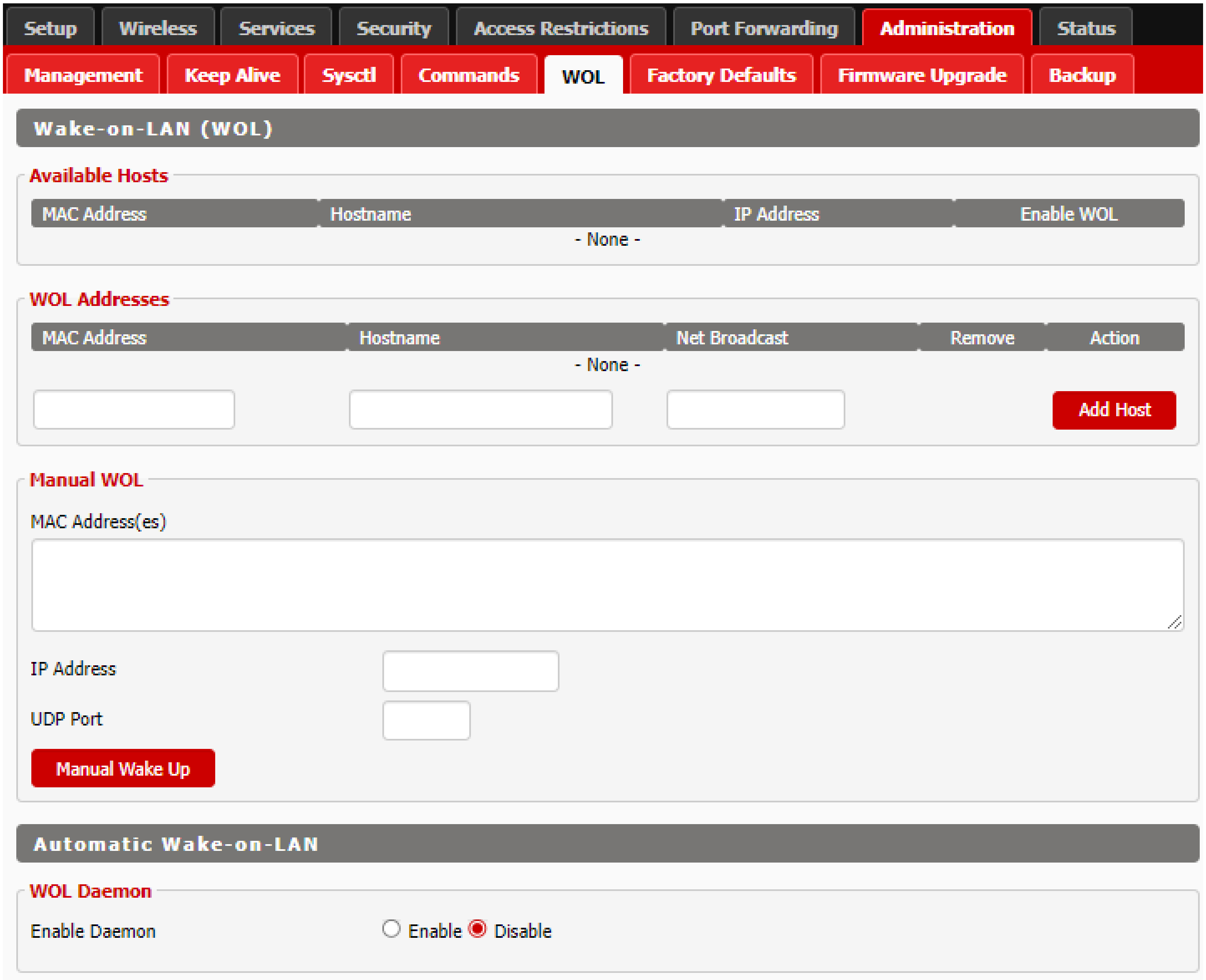


Recommended: a terminal connection via SSH/Telnet is a more suitable, flexible, faster and reliable for some commands.

NOTE: Recommended: a terminal connection via SSH/Telnet is a more suitable, flexible, faster and reliable for some commands.

8.5 Wake-on-LAN (WOL)

This page allows you to Wake Up hosts on your local network. You can manually wake up hosts by clicking the Wake Up button or alternatively by programing an automatic wake up schedule provided by the WOL Daemon.



Wake-on-LAN (WOL)

Available Hosts

MAC Address	Hostname	IP Address	Enable WOL
	- None -		

WOL Addresses

MAC Address	Hostname	Net Broadcast	Remove	Action
	- None -			

Manual WOL

MAC Address(es)

IP Address

UDP Port

Automatic Wake-on-LAN

WOL Daemon

Enable Daemon ○ Enable ● Disable

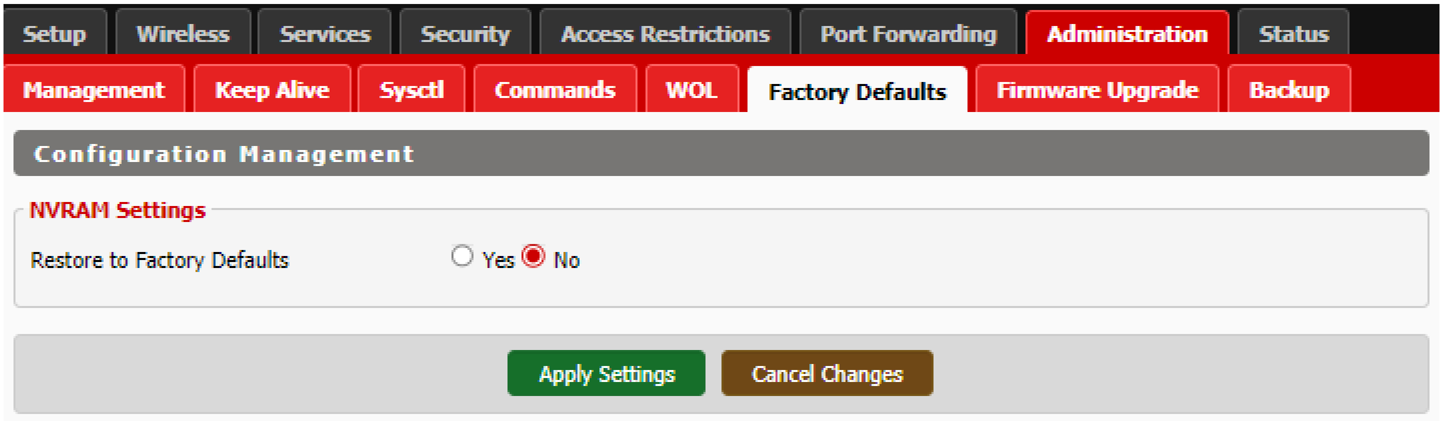
MAC Address(es): MAC address(es) are entered in the format e.g. 01:23:45:67:89:AB and must be separated by a SPACE.

IP Address: The IP address is typically the broadcast address for the local network, it could also be a remote address when e.g. the target host is not a LAN client

Wake on LAN	Description
Available Hosts	The available hosts section provides a list of hosts to add/remove from the WOL address list. This list is a combination of any defined static hosts or discovered DHCP clients
WOL Addresses	The WOL addresses section allows individual hosts in the WOL list (stored in the wol_hosts NVRAM variable) to be Woken Up. The list is a combination of selected (enabled) available hosts and manually added WOL hosts.
Manual WOL	The manila WOL section allows individual or a list of hosts to be woken up by clicking Wake Up to send it the WOL magic packet.
WOL daemon	Besides attempting to Wake Up the manually specified hosts, clicking the WOL daemon button will save the MAC addresses, Network Broadcast, and UDP port values into the manual_wol_mac, manual_wol_network, and manual_wol_port NVRAM variables and commits them to memory.
Hostname	Enter a hostname for the WOL daemon.
SecureOn Password	Enter a password.
MAC Addresses	Fill the MAC address(es) (either separated by spaces or one per line) of the computer(s) you would like to wake up.

8.6 Factory Defaults

This will reset all current NVRAM settings back to the Antaria's default values. All of your current settings will be erased.



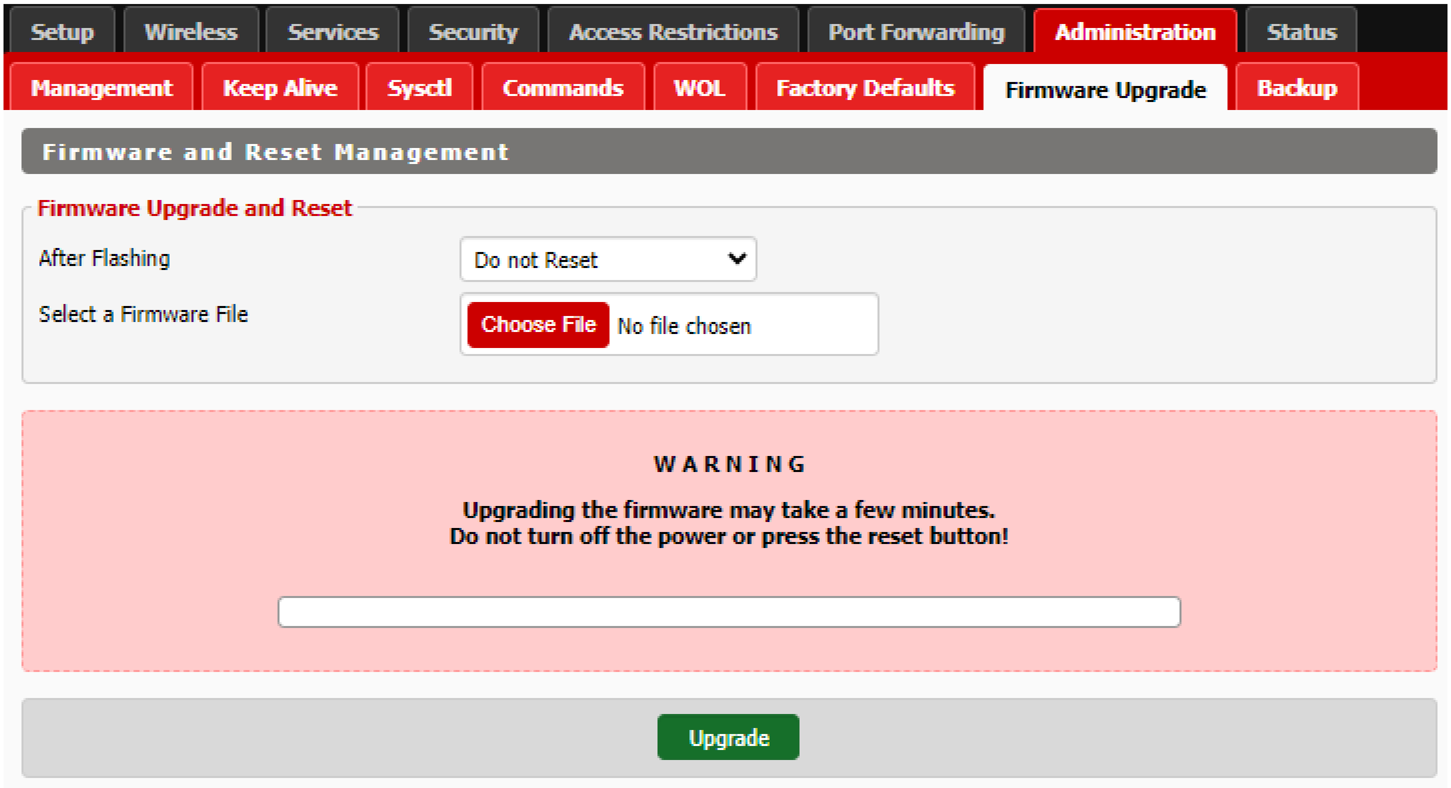
Configuration Management

NVRAM Settings

Restore to Factory Defaults ○ Yes ● No

8.7 Firmware Upgrade

Firmware Upgrade and Reset



Firmware and Reset Management

Firmware Upgrade and Reset

After Flashing: Do not Reset

Select a Firmware File: No file chosen

WARNING

Upgrading the firmware may take a few minutes.
Do not turn off the power or press the reset button!

New firmware versions are available at www.antaira.com. When you upgrade the router's firmware, you may lose its configuration settings, so make sure you write down the router settings before you updgrade its firmware.

To upgrade the router's firmware:

1. Download the firmware upgrade file from the website.
2. Click the Choose File button and choose the firmware to upgrade.
3. Click the Upgrade button and wait until the upgrade is finished and the router has rebooted.

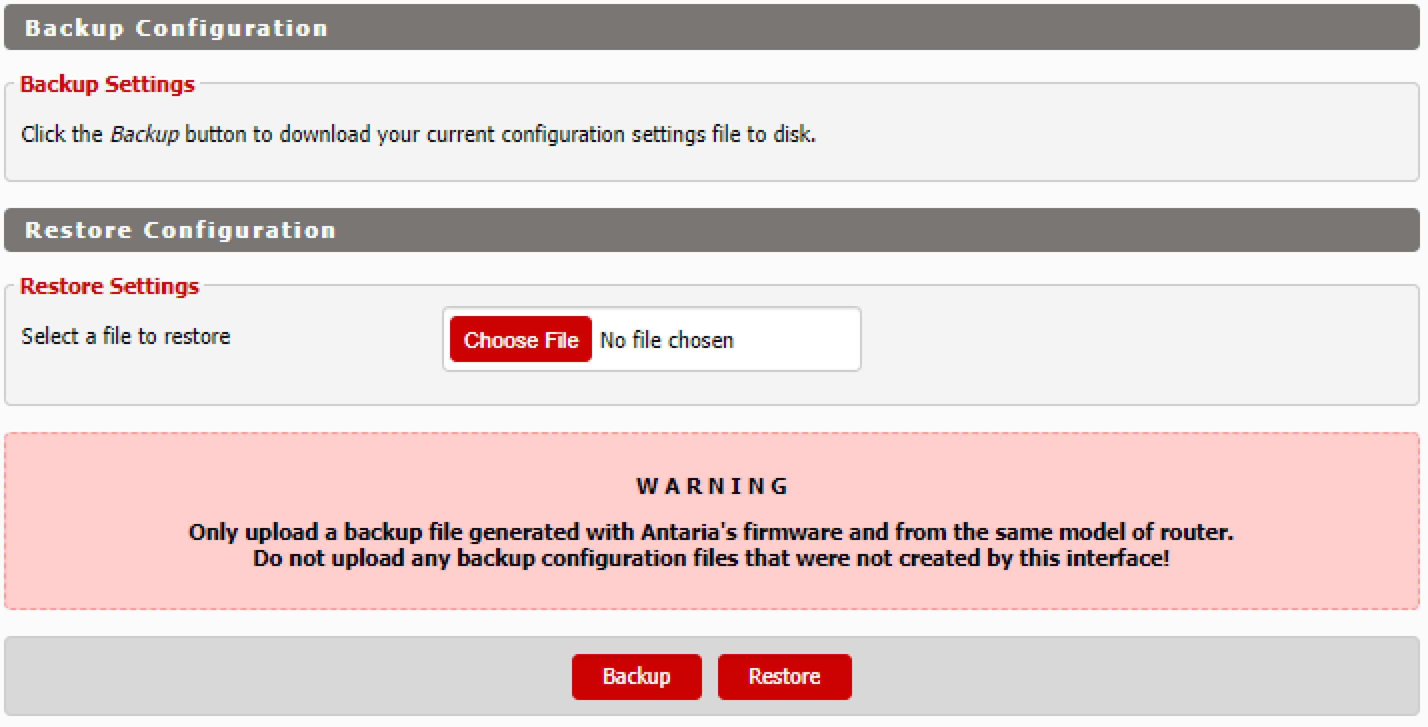
Do not power off the router, press the reset button, or interrput the browser window while the firmware is being upgraded.

If you want to reset the router to the default settings for the firmware version you are upgrading to, select the Reset to default settings option.

8.8 Backup

You may backup your current configuration in case you need to reset the router back to factory default settings.

NOTE: Over terminal type nvram show > /tmp/mybackup.txt and grab that file to your desktop for a human readable backup of your current configuration, which can be used for reference purposes only.



Backup Configuration

Backup Settings

Click the *Backup* button to download your current configuration settings file to disk.

Restore Configuration

Restore Settings

Select a file to restore

WARNING

Only upload a backup file generated with Antaria's firmware and from the same model of router.
Do not upload any backup configuration files that were not created by this interface!

Restore Settings:
Click the Browse... button to search for a backup configuration file that you have previously saved to disk. Click the Restore button to overwrite all current configuration settings with the values in the backup file.

9. Status

9.1 Router

The Status screen displays the router's current status and configuration. All information is read-only.

Router Name:

This is the specified router name, you had input on the *Setup* tab under the *Router Name* field.

MAC Address:

This is the router's MAC Address, as seen by your ISP.

Firmware Version:

This is the router's current firmware.

Current Time:

This is time received from the NTP server set on the *Setup | Basic Setup* tab.

Uptime:

This is the measure of the time the router has been "up" and running.

Load Average:

This is obtained from the three numbers that represent the system load during the last one, five, and fifteen minute periods.

9.2 WAN

Configuration Type:

This shows the information required by your ISP for connection to the Internet. This information was entered on the Setup Tab. You can *Connect* or *Disconnect* your connection here by clicking on that button.

Total Traffic:

This shows your router's Internet traffic since last reboot.

Traffic by Month:

This shows your router's Internet traffic by month. Drag the mouse over graph to see daily data. Data is stored in NVRAM.

9.3 LAN

MAC Address:

This is the router's MAC address, as seen on your local Ethernet network.

IP Address:

This shows the router's IP address as it appears on your local Ethernet network.

Subnet Mask:

When the router is using a subnet mask, it is shown here.

DHCP Server:

If you are using the router as a DHCP server, that will be displayed here.

OUI Search:

By clicking on any MAC address, you will obtain the organizationally unique identifier of the network interface (IEEE Standards OUI database search).

9.4 Wireless

MAC Address:

This is the router's MAC address, as seen on your local, wireless network.

Network:

As selected from the wireless tab, this will display the wireless mode (Mixed, G Only, B Only or Disabled) used by the network.

OUI Search:

By clicking on any MAC address, you will obtain the organizationally unique identifier of the network interface (IEEE Standards OUI database search).

9.5 Bandwidth

Bandwidth Monitoring:

A browser that supports SVG is required to display bandwidth graphs.

Switch to :

Click the label to switch unit (B/s or bit/s).

Autoscale:

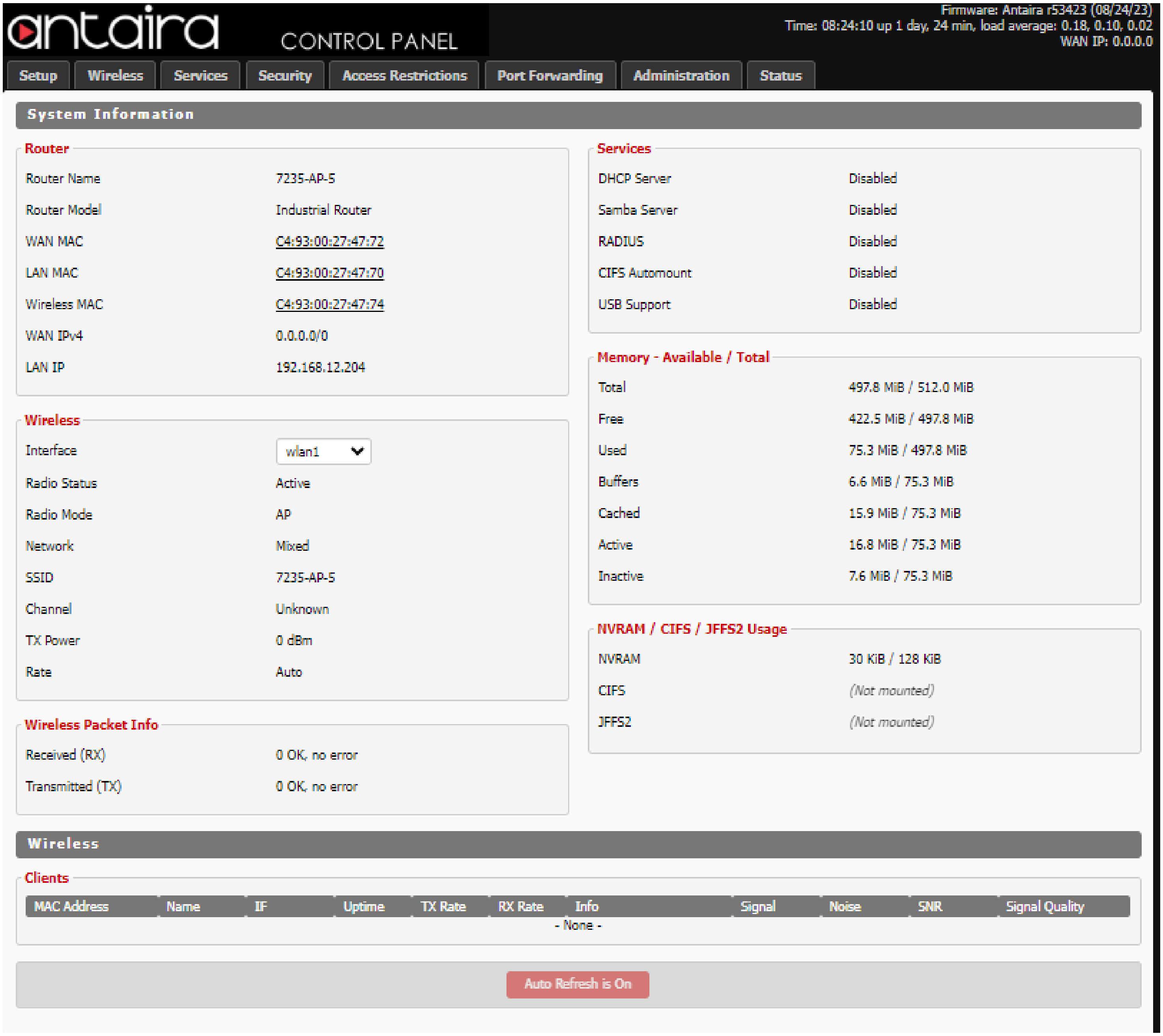
Click the label to choose graph scale type.

9.6 Syslog

Web UI of System log will show messages when syslogd is enabled

9.7 Sys Info

This page is the system information of the device.



Firmware: Antaira r53423 (08/24/23)
Time: 08:24:10 up 1 day, 24 min, load average: 0.18, 0.10, 0.02
WAN IP: 0.0.0.0

System Information

Router

Router Name	7235-AP-5
Router Model	Industrial Router
WAN MAC	C4:93:00:27:47:72
LAN MAC	C4:93:00:27:47:70
Wireless MAC	C4:93:00:27:47:74
WAN IPv4	0.0.0.0/0
LAN IP	192.168.12.204

Wireless

Interface	wlan1
Radio Status	Active
Radio Mode	AP
Network	Mixed
SSID	7235-AP-5
Channel	Unknown
TX Power	0 dBm
Rate	Auto

Wireless Packet Info

Received (RX)	0 OK, no error
Transmitted (TX)	0 OK, no error

Services

DHCP Server	Disabled
Samba Server	Disabled
RADIUS	Disabled
CIFS Automount	Disabled
USB Support	Disabled

Memory - Available / Total

Total	497.8 MiB / 512.0 MiB
Free	422.5 MiB / 497.8 MiB
Used	75.3 MiB / 497.8 MiB
Buffers	6.6 MiB / 75.3 MiB
Cached	15.9 MiB / 75.3 MiB
Active	16.8 MiB / 75.3 MiB
Inactive	7.6 MiB / 75.3 MiB

NVRAM / CIFS / JFFS2 Usage

NVRAM	30 KiB / 128 KiB
CIFS	*(Not mounted)*
JFFS2	*(Not mounted)*

Wireless

Clients

MAC Address	Name	IF	Uptime	TX Rate	RX Rate	Info	Signal	Noise	SNR	Signal Quality
						- None -				