antaira®

making connectivity simple...

Software Manual

Version 1.0
(February 2023)

LRX-0200 Series

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.

Software Manual
Version 1.0 (February 2023)

The manual supports the following models:

- LRX-0200
- LRX-0200-T

This manual supports the following firmware version:

- Release: Antaira r50399 (10/06/22)

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

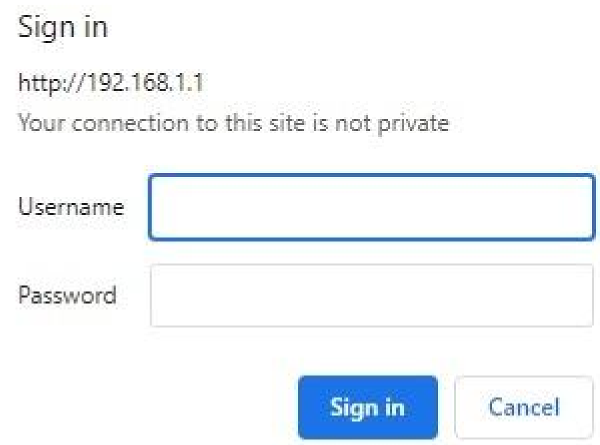
1 Access with Web Browser

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 allow 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

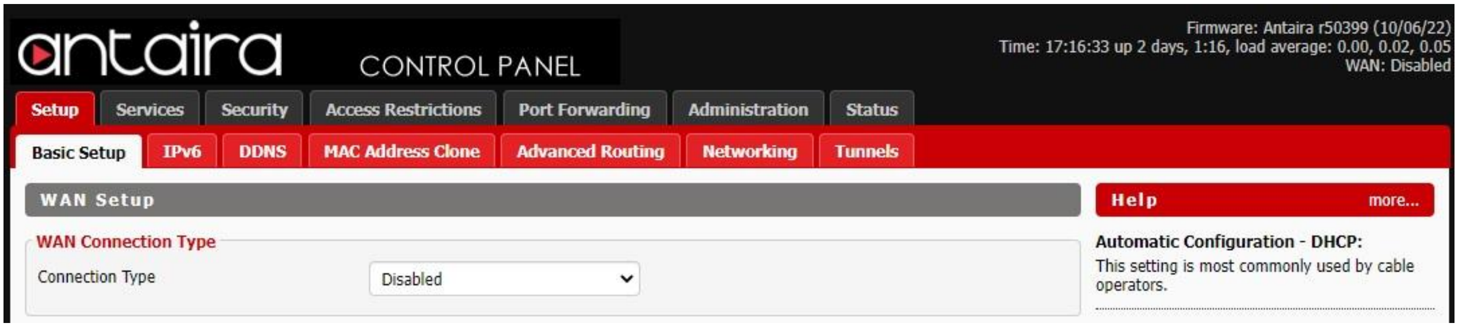
http://192.168.1.1

Your connection to this site is not private

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.



Firmware: Antaira r50399 (10/06/22)
Time: 17:16:33 up 2 days, 1:16, load average: 0.00, 0.02, 0.05
WAN: Disabled

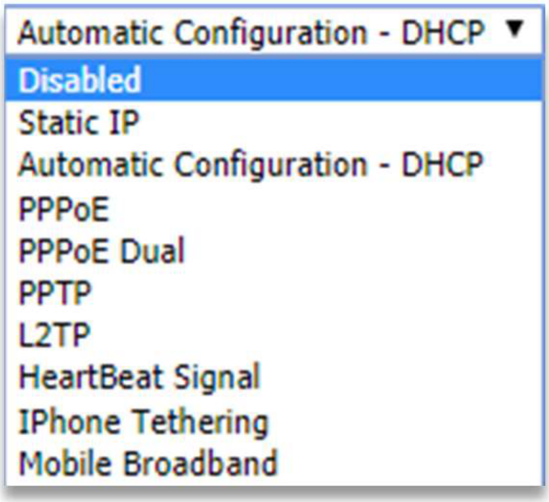
WAN Connection Type

Connection Type: Disabled

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

Setup > Basic Setup

2.1.1 WAN Setup



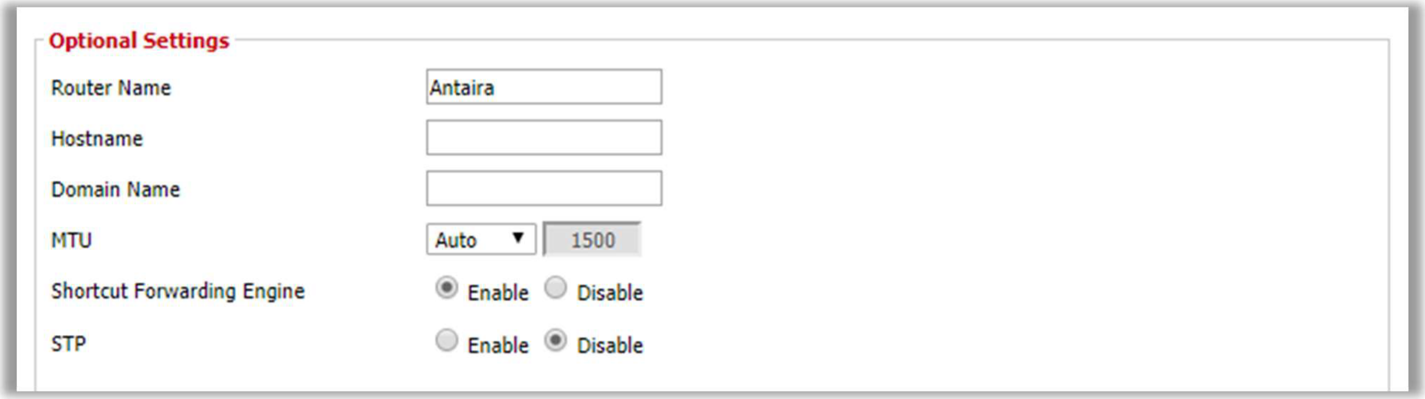
Automatic Configuration - DHCP ▼

Setup > Basic Setup > WAN Setup

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



Optional Settings

Router Name	Antaira
Hostname	
Domain Name	
MTU	Auto ▼ 1500
Shortcut Forwarding Engine	● Enable ○ Disable
STP	○ Enable ● Disable

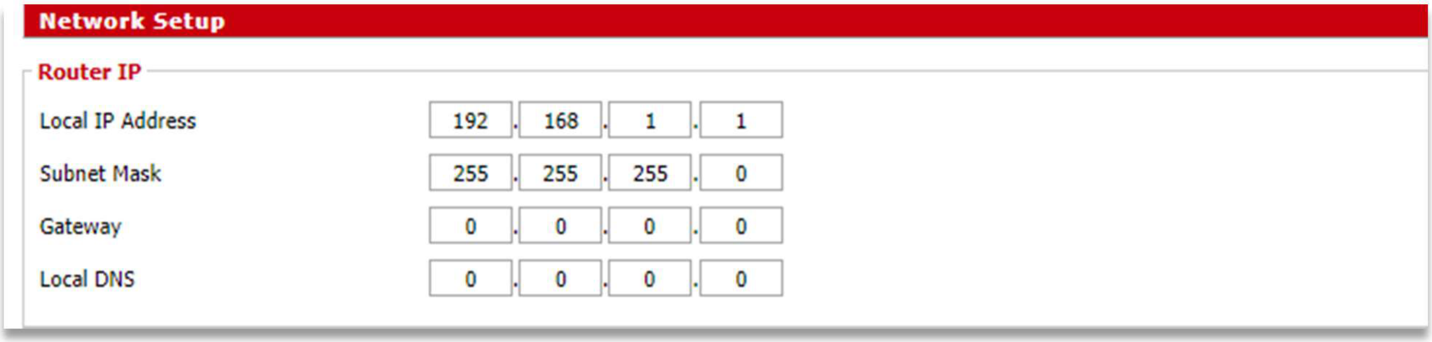
Setup > Basic Setup > Optional Settings

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.



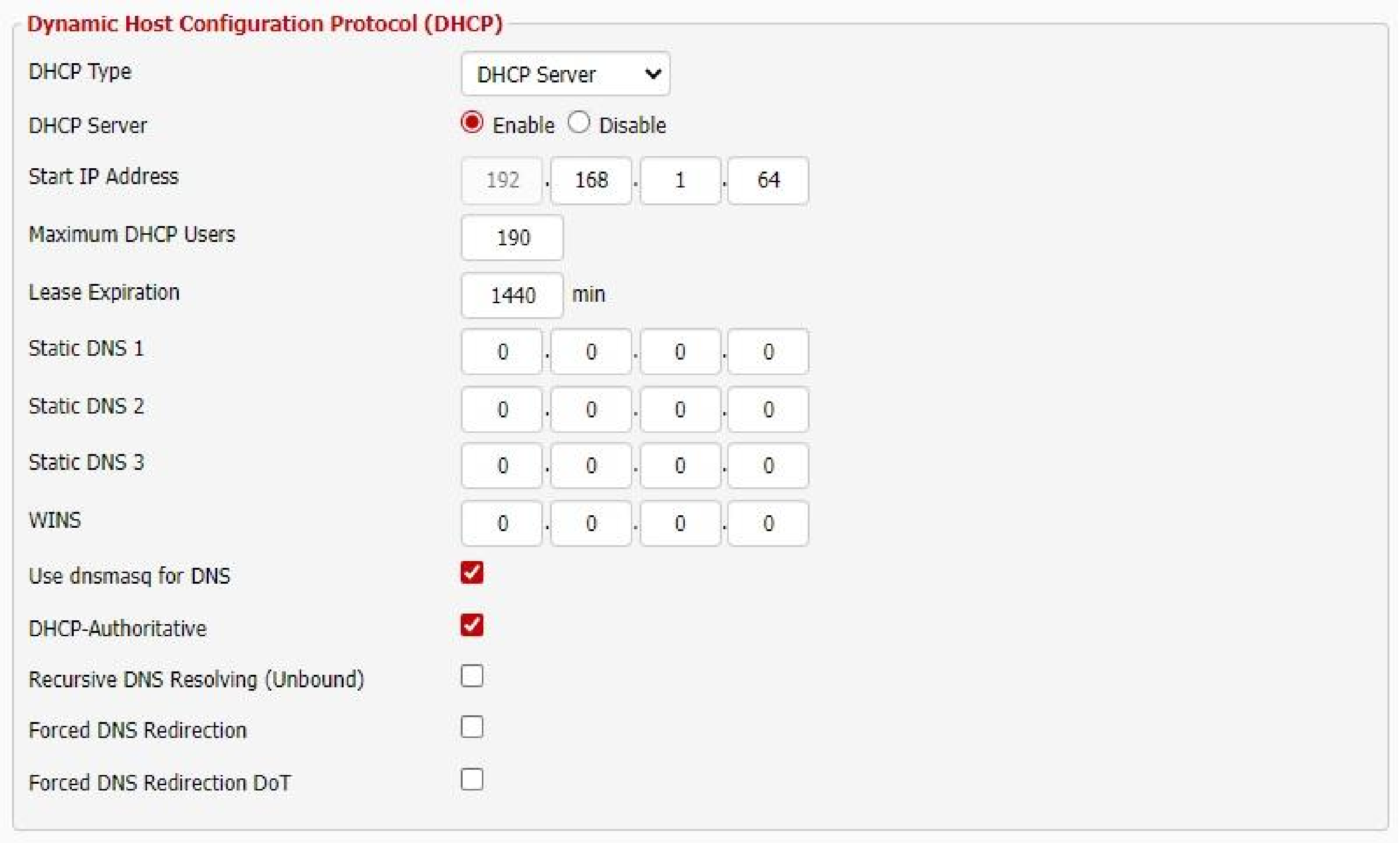
Network Setup

Router IP

Local IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 255 . 0
Gateway	0 . 0 . 0 . 0
Local DNS	0 . 0 . 0 . 0

Setup > Basic Setup > Network Setup

2.1.4 Network Address Server Settings (DHCP)



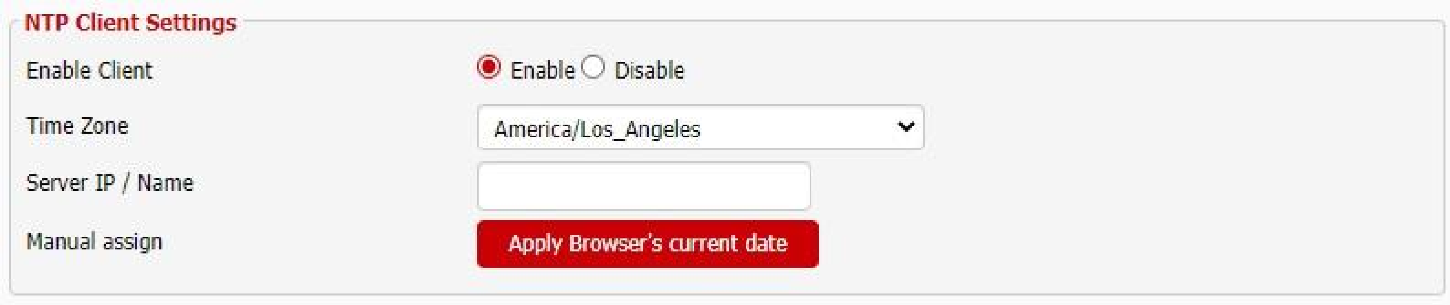
Dynamic Host Configuration Protocol (DHCP)

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	☐

Setup > Basic Setup > Network Address Server Settings

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 router's IP address. ****
Maximum DHCP Users	The maximum number of devices the router will assign IP addresses 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 NTP Client Settings



NTP Client Settings

Enable Client ● Enable ○ Disable

Time Zone America/Los_Angeles

Server IP / Name

Manual assign

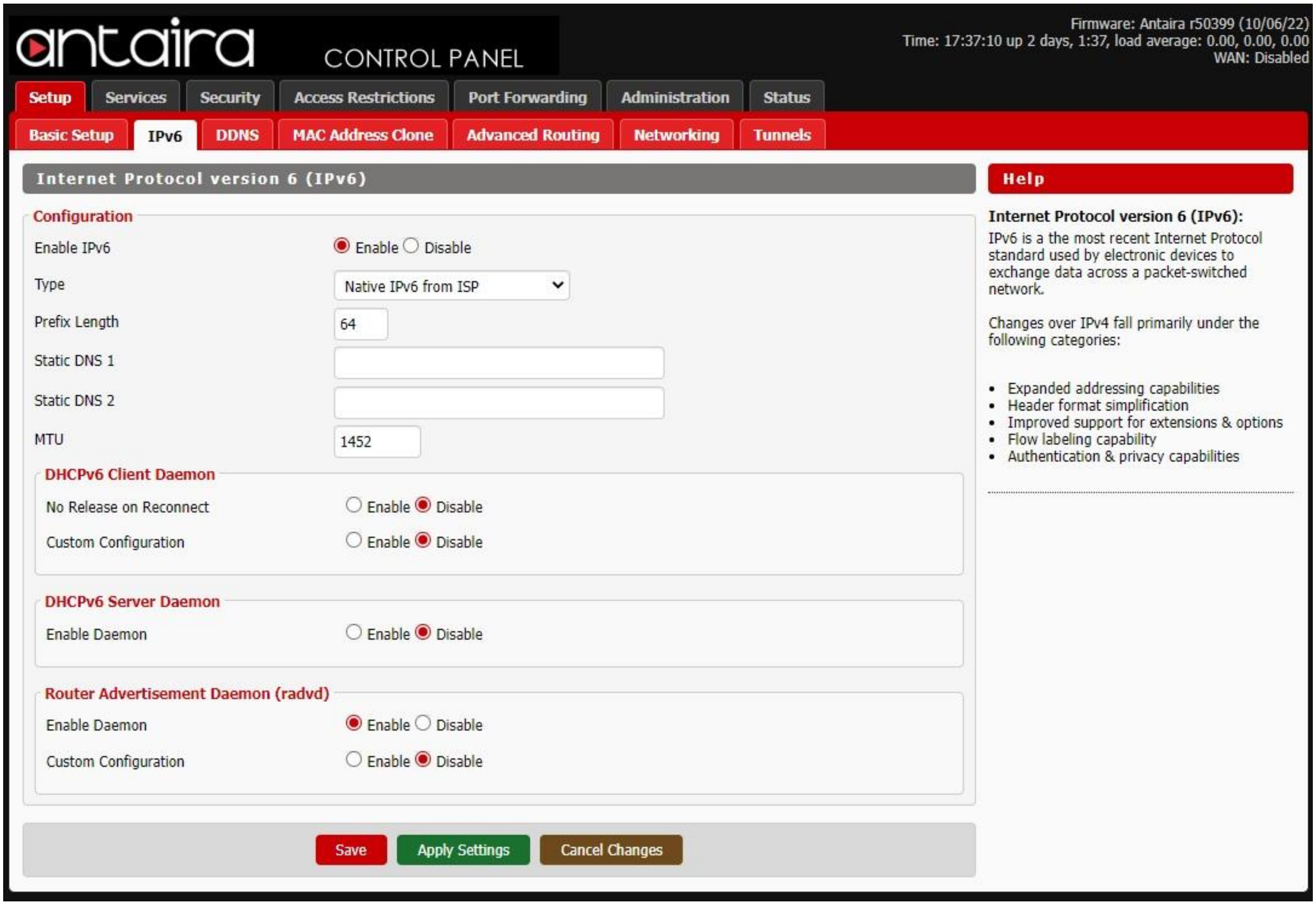
Setup > Basic Setup > NTP Client Settings

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.



Firmware: Antaira r50399 (10/06/22)
Time: 17:37:10 up 2 days, 1:37, load average: 0.00, 0.00, 0.00
WAN: Disabled

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

Help

Internet Protocol version 6 (IPv6):

IPv6 is a the most recent Internet Protocol standard used by electronic devices to exchange data across a packet-switched network.

Changes over IPv4 fall primarily under the following categories:

- Expanded addressing capabilities
- Header format simplification
- Improved support for extensions & options
- Flow labeling capability
- Authentication & privacy capabilities

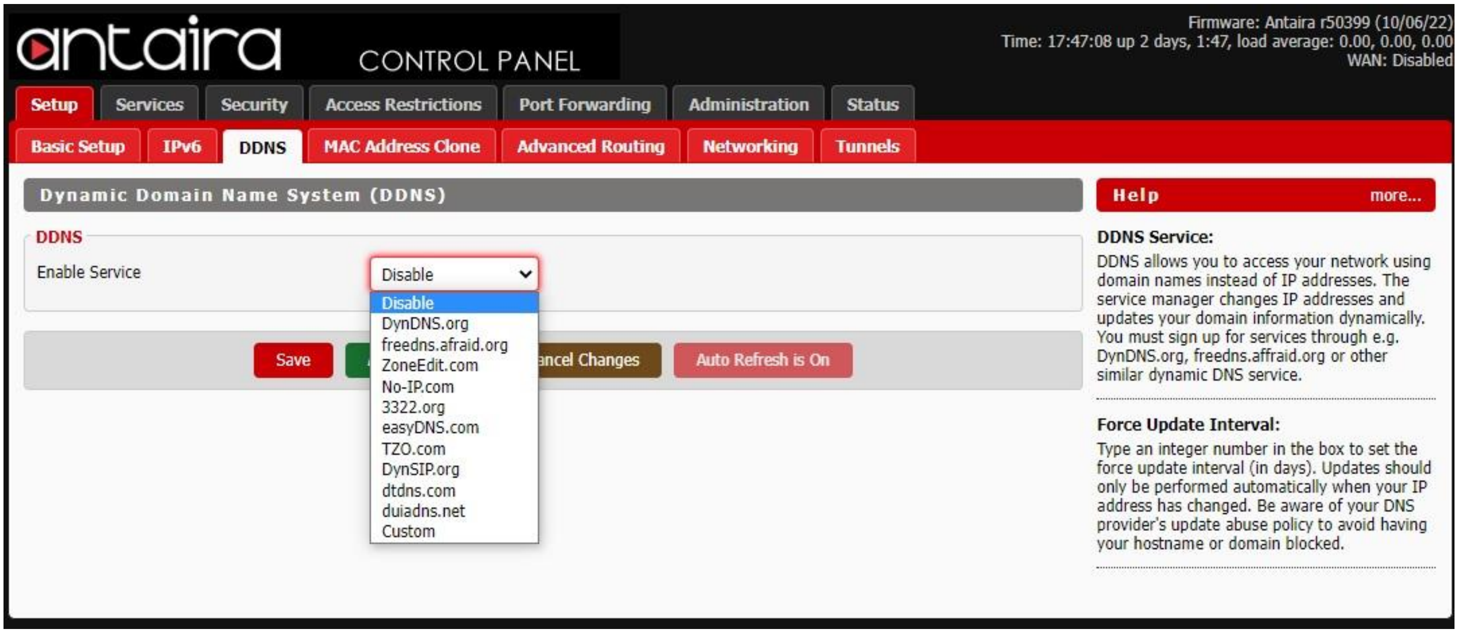
Setup > IPv6

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.



Firmware: Antaira r50399 (10/06/22)
Time: 17:47:08 up 2 days, 1:47, load average: 0.00, 0.00, 0.00
WAN: Disabled

Enable Service: Disable

DDNS Service:
DDNS allows you to access your network using domain names instead of IP addresses. The service manager changes IP addresses and updates your domain information dynamically. You must sign up for services through e.g. DynDNS.org, freedns.affraid.org or other similar dynamic DNS service.

Force Update Interval:
Type an integer number in the box to set the force update interval (in days). Updates should only be performed automatically when your IP address has changed. Be aware of your DNS provider's update abuse policy to avoid having your hostname or domain blocked.

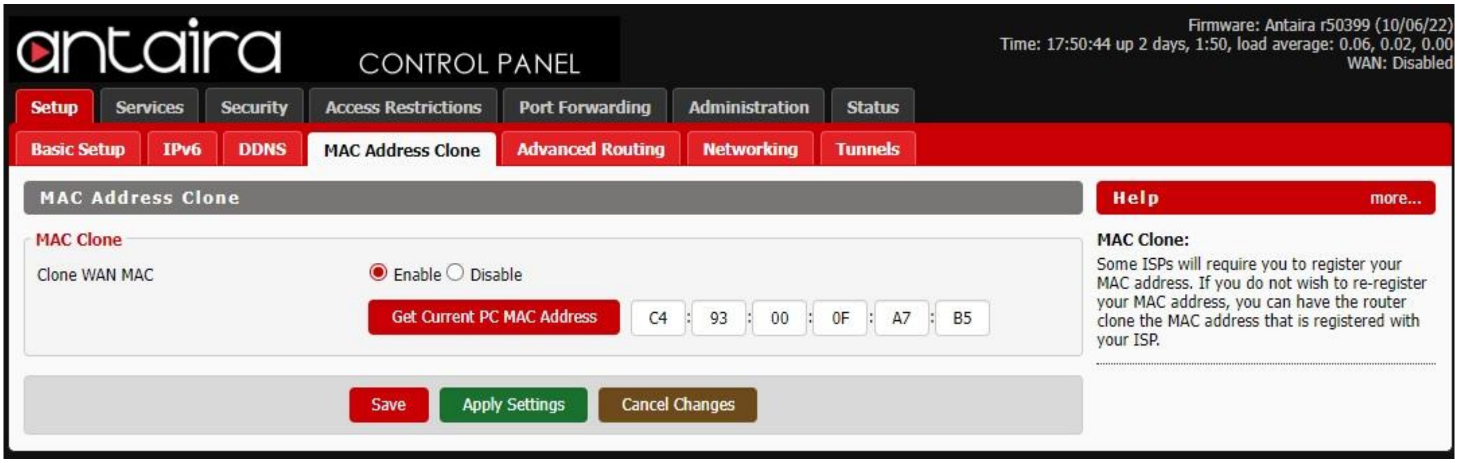
Setup > DDNS

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 user's 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	This 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.



Firmware: Antaira r50399 (10/06/22)
Time: 17:50:44 up 2 days, 1:50, load average: 0.06, 0.02, 0.00
WAN: Disabled

MAC Clone

Clone WAN MAC ● Enable ○ Disable

C4 : 93 : 00 : 0F : A7 : B5

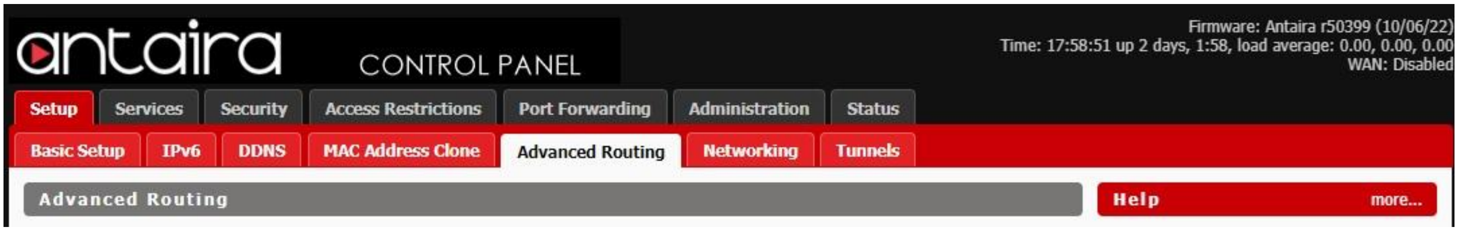
MAC Clone:
Some ISPs will require you to register your MAC address. If you do not wish to re-register your MAC address, you can have the router clone the MAC address that is registered with your ISP.

Setup > MAC Address Clone

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 your 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.



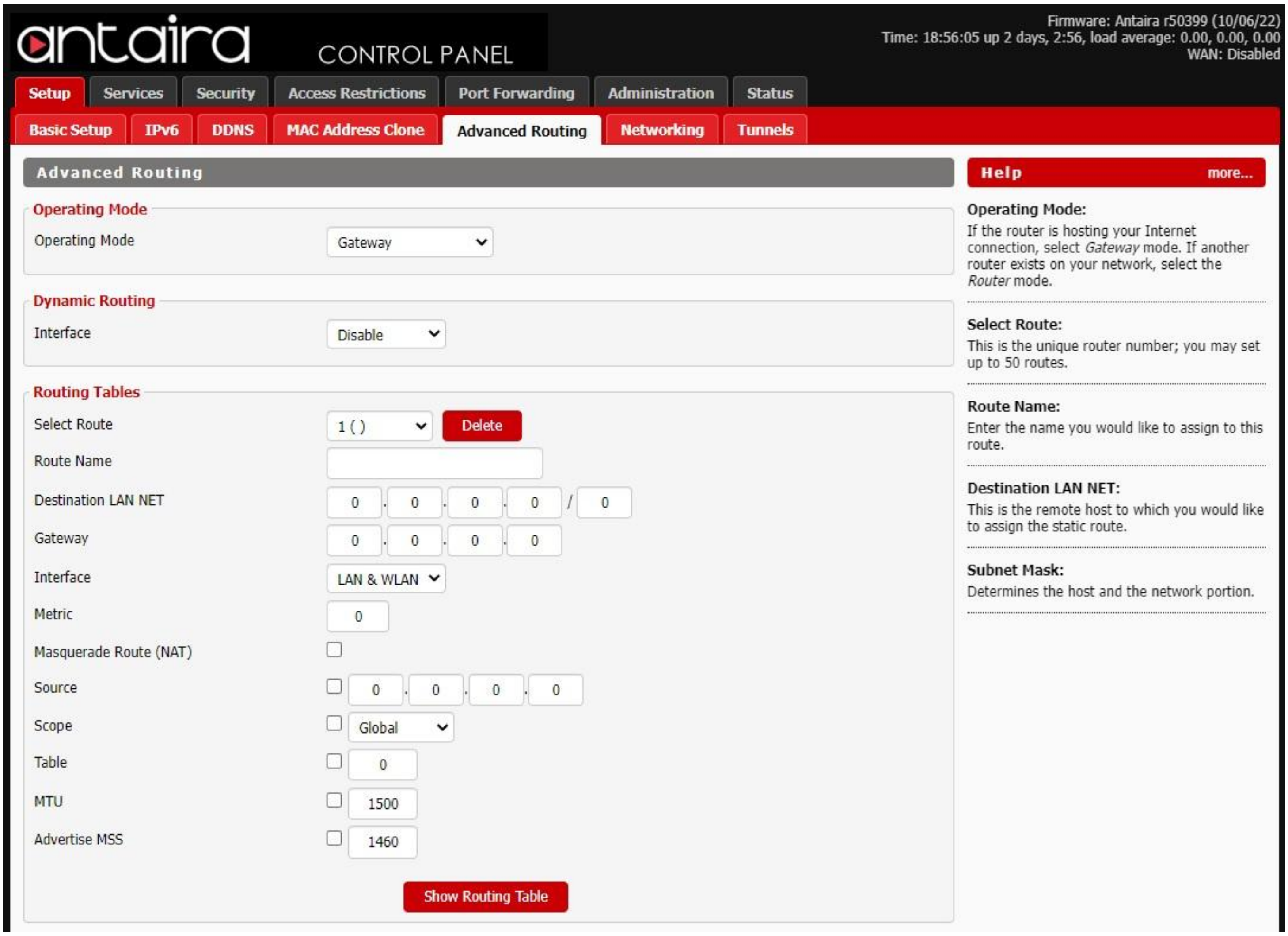
Firmware: Antaira r50399 (10/06/22)
Time: 17:58:51 up 2 days, 1:58, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Setup > Advanced Routing

2.5.1 Gateway

In the Gateway operating mode, the router will route packets between the LAN/WAN 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.



Firmware: Antaira r50399 (10/06/22)
Time: 18:56:05 up 2 days, 2:56, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode: Gateway

Dynamic Routing

Interface: Disable

Routing Tables

Select Route	1 ( )
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

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
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.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

Subnet Mask:
Determines the host and the network portion.

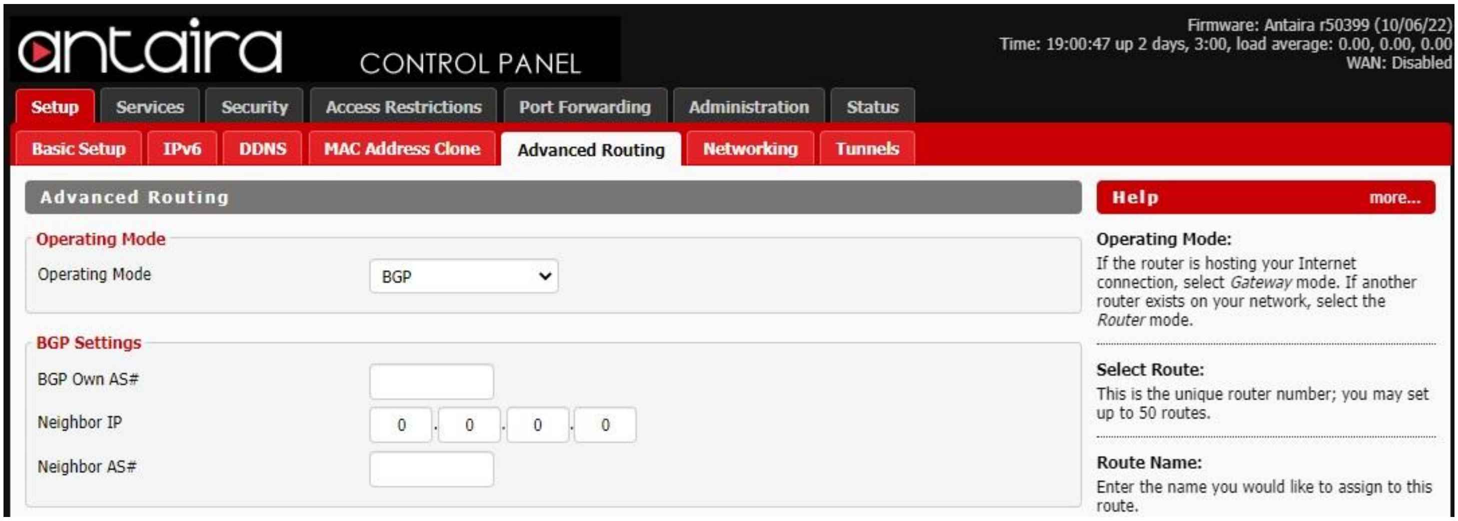
Setup > Advanced Routing > Operating Mode > Gateway

Gateway	Description
Operating Mode	**Gateway:** If the router is hosting the Internet connection, the router will perform NAT in Gateway mode.

	BGP: Border 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.

2.5.2 BGP

Border Gateway Protocol (BGP) is the core routing protocol of the Internet, generally used by Internet Service Providers to establish routing amongst each other. It is also used on private networks to create multi-home networks. BGP is designed to create a redundant link to the Internet using multiple Internet Service Providers.



Firmware: Antaira r50399 (10/06/22)
Time: 19:00:47 up 2 days, 3:00, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode: BGP

BGP Settings

BGP Own AS#:

Neighbor IP: 0 . 0 . 0 . 0

Neighbor AS#:

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
This is the unique router number; you may set up to 50 routes.

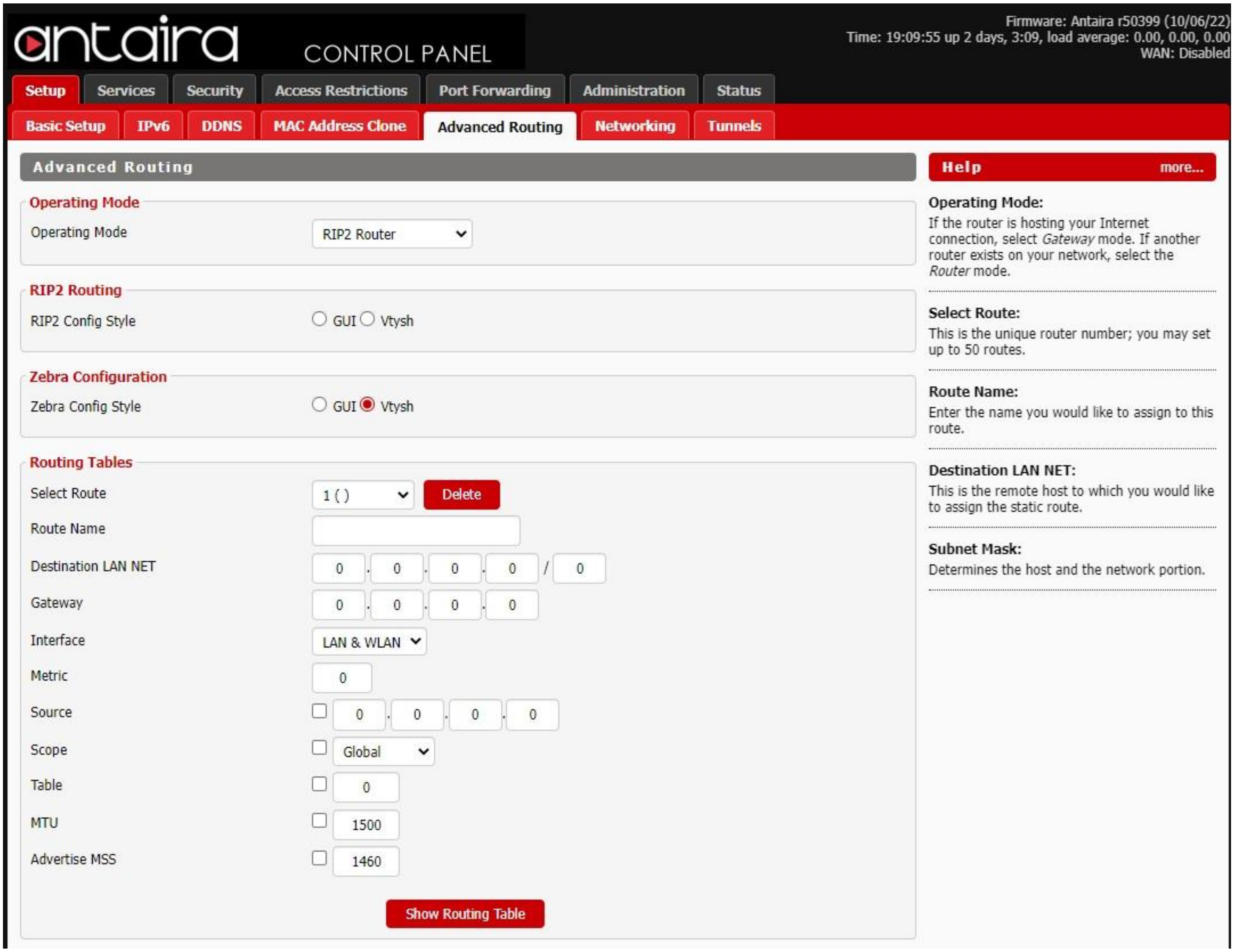
Route Name:
Enter the name you would like to assign to this route.

Setup > Advanced Routing > Operating Mode > BGP

BGP	Description
BGP Own AS#	Autonomous System Number.
Neighbor IP	IPv4 address of neighbor system.
Neighbor AS#	Autonomous System Number of Neighboring systems.
Zebra Config Style	Select the style for the Routing Software package (Zebra).
Select Set Number	Select the Route set (1-64).
Route Name	Give the route a name.
Metric	An integer giving weight to the cost of the route.
Destination LAN NET	Select the style for the Routing Software package (Zebra).
Subnet Mask	Subnet mask of destination LAN.
Gateway	Gateway IP address.
Interface	Select the interface for the path of the route.

2.5.3 RIP2 Router

Routing Information Protocol (RIP), an older protocol and should be used only when an existing network does not have OSPF compliant equipment.



Firmware: Antaira r50399 (10/06/22)
Time: 19:09:55 up 2 days, 3:09, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode: RIP2 Router

RIP2 Routing

RIP2 Config Style: ○ GUI ○ Vtysh

Zebra Configuration

Zebra Config Style: ○ GUI ● Vtysh

Routing Tables

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

Help

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
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.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

Subnet Mask:
Determines the host and the network portion.

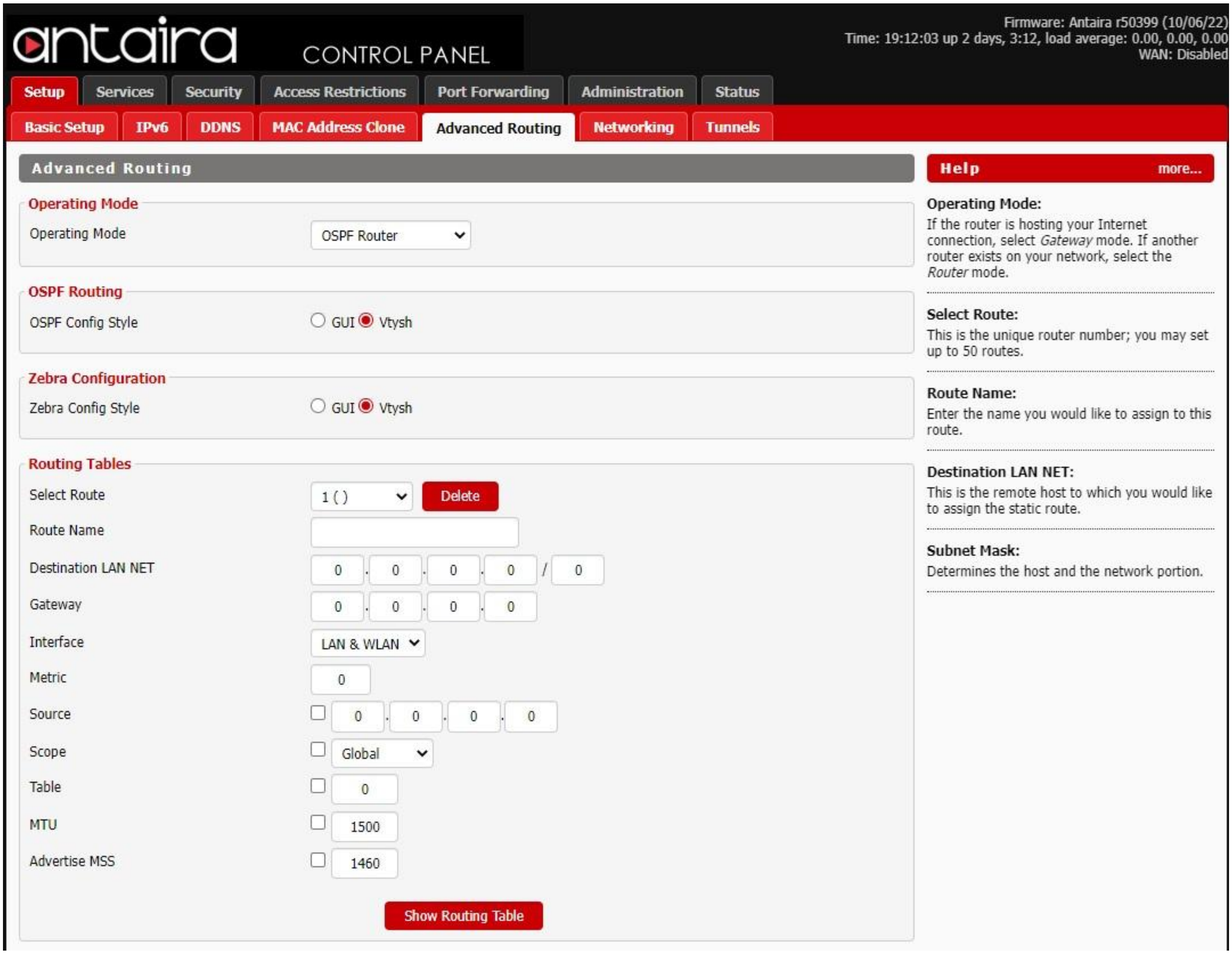
Setup > Advanced Routing > Operating Mode > RIP2 Router

RIP2	Description
RIP2 Config Style	Sets the configuration style for RIP2.
Zebra Config Style	Sets the Zebra configuration style.
Select Set Number	Select the Route set (1-64).
Route Name	Give the route a name.
Metric	An integer giving weight to the cost of the route.
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.

2.5.4 OSPF Router

Open Shortest Path First (OSPF). Using OSPF, a host that obtains a change to a routing table or detects a change in the network will immediately multicast the information to all other hosts in the network so that all will have the same routing table information. This method is more efficient than RIP, which sends the entire routing table to a neighboring host every 30 seconds. OSPF also uses more advanced algorithms to determine the shortest path, whereas RIP simply uses hop counts. If your router is acting as a repeater, OSPF is the recommended protocol to use unless the network has other devices that only support RIP.



Firmware: Antaira r50399 (10/06/22)
Time: 19:12:03 up 2 days, 3:12, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode	OSPF Router

OSPF Routing

OSPF Config Style	○ GUI ● Vtysh

Zebra Configuration

Zebra Config Style	○ GUI ● Vtysh

Routing Tables

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

Help

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
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.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

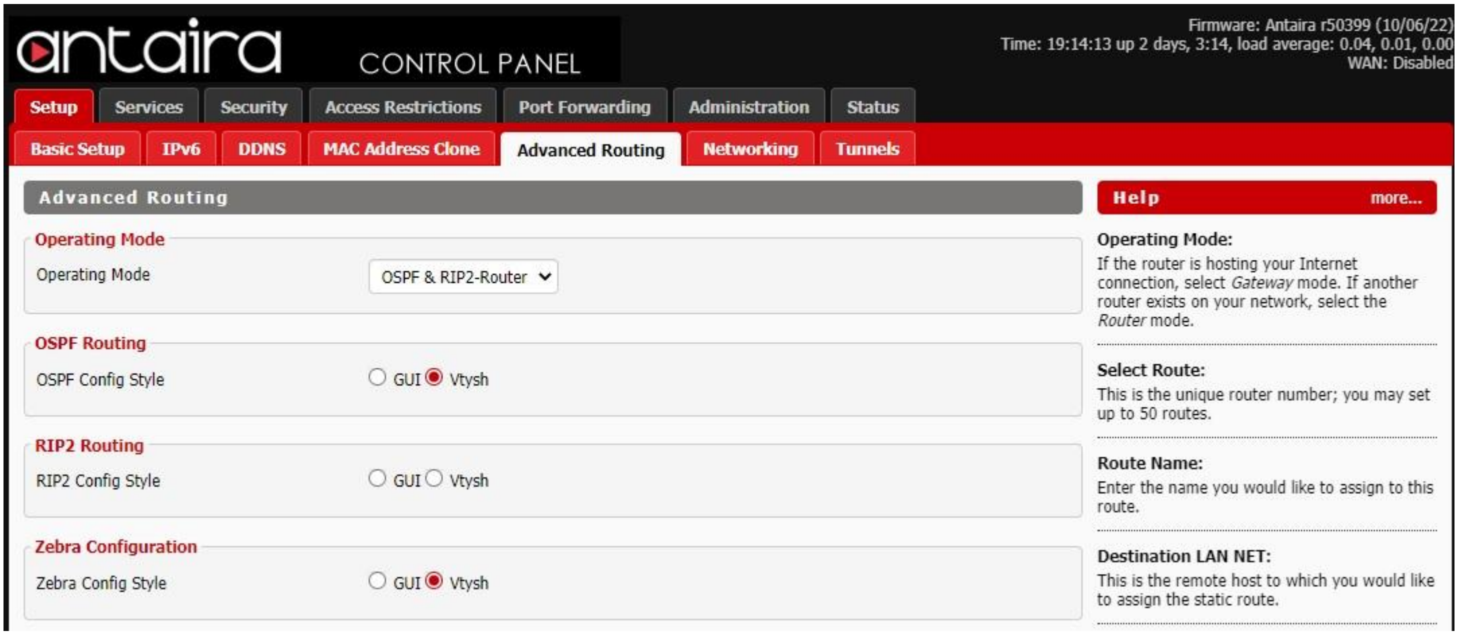
Subnet Mask:
Determines the host and the network portion.

Setup > Advanced Routing > Operating Mode > OSPF Router

OSPF Router	Description
OSPF Config Style	Sets the configuration style for OSPF.
Zebra Config Style	Sets the Zebra configuration style.

Select Set Number	Select the Route set (1-64).
Route Name	Give the route a name.
Metric	An integer giving weight to the cost of the route.
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.

2.5.5 OSPF & RIP2 Router



Firmware: Antaira r50399 (10/06/22)
Time: 19:14:13 up 2 days, 3:14, load average: 0.04, 0.01, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode: OSPF & RIP2-Router

OSPF Routing

OSPF Config Style: ○ GUI ● Vtysh

RIP2 Routing

RIP2 Config Style: ○ GUI ○ Vtysh

Zebra Configuration

Zebra Config Style: ○ GUI ● Vtysh

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
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.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

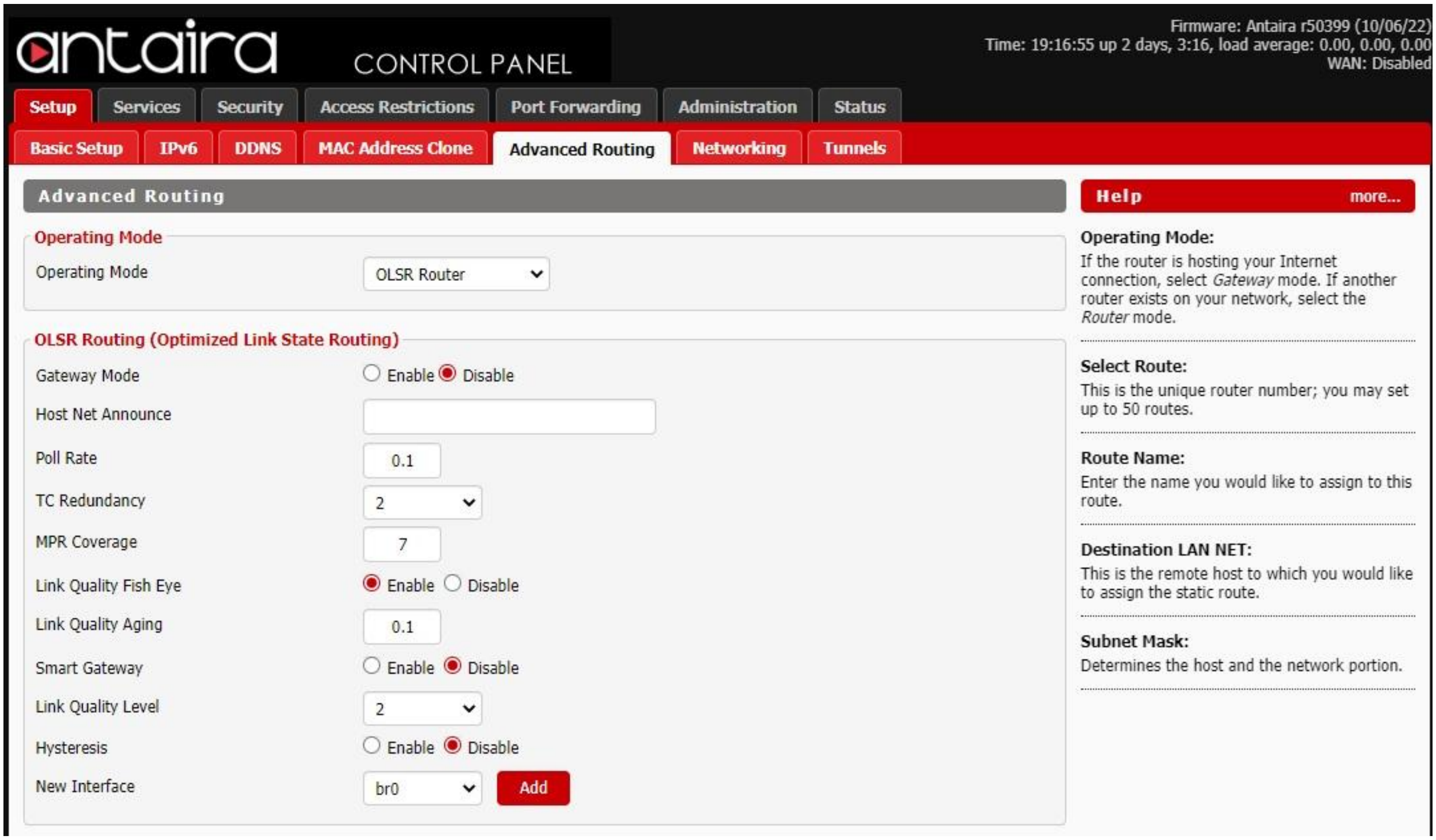
Setup > Advanced Routing > Operating Mode > OSPF & RIP2 Router

OSPF & RIP2 Router	Description
OSPF Config Style	Sets the configuration style for OSPF.
RIP2 Config Style	Sets the configuration style for RIP2.
Zebra Config Style	Sets the Zebra configuration style.
Select Set Number	Select the Route set (1-64).
Route Name	Give the route a name.
Metric	An integer giving weight to the cost of the route.
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.

2.5.6 OLSR Router

Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad-hoc networks, which can also be used on other wireless ad-hoc networks. OLSR is a proactive link-state routing protocol which uses hello and topology control (TC) messages to discover and then disseminate link state information through the mobile ad-hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.



Firmware: Antaira r50399 (10/06/22)
Time: 19:16:55 up 2 days, 3:16, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode: OLSR Router

OLSR Routing (Optimized Link State Routing)

Gateway Mode: ○ Enable ● Disable
Host Net Announce:
Poll Rate: 0.1
TC Redundancy: 2
MPR Coverage: 7
Link Quality Fish Eye: ● Enable ○ Disable
Link Quality Aging: 0.1
Smart Gateway: ○ Enable ● Disable
Link Quality Level: 2
Hysteresis: ○ Enable ● Disable
New Interface: br0

Help

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
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.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

Subnet Mask:
Determines the host and the network portion.

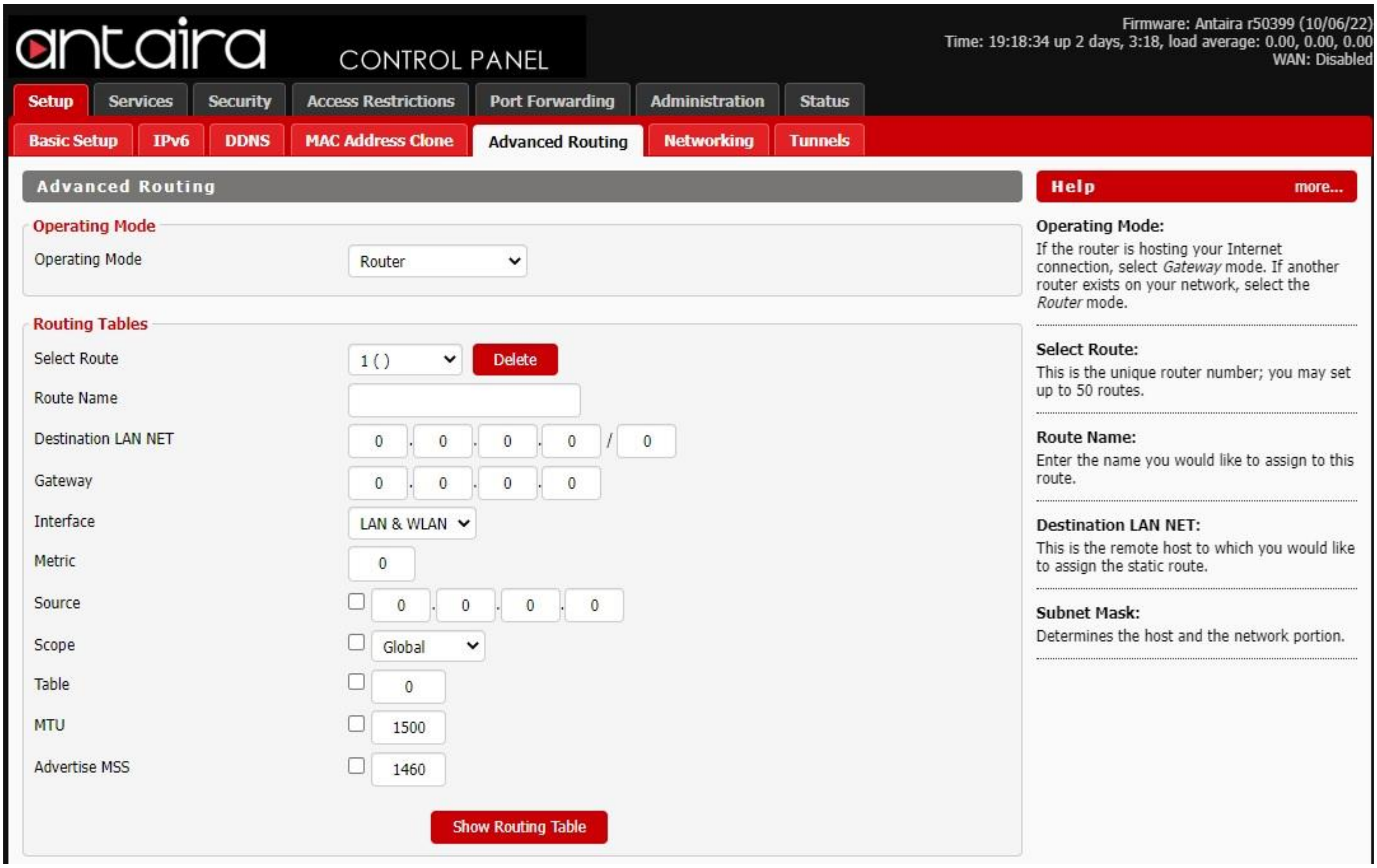
Setup > Advanced Routing > Operating Mode > OLSR Router

OLSR Router	Description
Gateway Mode	Enable or disable feature.
Host Net Announce	Enter a host net announce.
Poll Rate	Set the poll rate interval.
TC Redundancy	Set the TC Redundancy.

MPR Coverage	Set the MPR Coverage.
Link Quality Fish Eye	Enable or disable this feature.
Link Quality Aging	Set the link quality aging.
Smart Gateway	Enable or disable this feature.
Link Quality Level	Set the link quality level.
Hysteresis	Enable or disable this feature.
New Interface	Add a new interface.
Select Set Number	Select the Route set (1-64).
Route Name	Give the route a name.
Metric	An integer giving weight to the cost of the route.
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.

2.5.7 Router

Router Mode allows users to set static routes.



Firmware: Antaira r50399 (10/06/22)
Time: 19:18:34 up 2 days, 3:18, load average: 0.00, 0.00, 0.00
WAN: Disabled

Advanced Routing

Operating Mode

Operating Mode	Router

Routing Tables

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

Operating Mode:
If the router is hosting your Internet connection, select *Gateway* mode. If another router exists on your network, select the *Router* mode.

Select Route:
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.

Destination LAN NET:
This is the remote host to which you would like to assign the static route.

Subnet Mask:
Determines the host and the network portion.

Setup > Advanced Routing > Operating Mode > Router

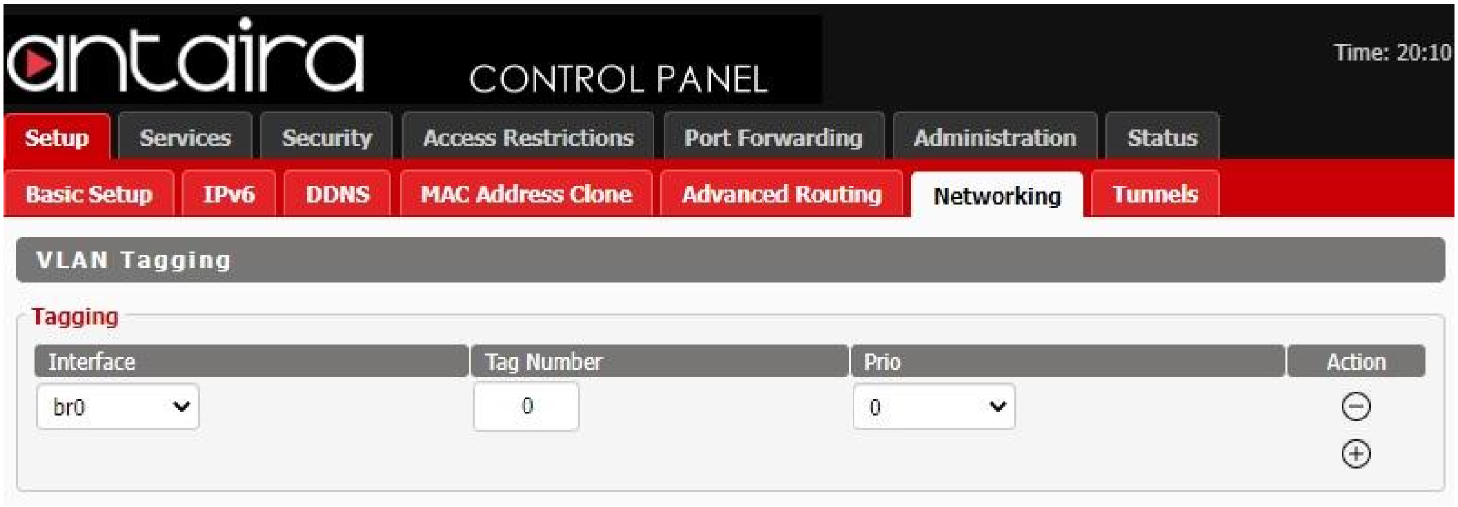
Router	Description
Select Set Number	This is the unique router number. You may set up to 50 routes.
Route Name	Enter the name you would like to assign to this route.
Metric	An integer giving weight to the cost of the route.
Destination LAN NET	This is the remote host to which you would like to assign 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.



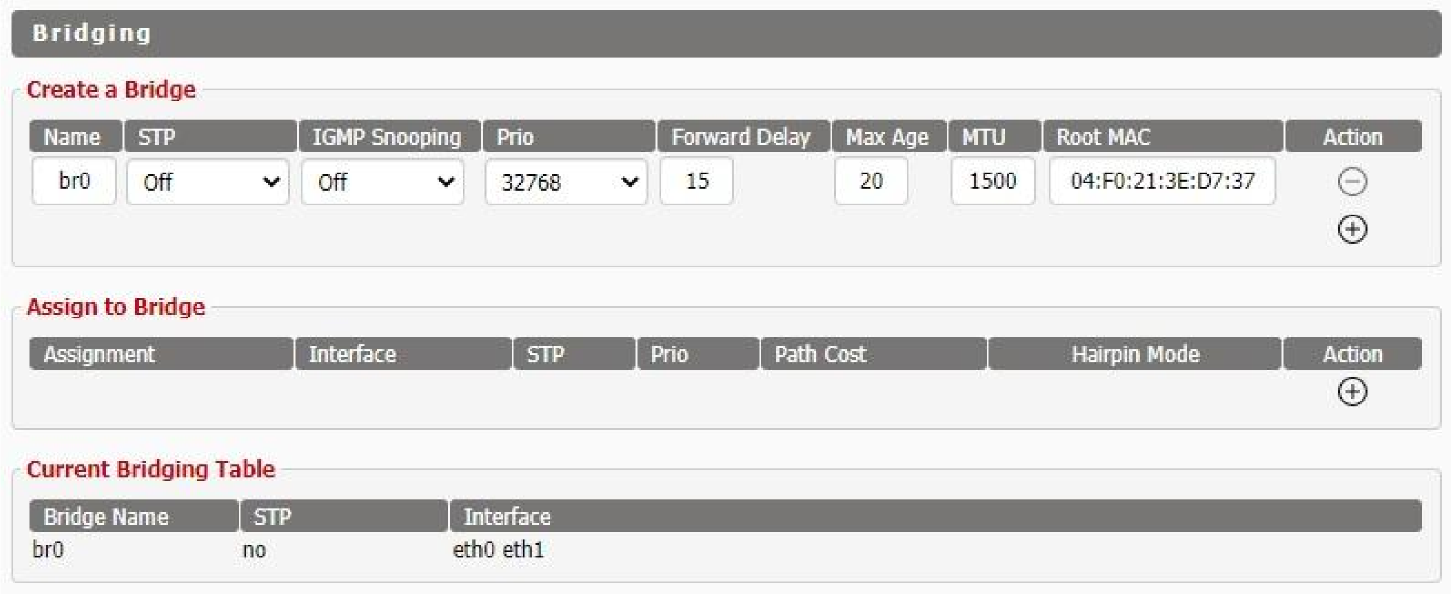
VLAN Tagging

Tagging

Interface	Tag Number	Prio	Action
br0	0	0	⊖ ⊕

Setup > Networking > VLAN Tagging

2.6.2 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	04:F0:21:3E:D7:37	⊖ ⊕

Assign to Bridge

Assignment	Interface	STP	Prio	Path Cost	Hairpin Mode	Action
						⊕

Current Bridging Table

Bridge Name	STP	Interface
br0	no	eth0 eth1

Setup > Networking > Bridging

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

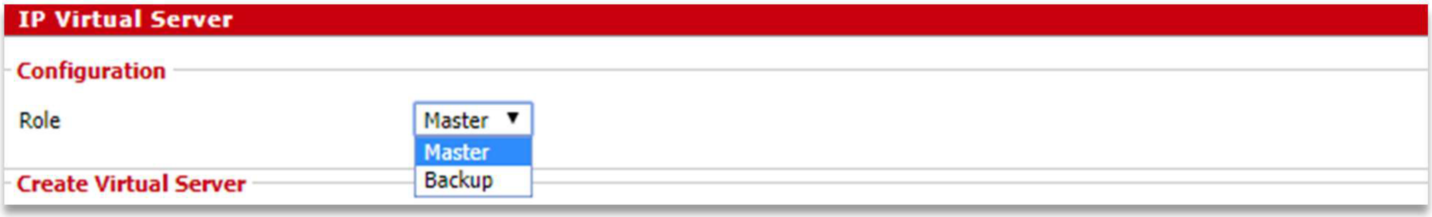
Create Bridge	Description
Add	Create a new network bridge.
STP	Spanning Tree Protocol. Turn on or off.
IGMP Snooping	Turn on or off IGMP Snooping.
Prio	Sets the bridge priority order. (Lower numbers are a higher priority.)

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.
Prio	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


IP Virtual Server

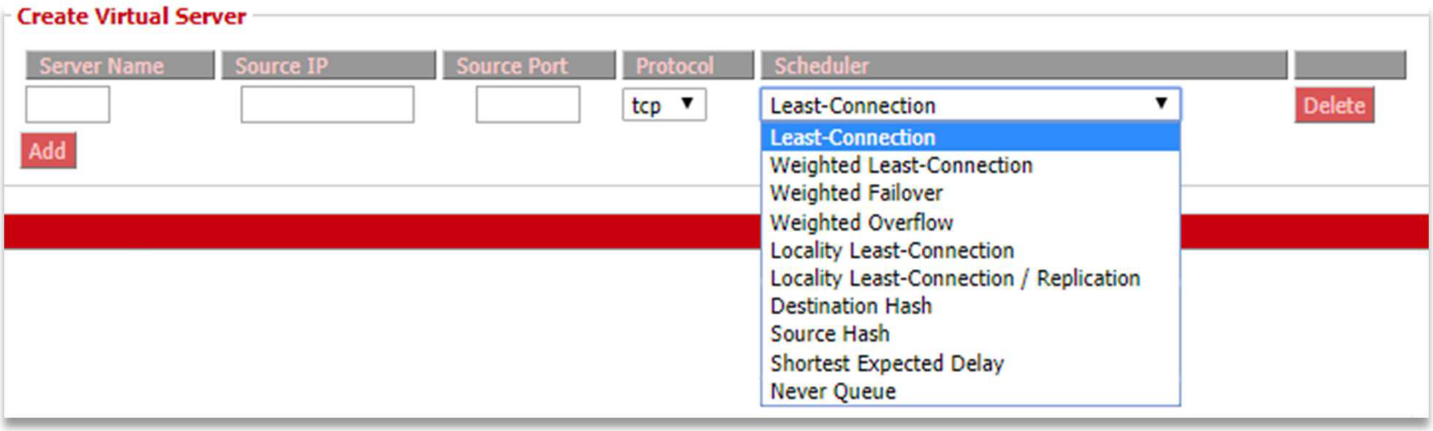
Configuration

Role: Master

Setup > Networking > IP Virtual Server

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

2.6.4 Create Virtual Server



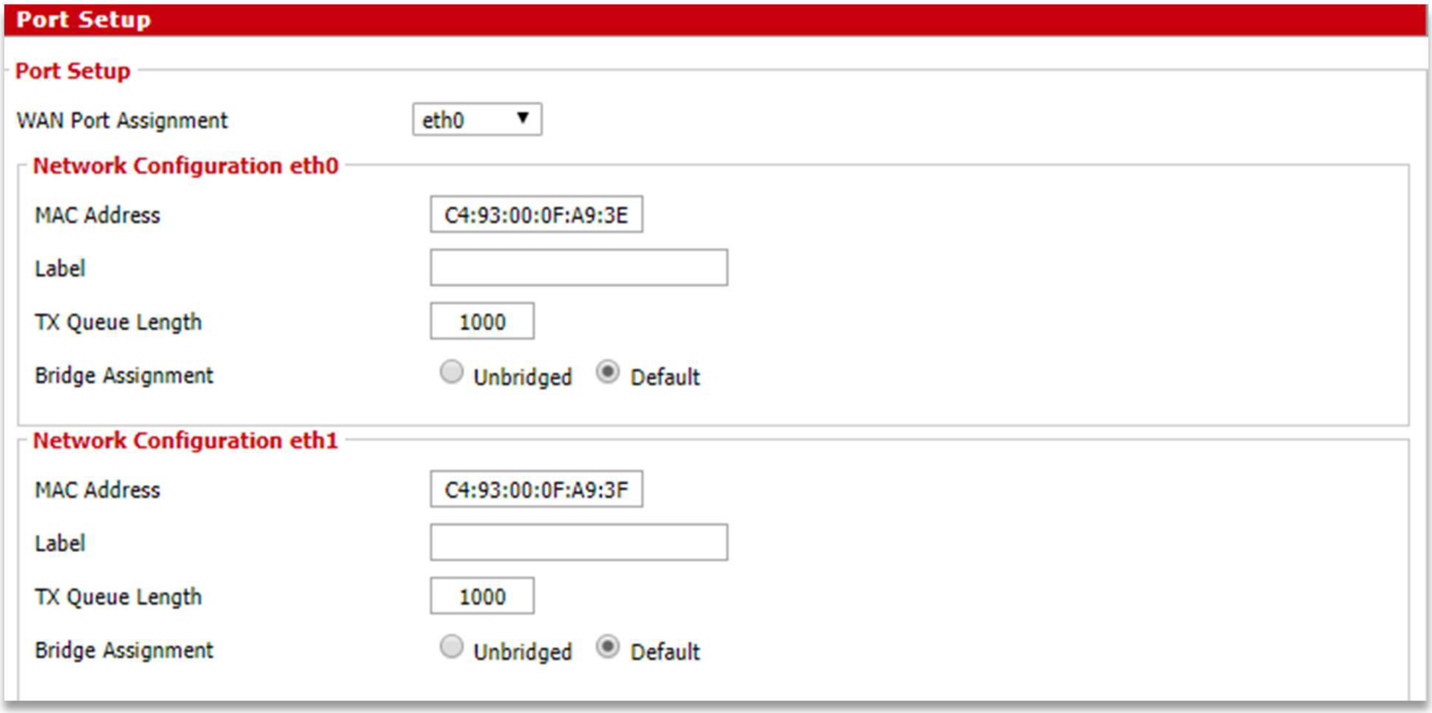
Create Virtual Server

Server Name	Source IP	Source Port	Protocol	Scheduler	
			tcp	Least-Connection	Delete

Setup > Networking > Create Virtual Server

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 Port Setup



Port Setup

Port Setup

WAN Port Assignment: eth0

Network Configuration eth0

MAC Address: C4:93:00:0F:A9:3E

Label:

TX Queue Length: 1000

Bridge Assignment: ○ Unbridged ● Default

Network Configuration eth1

MAC Address: C4:93:00:0F:A9:3F

Label:

TX Queue Length: 1000

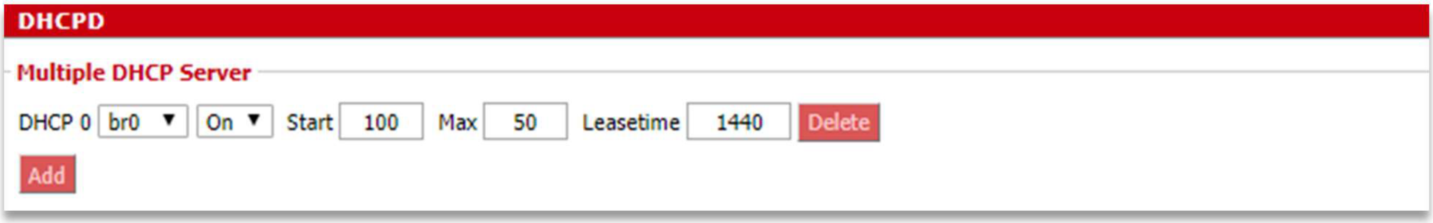
Bridge Assignment: ○ Unbridged ● Default

Setup > Networking > Port Setup

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.

2.6.6 DHCPD

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



DHCPD

Multiple DHCP Server

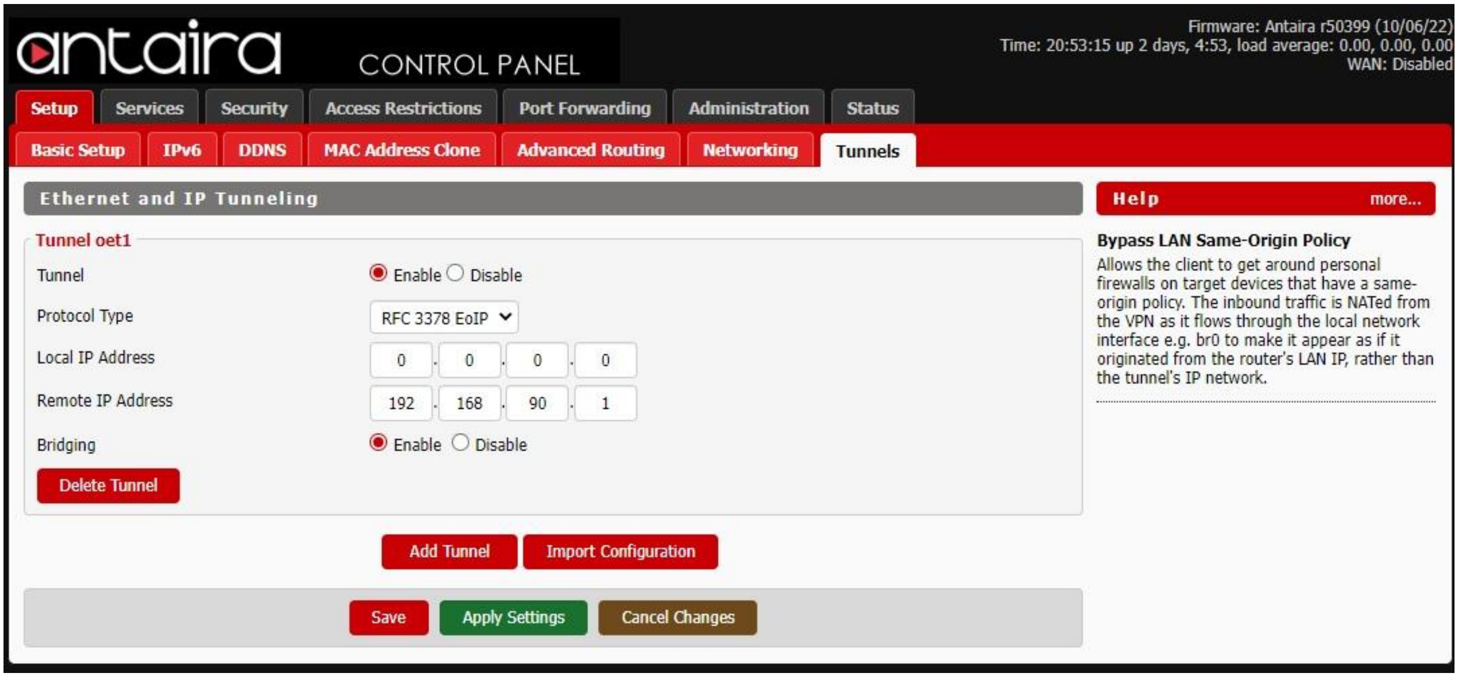
DHCP 0: br0, On, Start 100, Max 50, Leasetime 1440

Setup > Networking > DHCPD

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.



Firmware: Antaira r50399 (10/06/22)
Time: 20:53:15 up 2 days, 4:53, load average: 0.00, 0.00, 0.00
WAN: Disabled

Ethernet and IP Tunneling

Tunnel oet1

Tunnel	● Enable ○ Disable
Protocol Type	RFC 3378 EoIP
Local IP Address	0 . 0 . 0 . 0
Remote IP Address	192 . 168 . 90 . 1
Bridging	● Enable ○ Disable

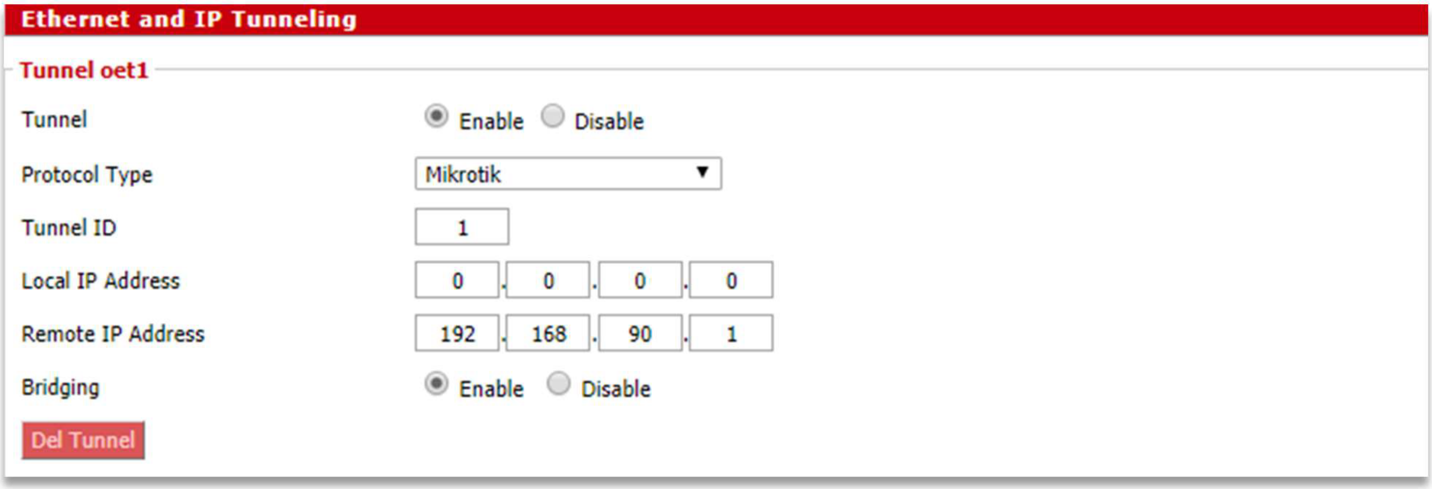
Bypass LAN Same-Origin Policy

Allows the client to get around personal firewalls on target devices that have a same-origin policy. The inbound traffic is NATed from the VPN as it flows through the local network interface e.g. br0 to make it appear as if it originated from the router's LAN IP, rather than the tunnel's IP network.

Setup > Tunnels

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



Ethernet and IP Tunneling

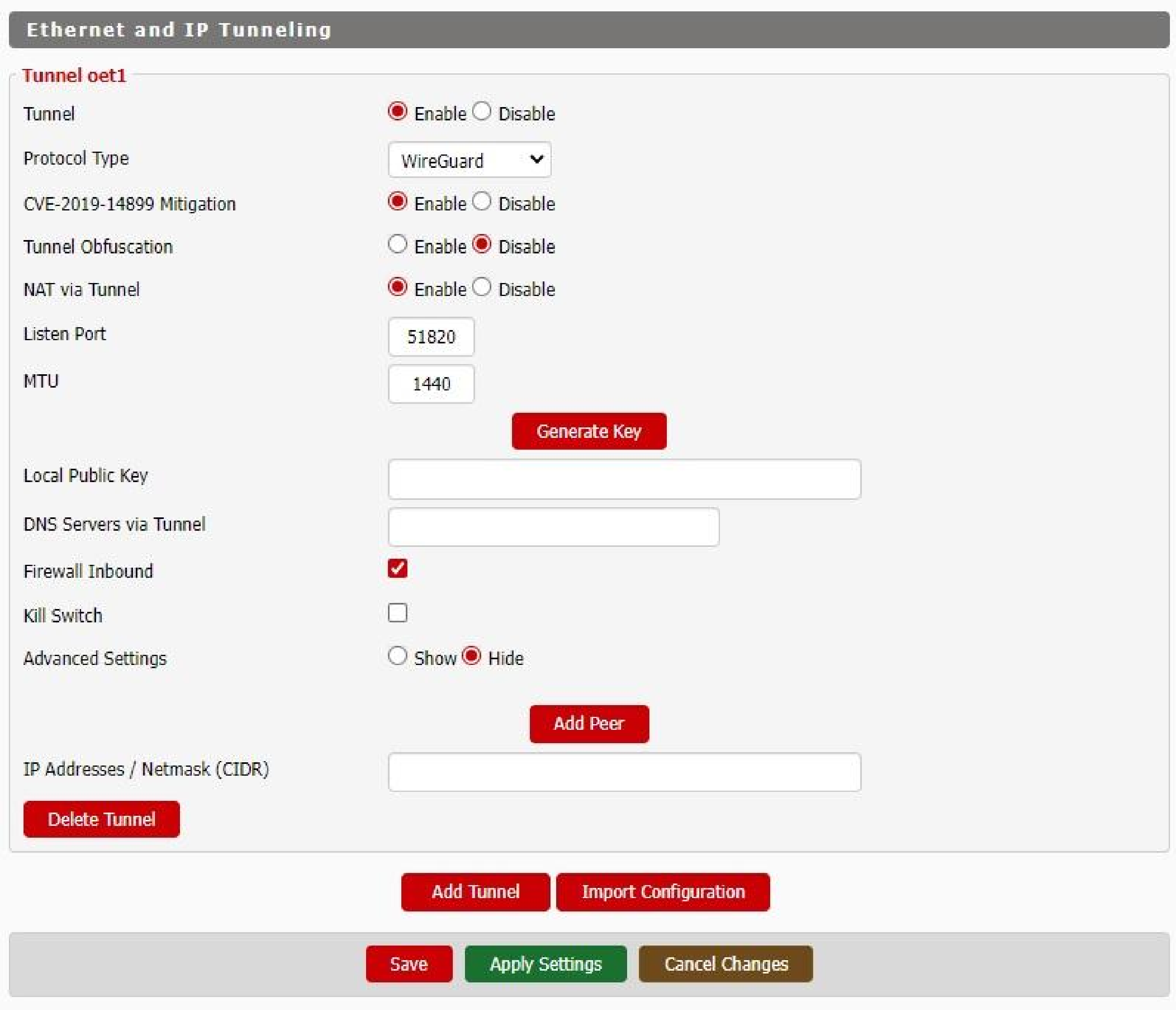
Tunnel oet1

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

Setup > Tunnels > Ethernet and IP Tunneling > Mikrotik

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



Ethernet and IP Tunneling

Tunnel oet1

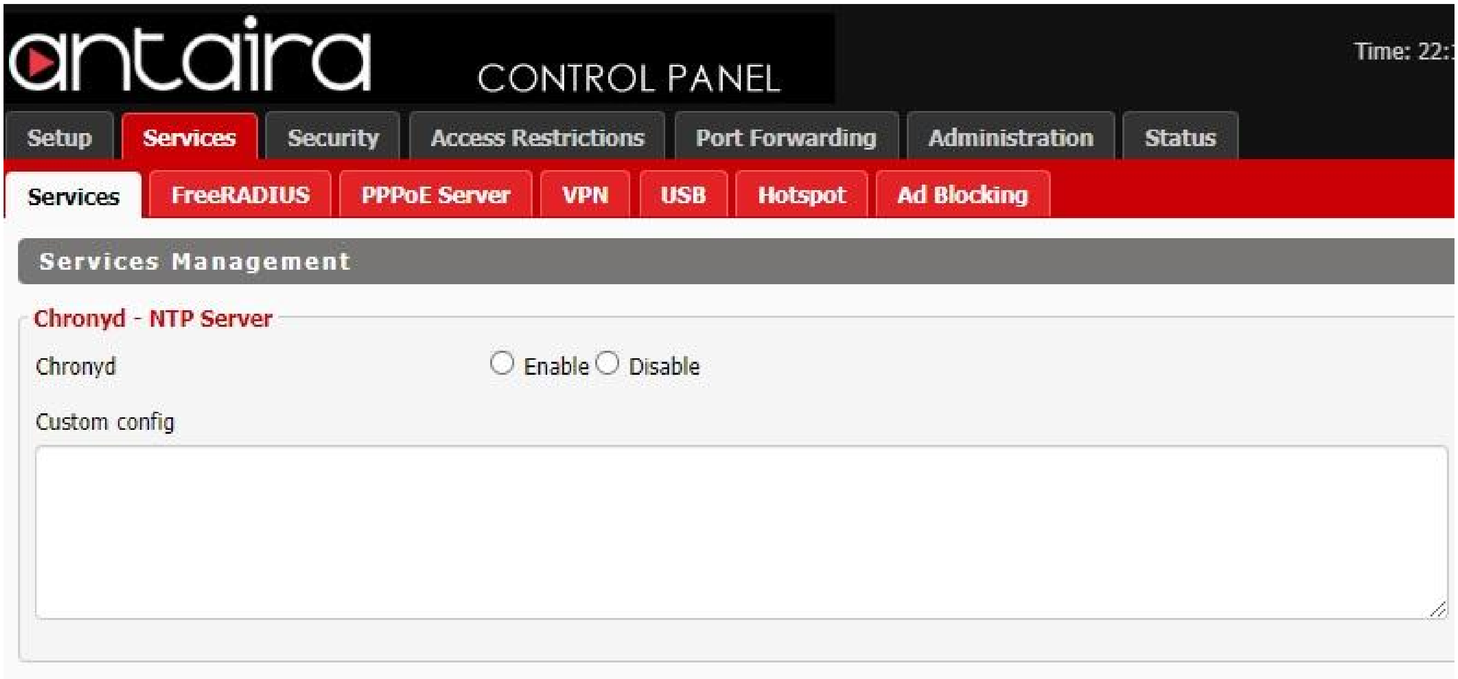
Tunnel	● Enable ○ Disable
Protocol Type	WireGuard
CVE-2019-14899 Mitigation	● Enable ○ Disable
Tunnel Obfuscation	○ Enable ● Disable
NAT via Tunnel	● Enable ○ Disable
Listen Port	51820
MTU	1440
	Generate Key
Local Public Key	
DNS Servers via Tunnel	
Firewall Inbound	☑
Kill Switch	□
Advanced Settings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

Setup > Tunnels > Ethernet and IP Tunneling > WireGuard

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.

4 Services

4.1 Services



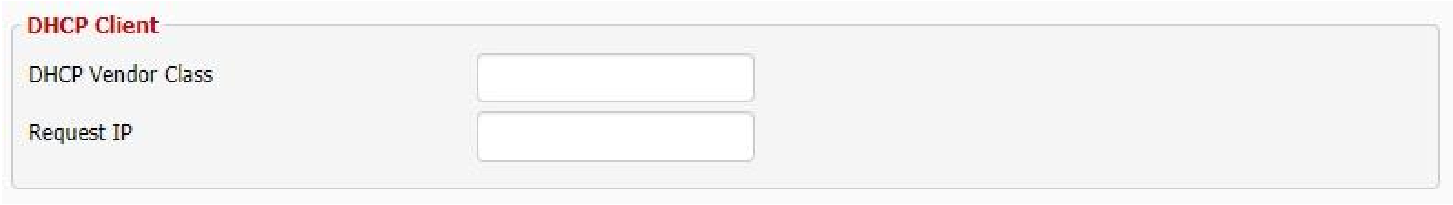
Services Management

Chronyd - NTP Server

Chronyd ○ Enable ○ Disable

Custom config

4.1.1 DHCP Client



DHCP Client

DHCP Vendor Class

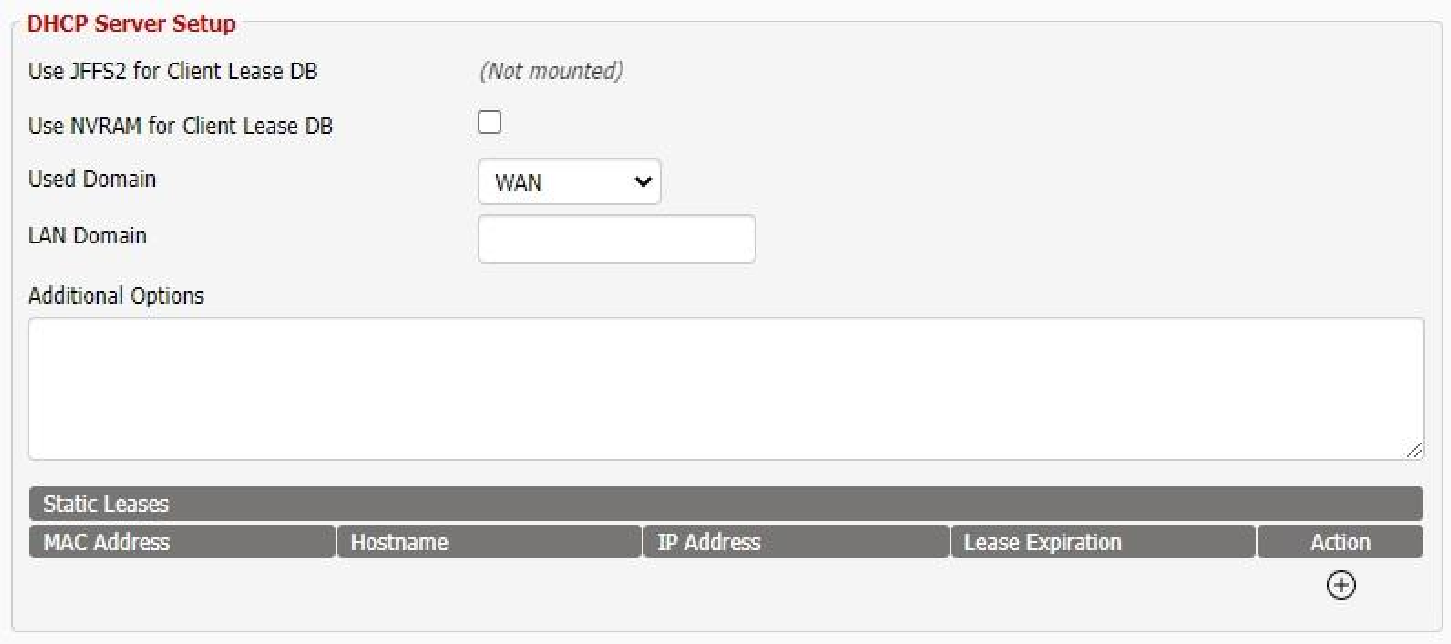
Request IP

Services > Services > DHCP Client

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.



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

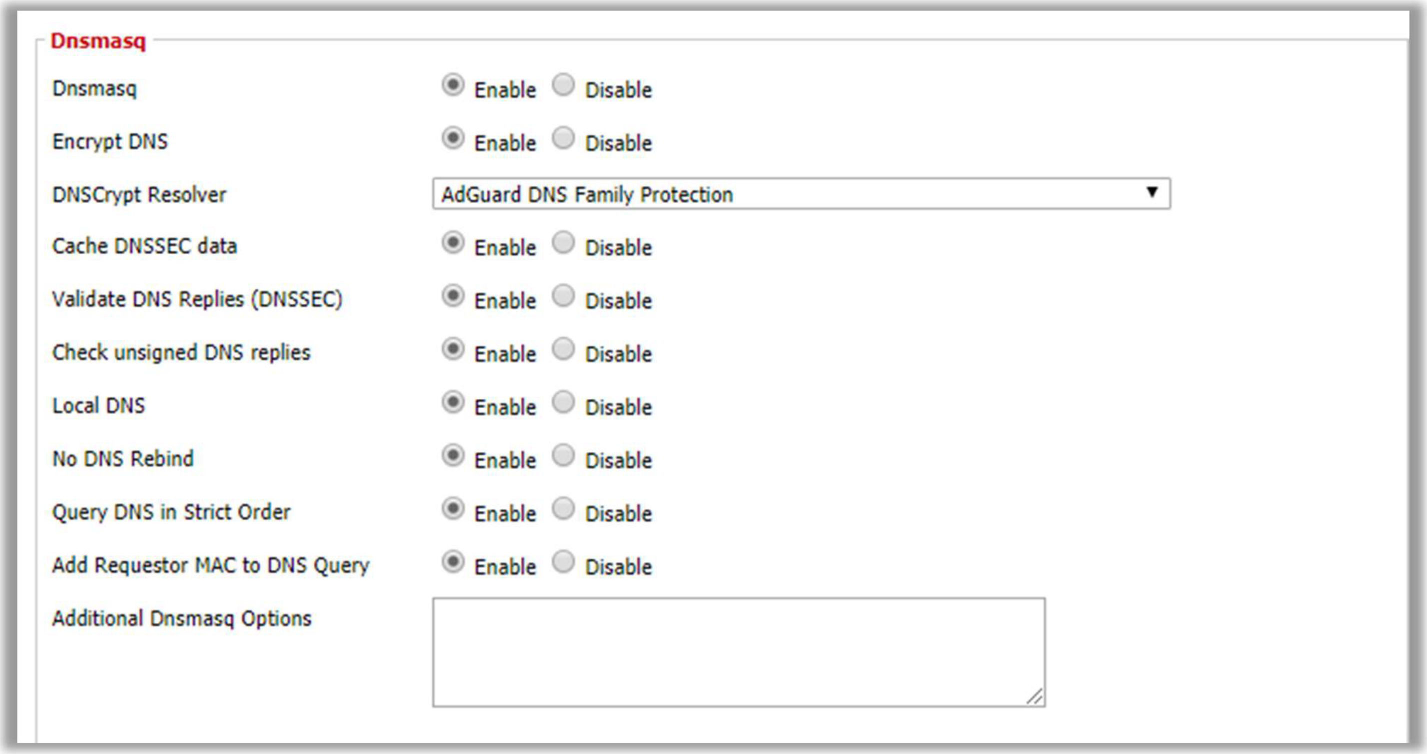
MAC Address	Hostname	IP Address	Lease Expiration	Action

Services > Services > DHCP Server

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 hostnames known to the router from DHCP as well as forwarding and caching DNS entries from remote DNS servers.



Dnsmasq

Dnsmasq ● Enable ○ Disable

Encrypt DNS ● Enable ○ Disable

DNSCrypt Resolver: AdGuard DNS Family Protection ▼

Cache DNSSEC data ● Enable ○ Disable

Validate DNS Replies (DNSSEC) ● Enable ○ Disable

Check unsigned DNS replies ● Enable ○ Disable

Local DNS ● Enable ○ Disable

No DNS Rebind ● Enable ○ Disable

Query DNS in Strict Order ● Enable ○ Disable

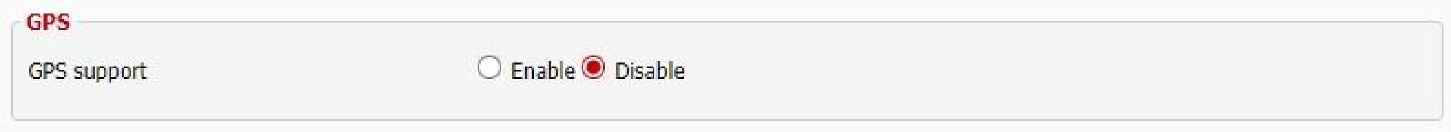
Add Requestor MAC to DNS Query ● Enable ○ Disable

Additional Dnsmasq Options

Services > Services > Dnsmasq

Dnsmasq	Description
Dnsmasq	Enable or disable this feature.
Encrypt DNS	Enable or disable this feature.
DNSCrypt Resolver	
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.

4.1.4 GPS

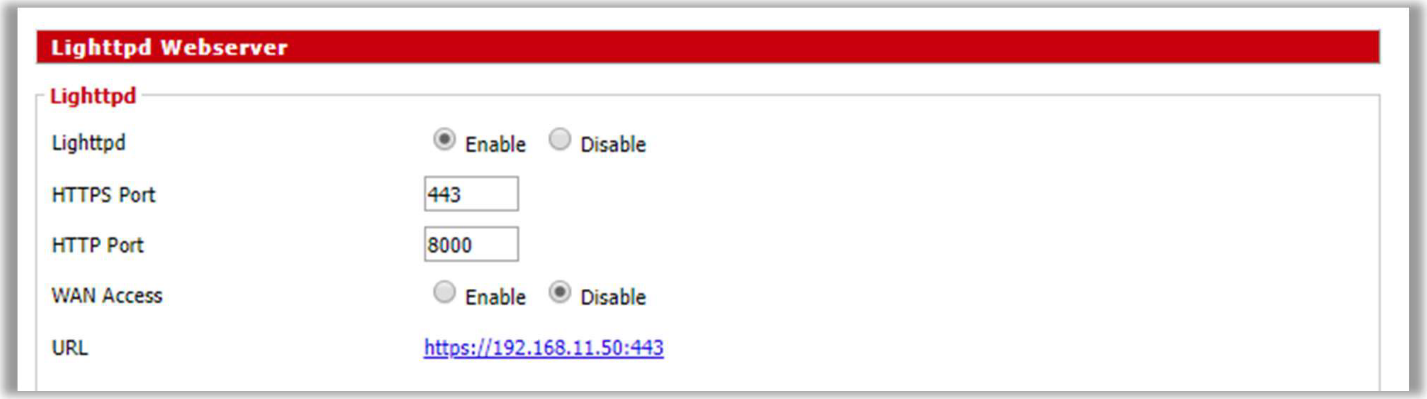


GPS

GPS support ○ Enable ● Disable

Services > Services > GPS

4.1.5 Lighttpd Webserver



Lighttpd Webserver

Lighttpd

Lighttpd ● Enable ○ Disable

HTTPS Port 443

HTTP Port 8000

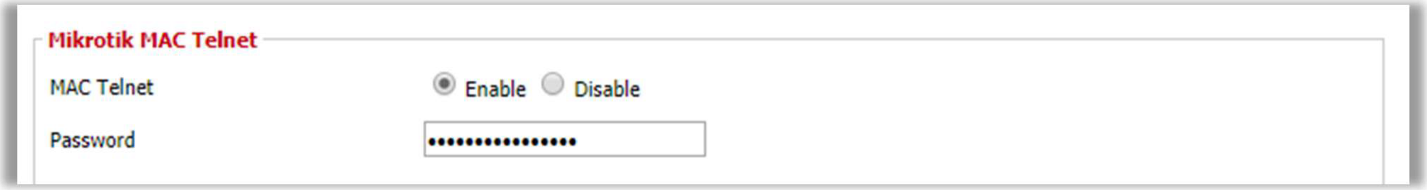
WAN Access ○ Enable ● Disable

URL https://192.168.11.50:443

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.

4.1.6 Mikrotik MAC Telnet



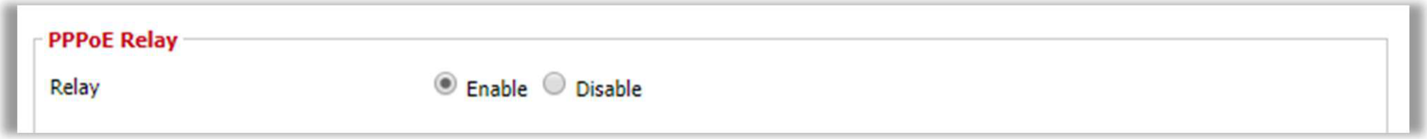
Mikrotik MAC Telnet

MAC Telnet ● Enable ○ Disable

Password ••••••••••••••••

Services > Services > Mikrotik MAC Telnet

4.1.7 PPPoE Relay

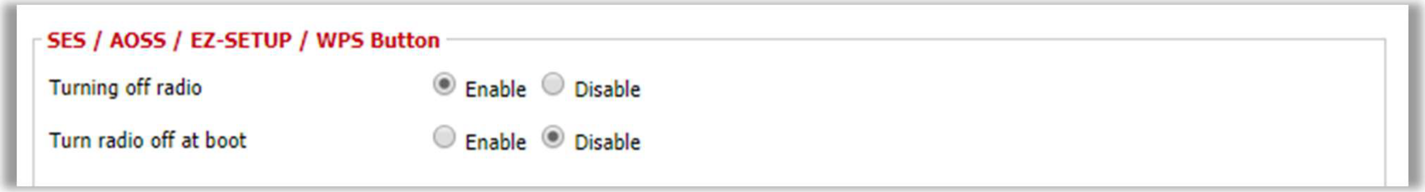


PPPoE Relay

Relay ● Enable ○ Disable

Services > Services > PPPoE Relay

4.1.8 SES/AOSS/EZ-SETUP/WPS Button



SES / AOSS / EZ-SETUP / WPS Button

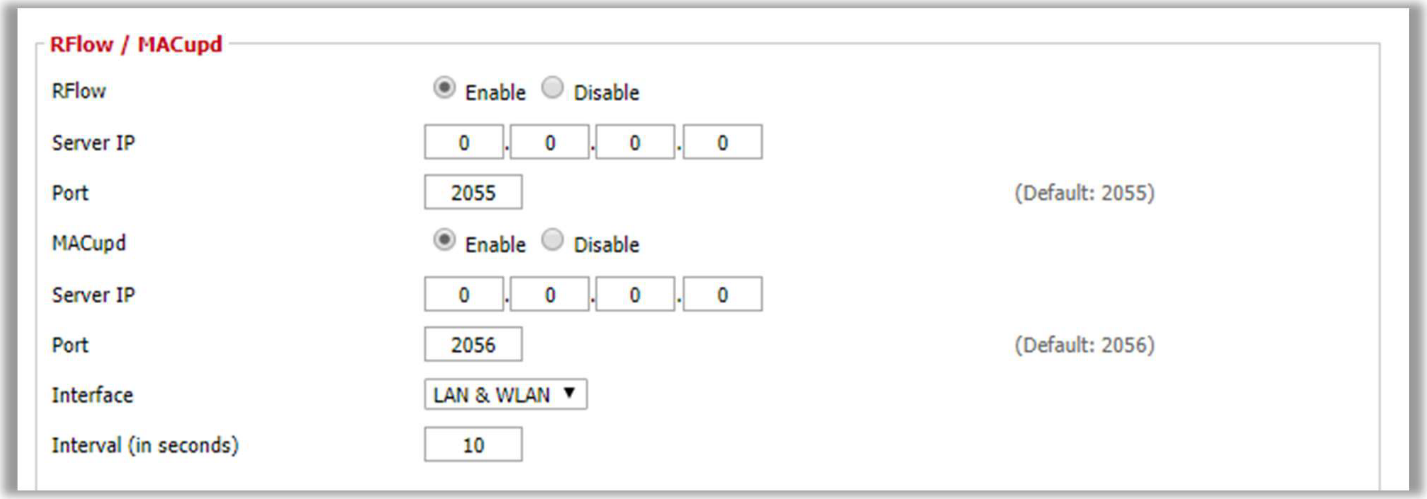
Turning off radio ● Enable ○ Disable

Turn radio off at boot ○ Enable ● Disable

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

4.1.9 RFlow/MACupd

RFlow Collector is a traffic monitoring and management tool that allows users to watch a complete network of routers.



RFlow / MACupd

RFlow ● Enable ○ Disable

Server IP 0 . 0 . 0 . 0

Port 2055 (Default: 2055)

MACupd ● Enable ○ Disable

Server IP 0 . 0 . 0 . 0

Port 2056 (Default: 2056)

Interface LAN & WLAN ▼

Interval (in seconds) 10

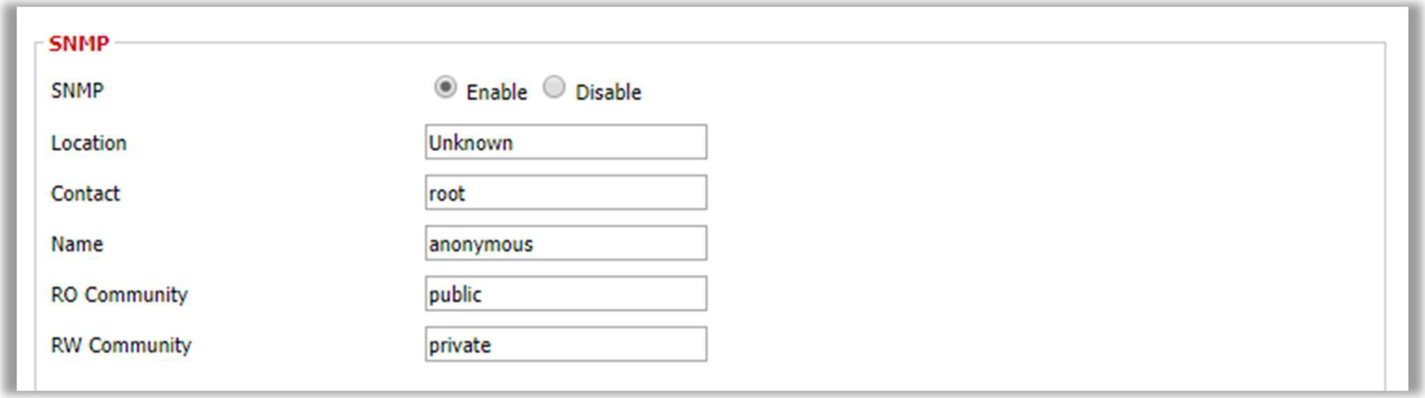
Services > Services > RFlow/MACupd

RFlow/MACupd	Description
RFlow	Enable or disable this feature.
Server IP	Enter the Server IP address.
Port	Enter a port number. Default is port 2055.
MACupd	Enable or disable MACupd.
Server IP	Enter the server IP address.

Port	Enter a port number. Default is port 2056.
Interface	Select an interface.
Interval	Set the interval in seconds.

4.1.10 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.



SNMP

SNMP ● Enable ○ Disable

Location: Unknown

Contact: root

Name: anonymous

RO Community: public

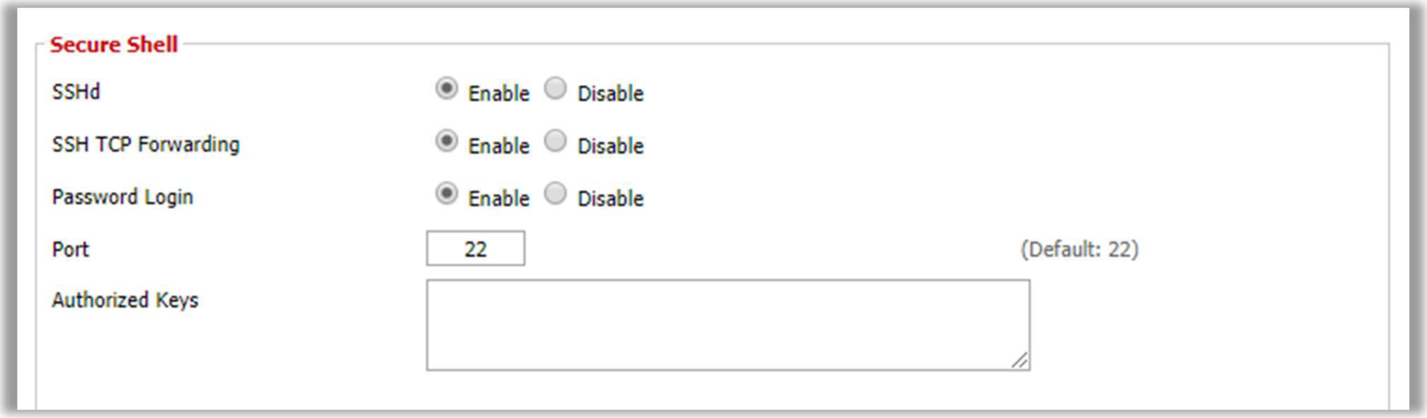
RW Community: private

Services > Services > SNMP

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.

4.1.11 Secure Shell

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



Secure Shell

SSHd ● Enable ○ Disable

SSH TCP Forwarding ● Enable ○ Disable

Password Login ● Enable ○ Disable

Port 22 (Default: 22)

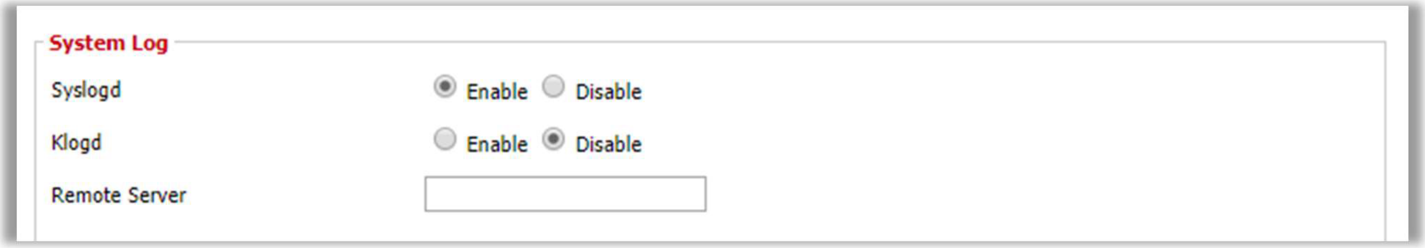
Authorized Keys

Services > Services > Secure Shell

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.

4.1.12 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.



System Log

Syslogd ● Enable ○ Disable

Klogd ○ Enable ● Disable

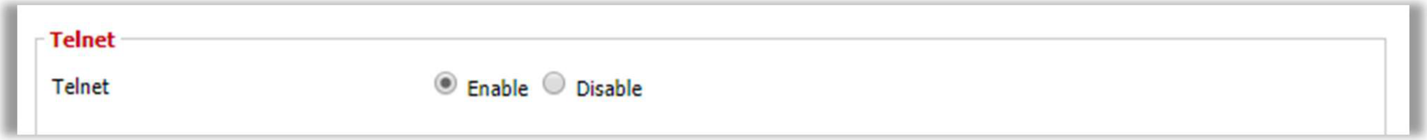
Remote Server

Services > Services > System Log

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

4.1.13 Telnet

Enable or disable Telnet.

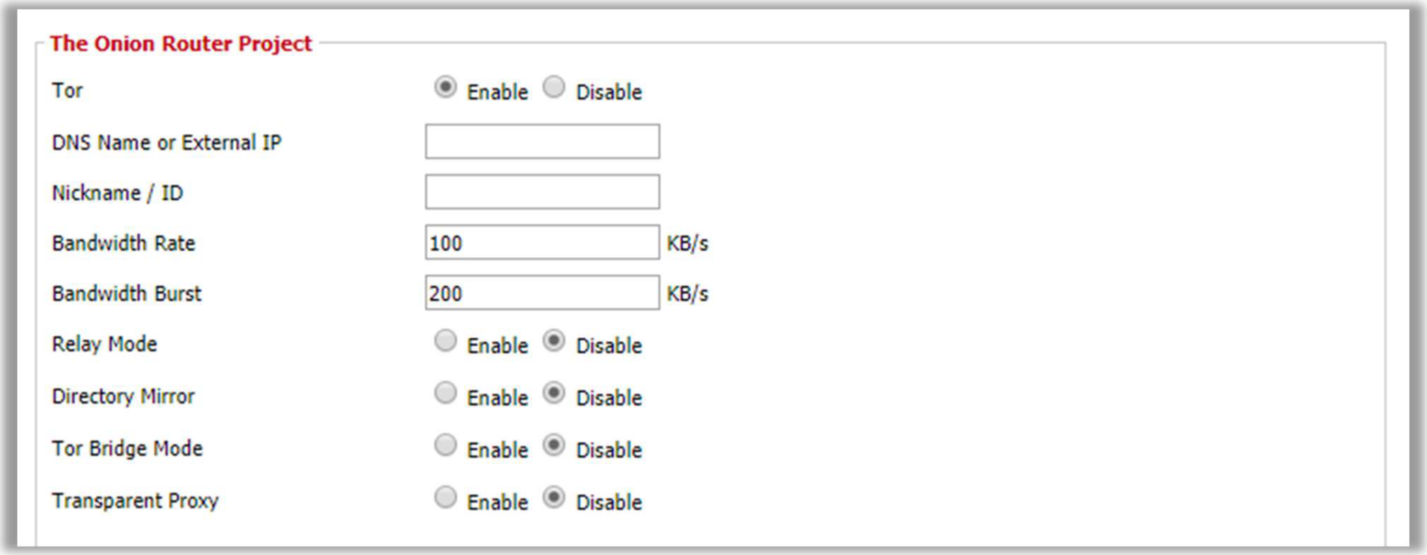


Telnet

Telnet	● Enable ○ Disable

Services > Services > Telnet

4.1.14 The Onion Router Project



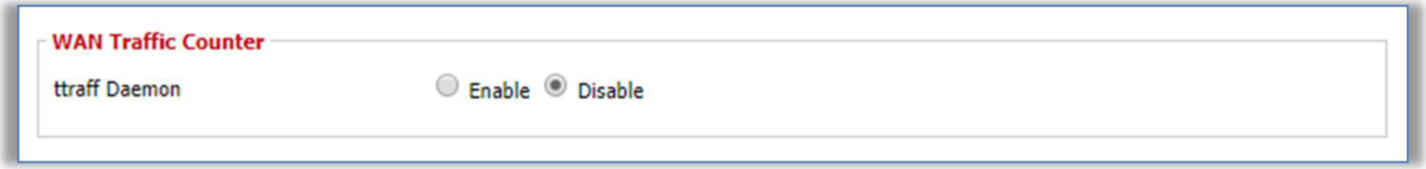
The Onion Router Project

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

Services > Services > The Onion Router Project

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.

4.1.14 WAN Traffic Counter



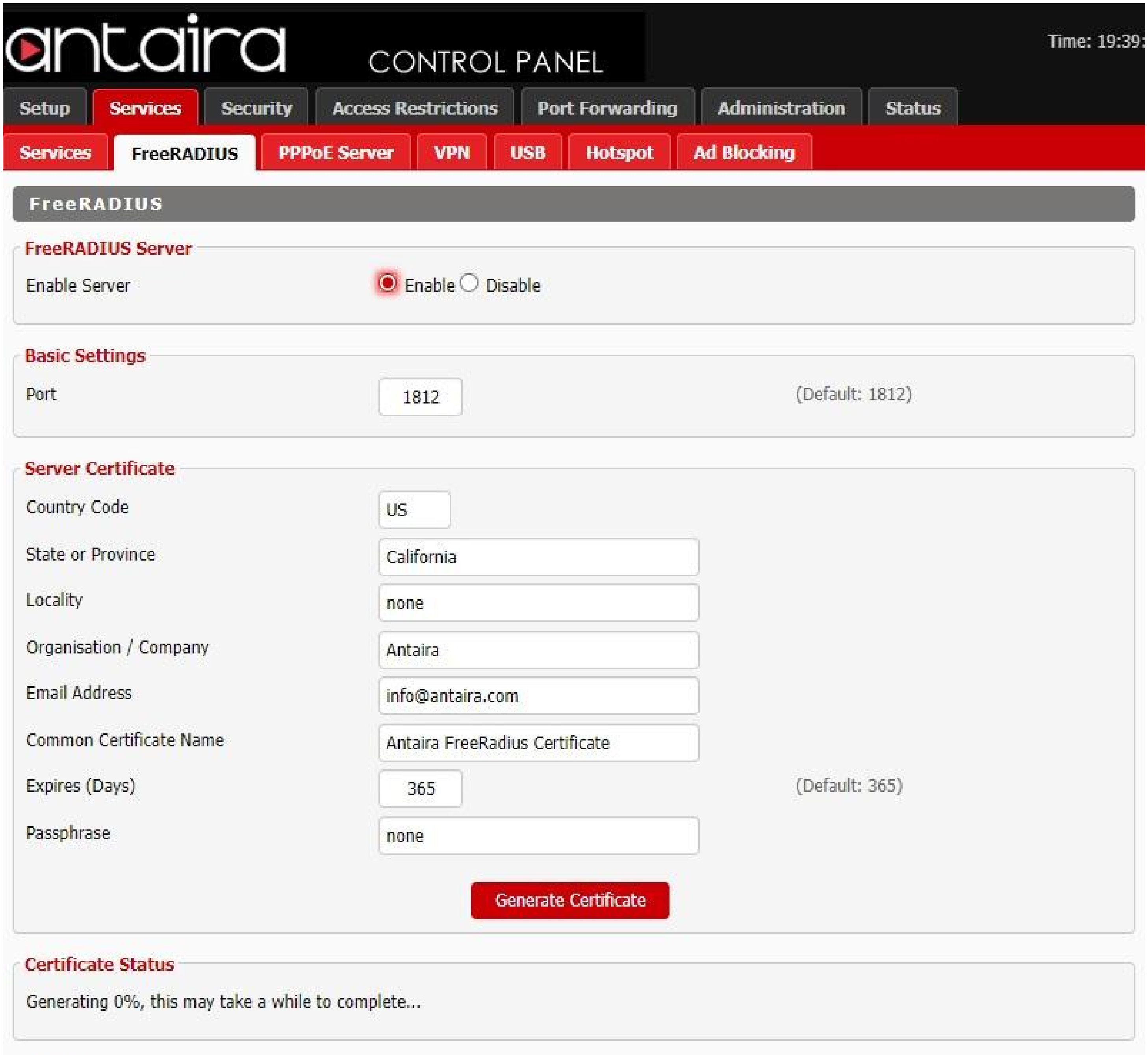
WAN Traffic Counter

ttraff Daemon ○ Enable ● Disable

Services > Services > WAN Traffic Counter

4.2 FreeRadius

FreeRADIUS is a widely deployed RADIUS. FreeRADIUS can be used to authenticate WLAN clients using WPA/WPA2 Enterprise.



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

Certificate Status

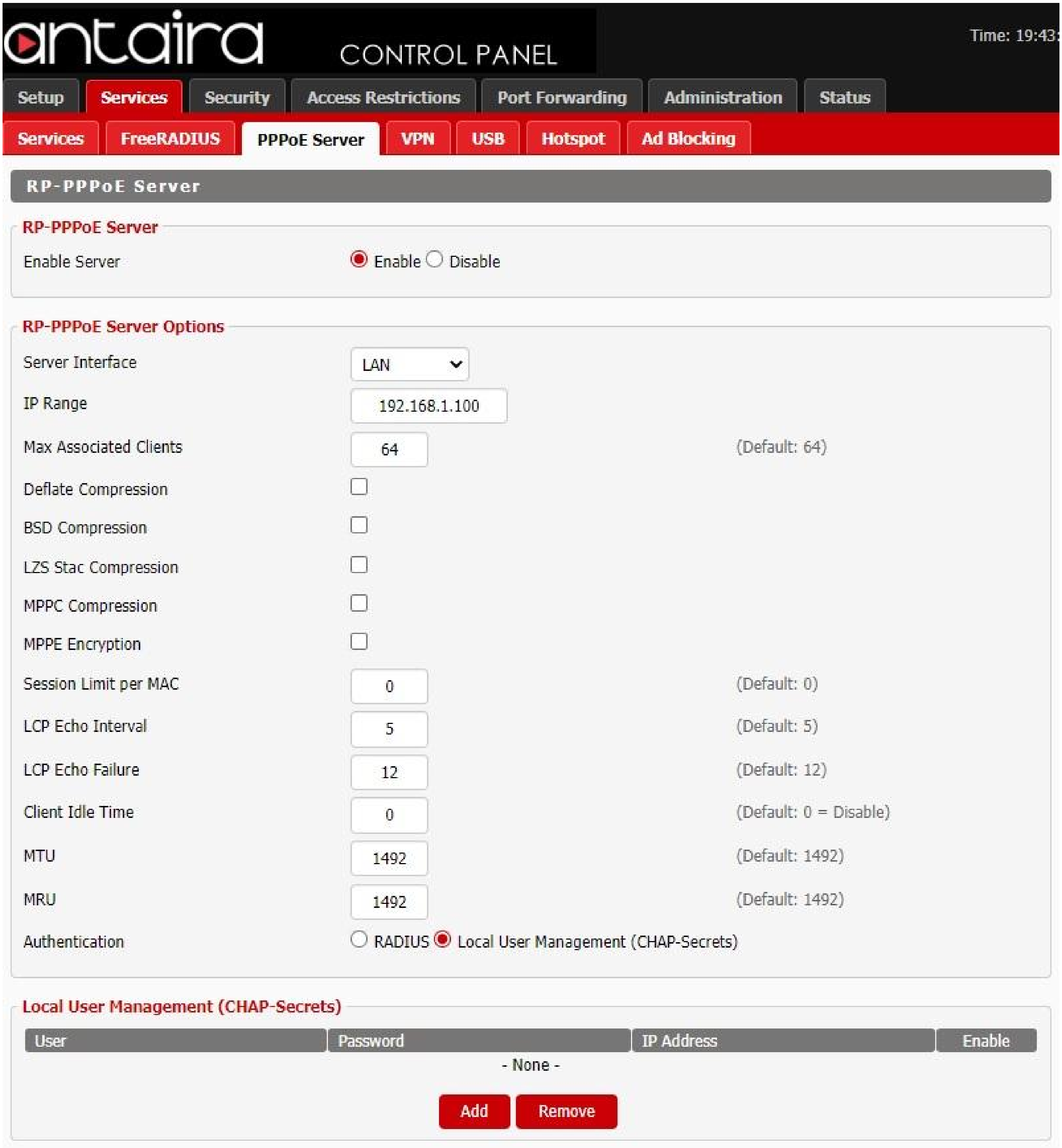
Generating 0%, this may take a while to complete...

Services > FreeRadius

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.



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 -			

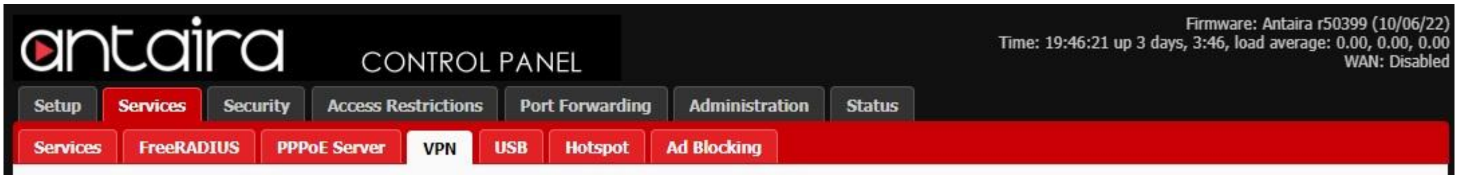
Services > PPPoE Server

PPPoE Server	Description
RP-PPPoE Server Daemon	Enable or disable this feature.

RP-PPPoE Server Interface	Select the interface.
IP Range	Select 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 virtual tunnel connection between each other over the Internet. Typically used to extend a private network across a public network.

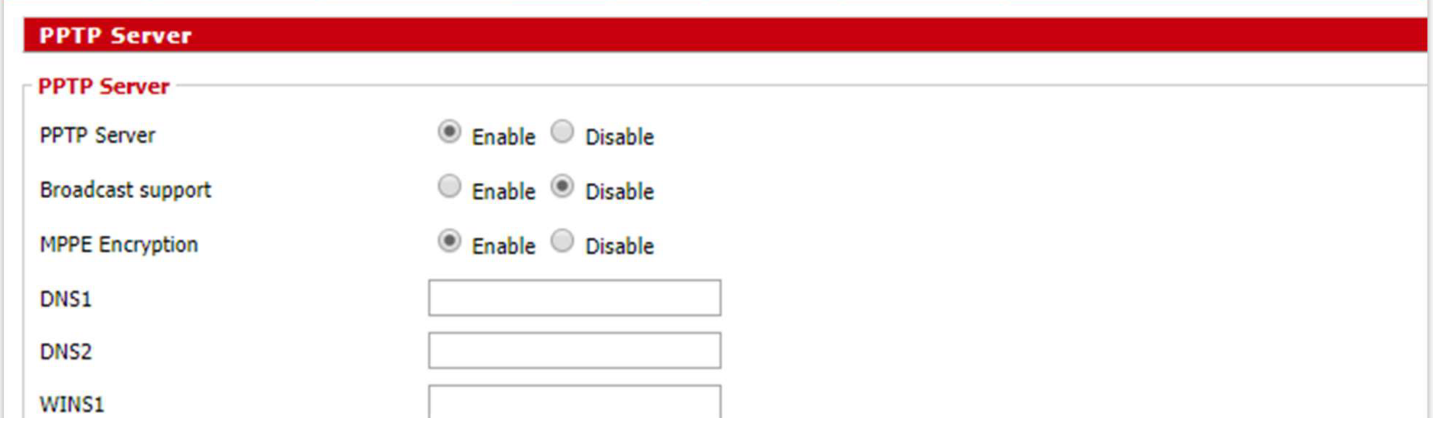


Firmware: Antaira r50399 (10/06/22)
Time: 19:46:21 up 3 days, 3:46, load average: 0.00, 0.00, 0.00
WAN: Disabled

Services > VPN

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).



PPTP Server

PPTP Server

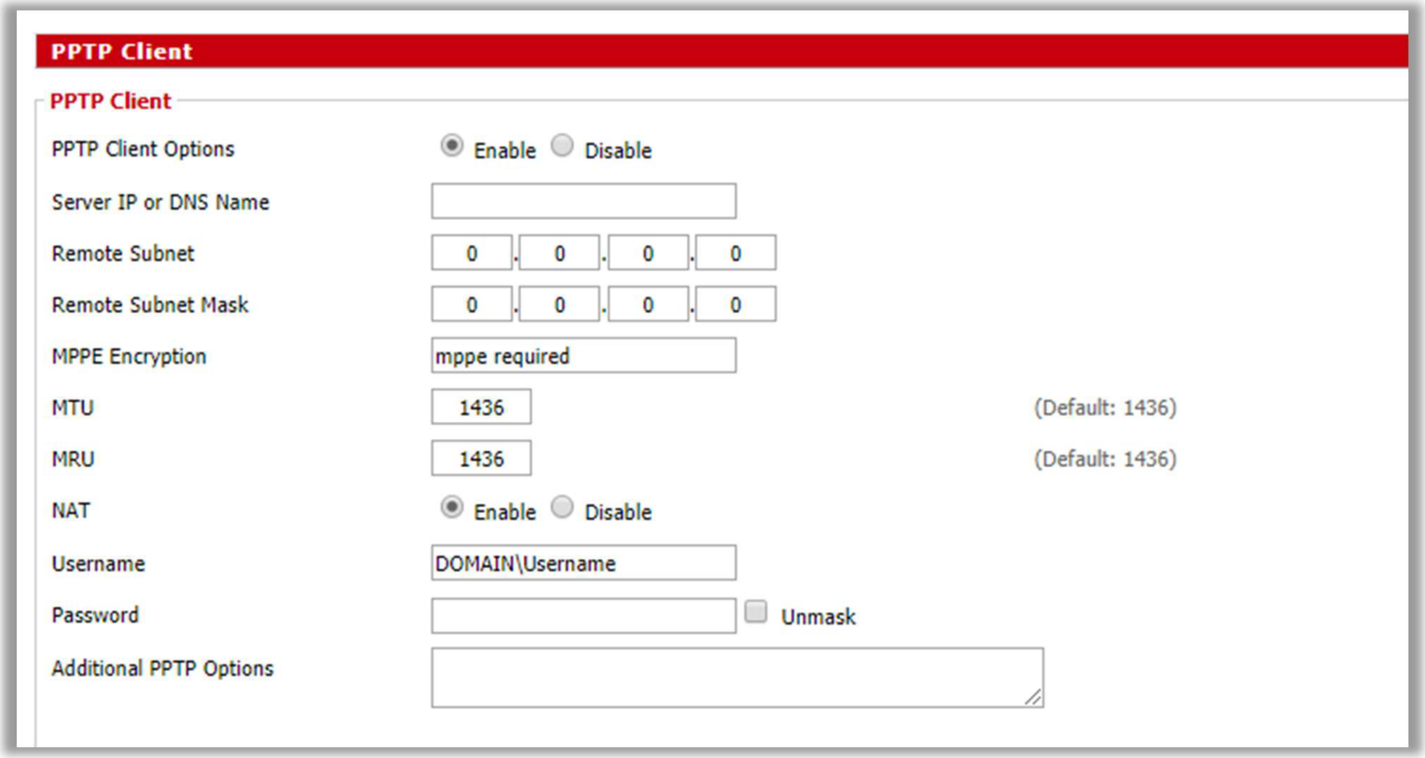
PPTP Server	● Enable ○ Disable
Broadcast support	○ Enable ● Disable
MPPE Encryption	● Enable ○ Disable
DNS1	
DNS2	
WINS1	

Services > VPN > PPTP Server

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.



PPTP Client

PPTP Client

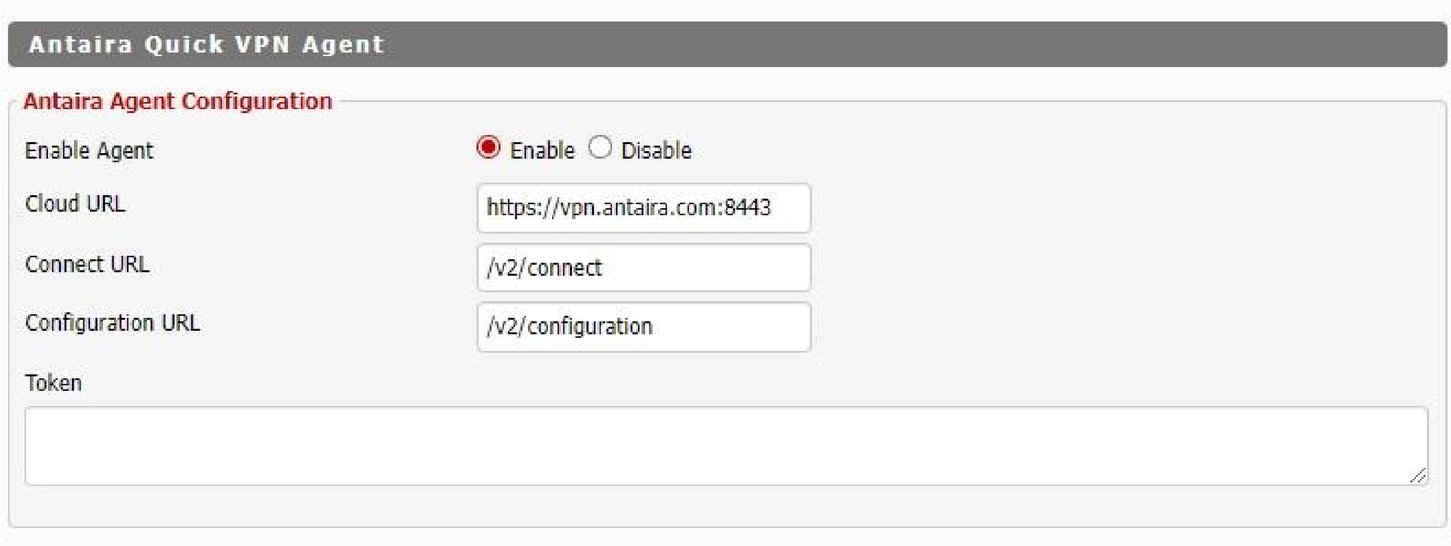
PPTP Client Options	● Enable ○ Disable
Server IP or DNS Name	
Remote Subnet	0 . 0 . 0 . 0
Remote Subnet Mask	0 . 0 . 0 . 0
MPPE Encryption	mppe required
MTU	1436 (Default: 1436)
MRU	1436 (Default: 1436)
NAT	● Enable ○ Disable
Username	DOMAIN\Username
Password	□ Unmask
Additional PPTP Options	

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 Mask	Use the Subnet Mask appropriate for the 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 Agent Configuration



Antaira Quick VPN Agent

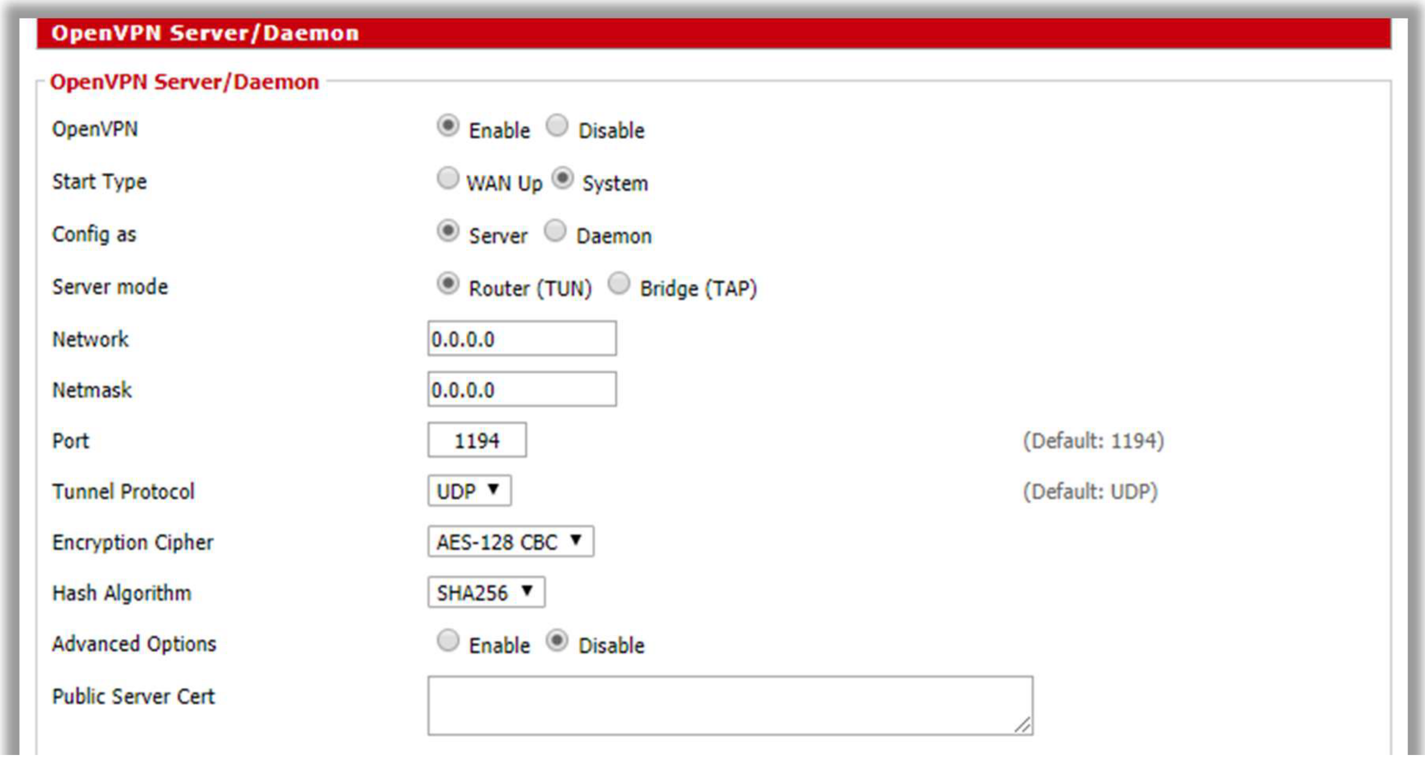
Antaira Agent Configuration

Enable Agent	● Enable ○ Disable
Cloud URL	https://vpn.antaira.com:8443
Connect URL	/v2/connect
Configuration URL	/v2/configuration
Token	

Services > VPN > Antaira Quick VPN Agent

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 set up an OpenVPN Server.



OpenVPN Server/Daemon

OpenVPN Server/Daemon

OpenVPN	● Enable ○ Disable	
Start Type	○ WAN Up ● System	
Config as	● Server ○ Daemon	
Server mode	● Router (TUN) ○ Bridge (TAP)	
Network	0.0.0.0	
Netmask	0.0.0.0	
Port	1194	(Default: 1194)
Tunnel Protocol	UDP ▼	(Default: UDP)
Encryption Cipher	AES-128 CBC ▼	
Hash Algorithm	SHA256 ▼	
Advanced Options	○ Enable ● Disable	
Public Server Cert		

Services > VPN > OpenVPN Server

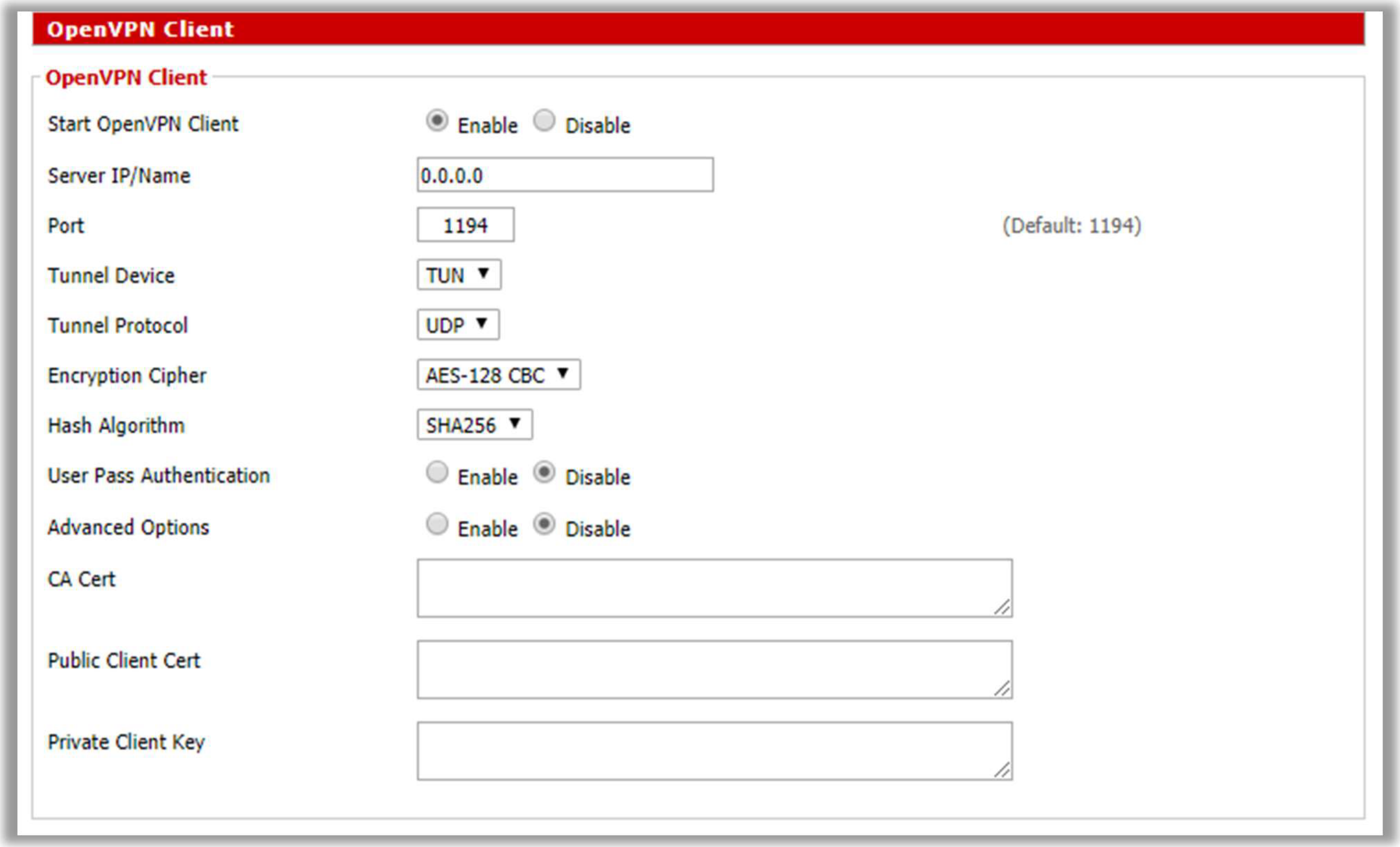
OpenVPN	Description
OpenVPN	Start OpenVPN server/daemon service.
Start Type	Select System for start type.
Config as	Choose to configure via GUI or config file.
Server Mode	The mode of tunneling. **TUN**: Routing (layer 3) **TAP**: Bridging networks (Layer 2, can be used for routing, but not common)
Network	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 the 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 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.
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 set up the router as an OpenVPN Client.



OpenVPN Client

OpenVPN Client

Start OpenVPN Client	● Enable ○ Disable
Server IP/Name	0.0.0.0
Port	1194 (Default: 1194)
Tunnel Device	TUN ▼
Tunnel Protocol	UDP ▼
Encryption Cipher	AES-128 CBC ▼
Hash Algorithm	SHA256 ▼
User Pass Authentication	○ Enable ● Disable
Advanced Options	○ Enable ● Disable
CA Cert	
Public Client Cert	
Private Client Key	

Services > VPN > OpenVPN Client

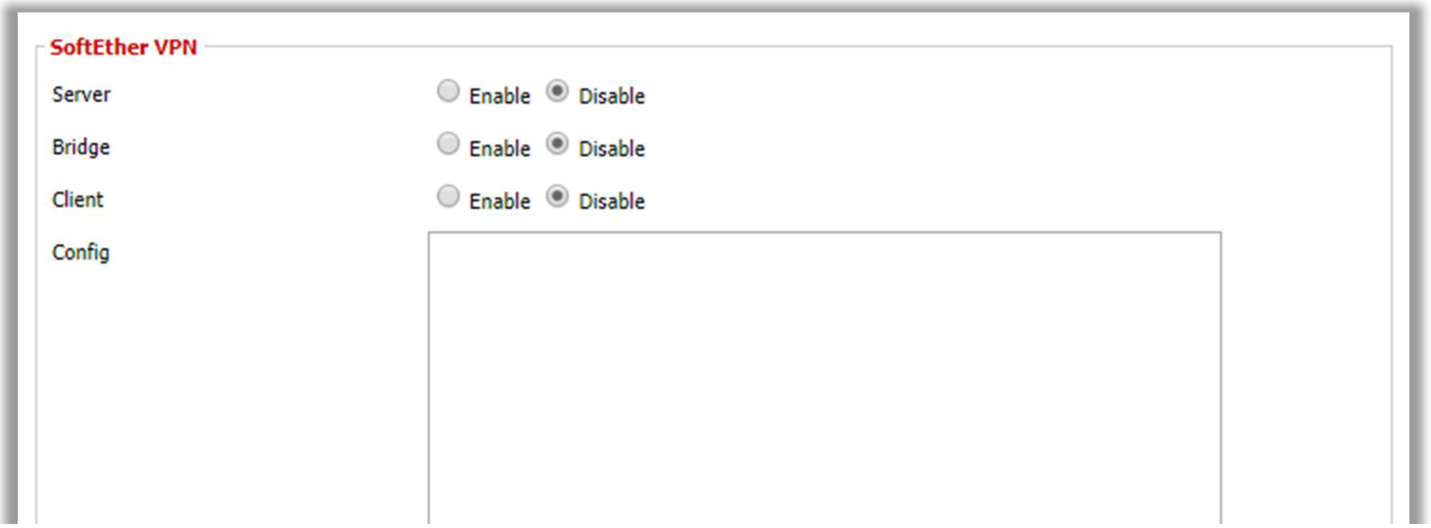
OpenVPN	Description
Start OpenVPN Client	Enable or disable OpenVPN client options.
Server IP/Name	IP address/hostname of the OpenVPN server you wish to connect to.
Port	The port which OpenVPN server is listening on. Default is port 1194.
Tunnel Device	The mode of tunneling. **TUN**: Routing (layer 3). **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.
Subnet 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.

4.4.6 SoftEther VPN

An alternative VPN service to OpenVPN.



SoftEther VPN

Server ○ Enable ● Disable

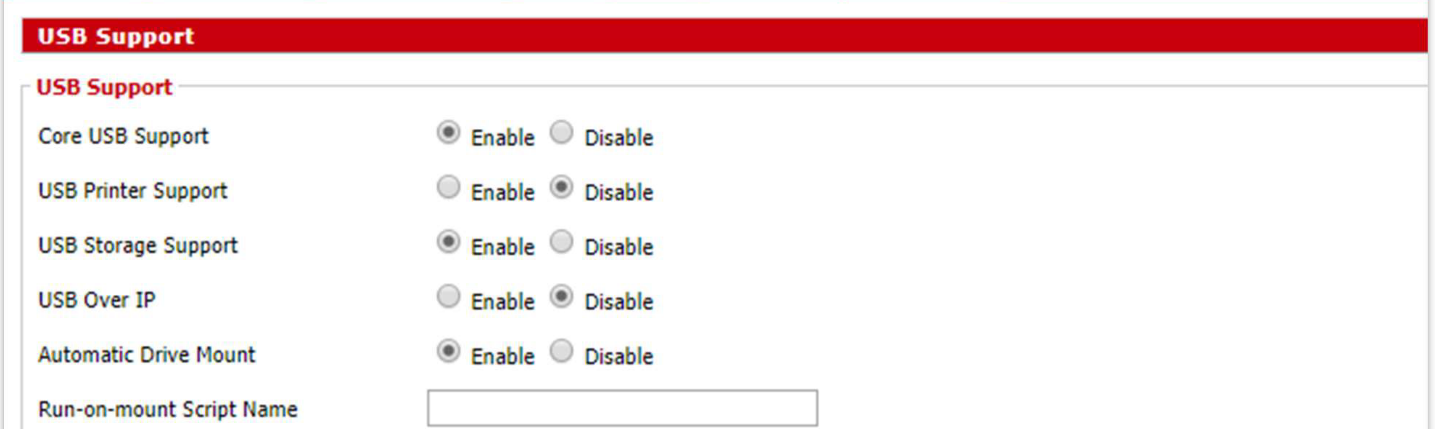
Bridge ○ Enable ● Disable

Client ○ Enable ● Disable

Config

Services > VPN > SoftEther VPN

4.5 USB



USB Support

USB Support

Core USB Support ● Enable ○ Disable

USB Printer Support ○ Enable ● Disable

USB Storage Support ● Enable ○ Disable

USB Over IP ○ Enable ● Disable

Automatic Drive Mount ● Enable ○ Disable

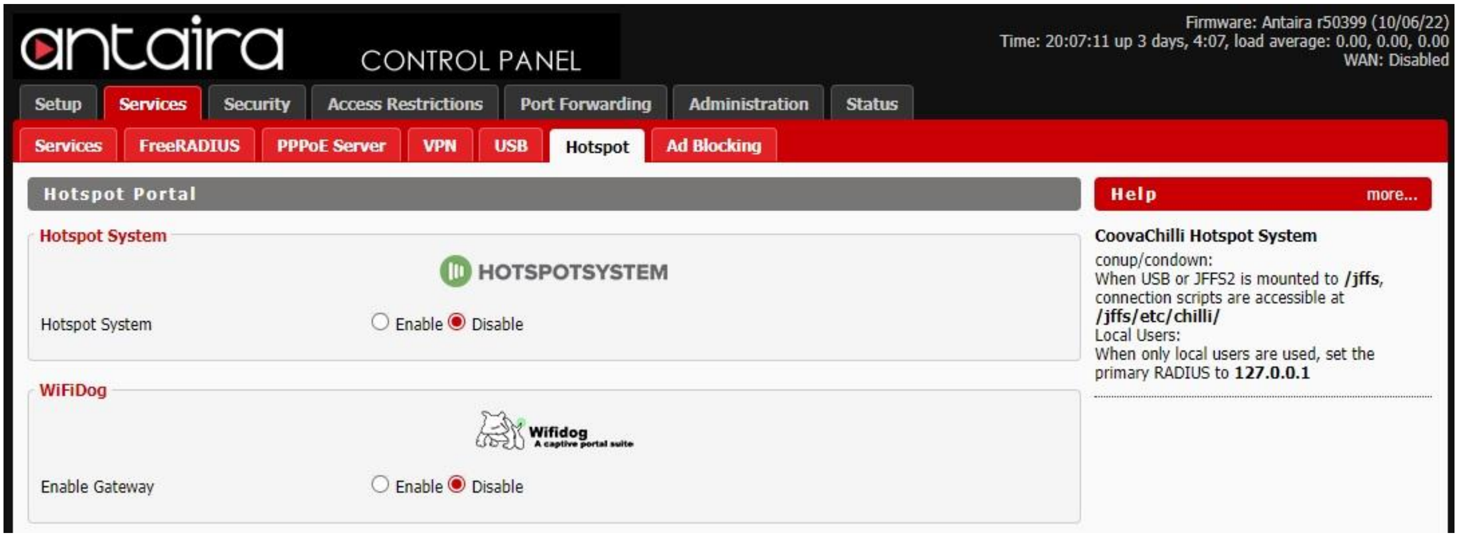
Run-on-mount Script Name

Services > USB

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



Firmware: Antaira r50399 (10/06/22)
Time: 20:07:11 up 3 days, 4:07, load average: 0.00, 0.00, 0.00
WAN: Disabled

Hotspot Portal

Hotspot System

Hotspot System ○ Enable ● Disable

WiFiDog

Enable Gateway ○ Enable ● Disable

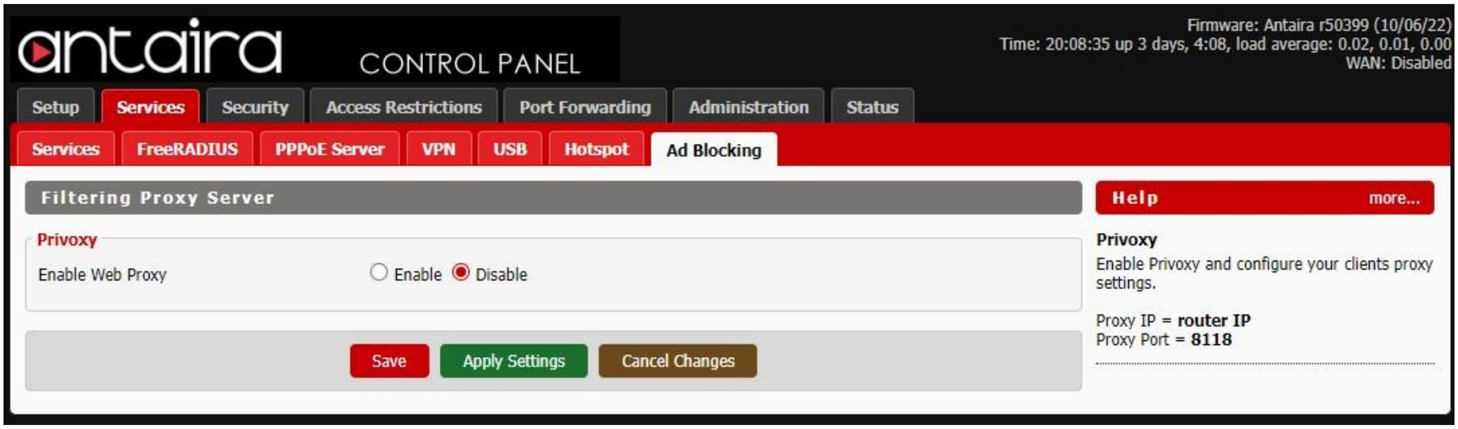
CoovaChilli Hotspot System
conup/condown:
When USB or JFFS2 is mounted to **/jffs**, connection scripts are accessible at **/jffs/etc/chilli/**
Local Users:
When only local users are used, set the primary RADIUS to **127.0.0.1**

Services > 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.

4.7 Adblocking

Privoxy enables you to filter common ads.



Firmware: Antaira r50399 (10/06/22)
Time: 20:08:35 up 3 days, 4:08, load average: 0.02, 0.01, 0.00
WAN: Disabled

Filtering Proxy Server

Privoxy

Enable Web Proxy ○ Enable ● Disable

Privoxy
Enable Privoxy and configure your clients proxy settings.
Proxy IP = **router IP**
Proxy Port = **8118**

Services > Adblocking

Ad Blocking	Description
Privoxy	Enables you to filter common ads.
Provide Proxy Autoconfig	Publishes a WPAD/PAC file that clients use to automatically set up

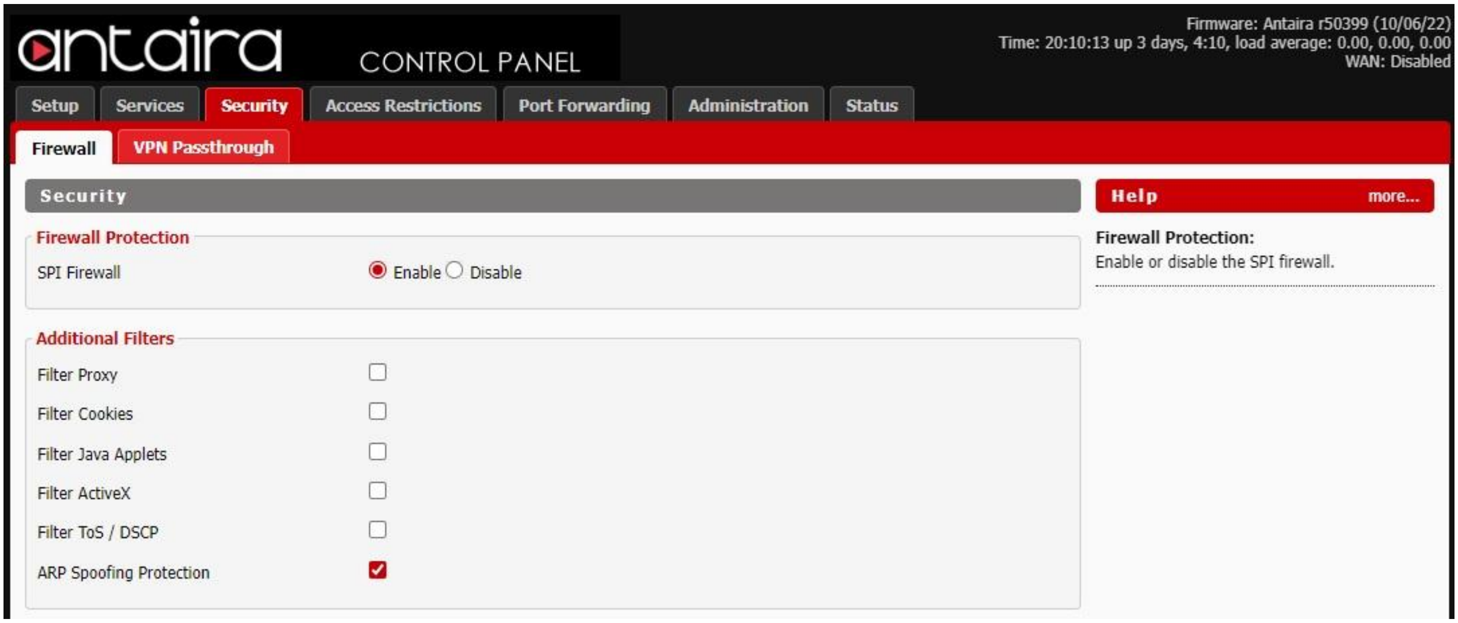
	proxy details.
Transparent Mode	Traffic to port 80 is intercepted by Privoxy even if the client did not configure any proxy settings, thus allowing you to enforce filtering. Transparent mode cannot intercept HTTPS connections. All HTTPS traffic will not be filtered by Privoxy unless added to the autoconfig.
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.



Firewall Protection

SPI Firewall ● Enable ○ Disable

Additional Filters

Filter Proxy □

Filter Cookies □

Filter Java Applets □

Filter ActiveX □

Filter ToS / DSCP □

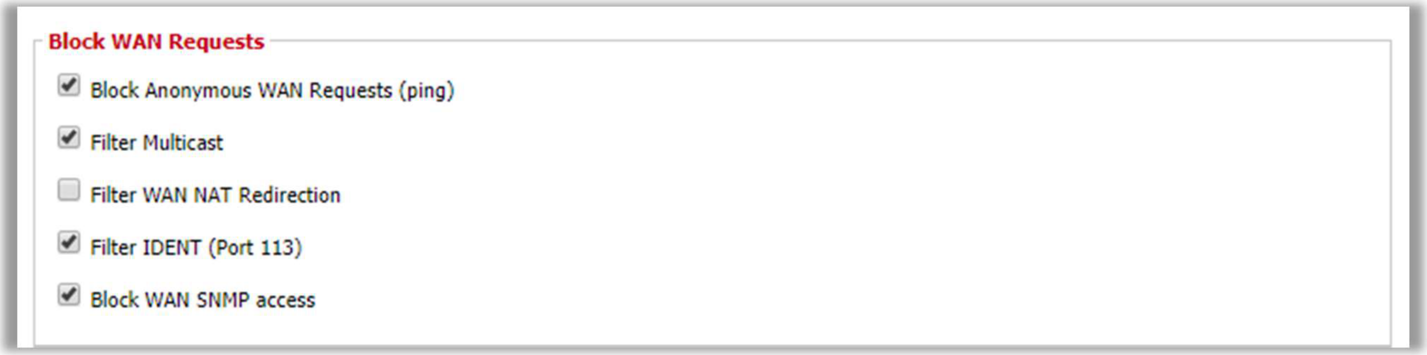
ARP Spoofing Protection ☑

Firewall Protection:
Enable or disable the SPI firewall.

Security > Firewall > Security

Security	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.

5.1.2 Block WAN Request



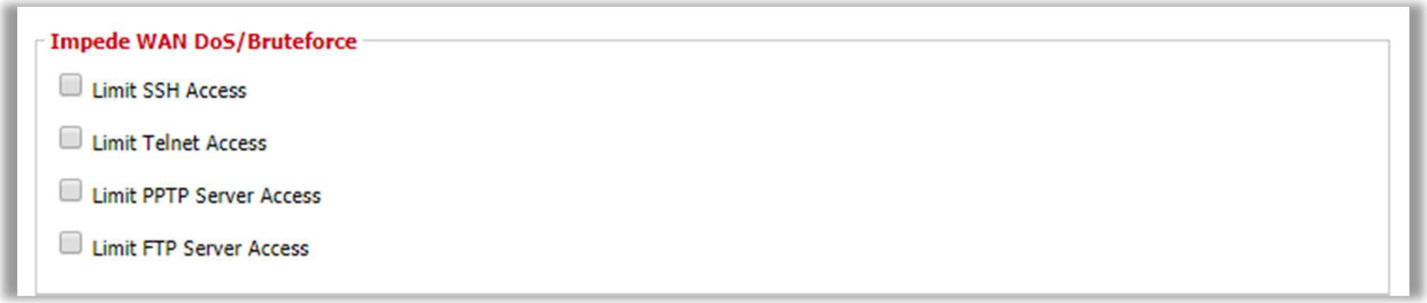
Block WAN Requests

- ☑ Block Anonymous WAN Requests (ping)
- ☑ Filter Multicast
- ☐ Filter WAN NAT Redirection
- ☑ Filter IDENT (Port 113)
- ☑ Block WAN SNMP access

Security > Firewall > Block WAN Request

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

5.1.3 Impede WAN DoS/Bruteforce



Impede WAN DoS/Bruteforce

- ☐ Limit SSH Access
- ☐ Limit Telnet Access
- ☐ Limit PPTP Server Access
- ☐ Limit FTP Server Access

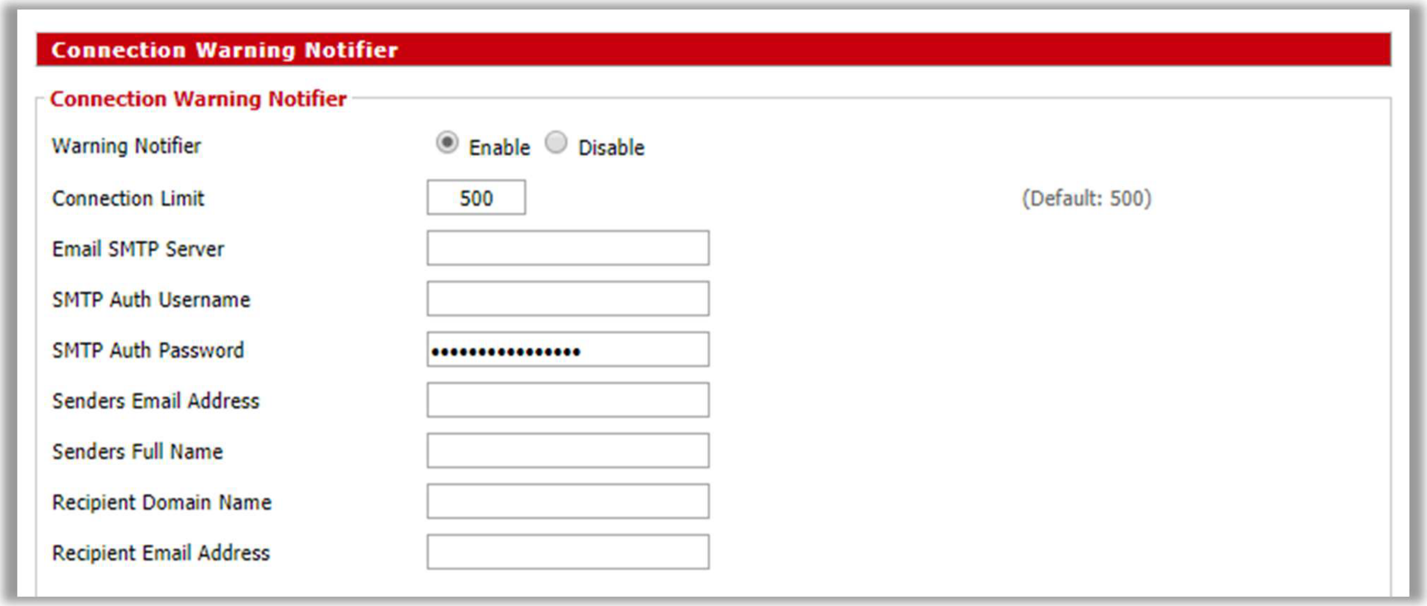
Security > Firewall > Impede WAN DoS/Bruteforce

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.

5.1.4 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

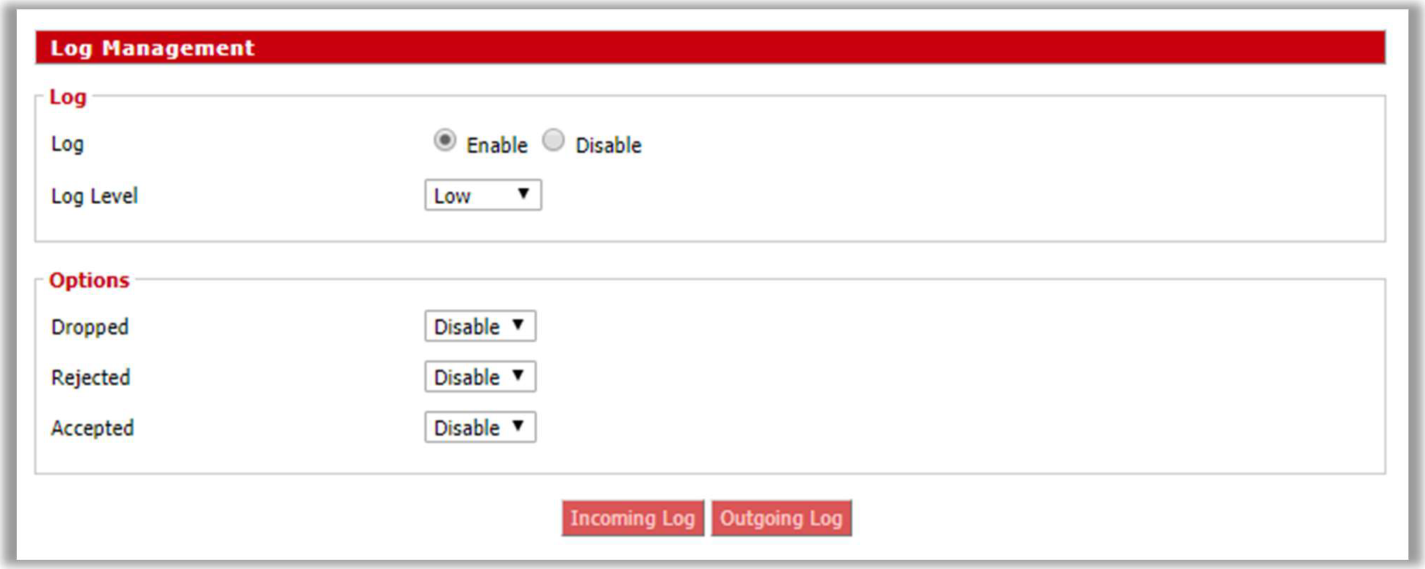
Warning Notifier	● Enable ○ Disable	
Connection Limit	500	(Default: 500)
Email SMTP Server		
SMTP Auth Username		
SMTP Auth Password	••••••••••••••••	
Senders Email Address		
Senders Full Name		
Recipient Domain Name		
Recipient Email Address		

Security > Firewall > Connection Warning Notifier

Connection Warning Notifier	Description
Warning Notifier	Enable or disable the Warning Notifier feature.
Connection Limit	The 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.

5.1.5 Log Management

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



Log Management

Log

Log ● Enable ○ Disable

Log Level: Low

Options

Dropped: Disable

Rejected: Disable

Accepted: Disable

Security > Firewall > Log Management

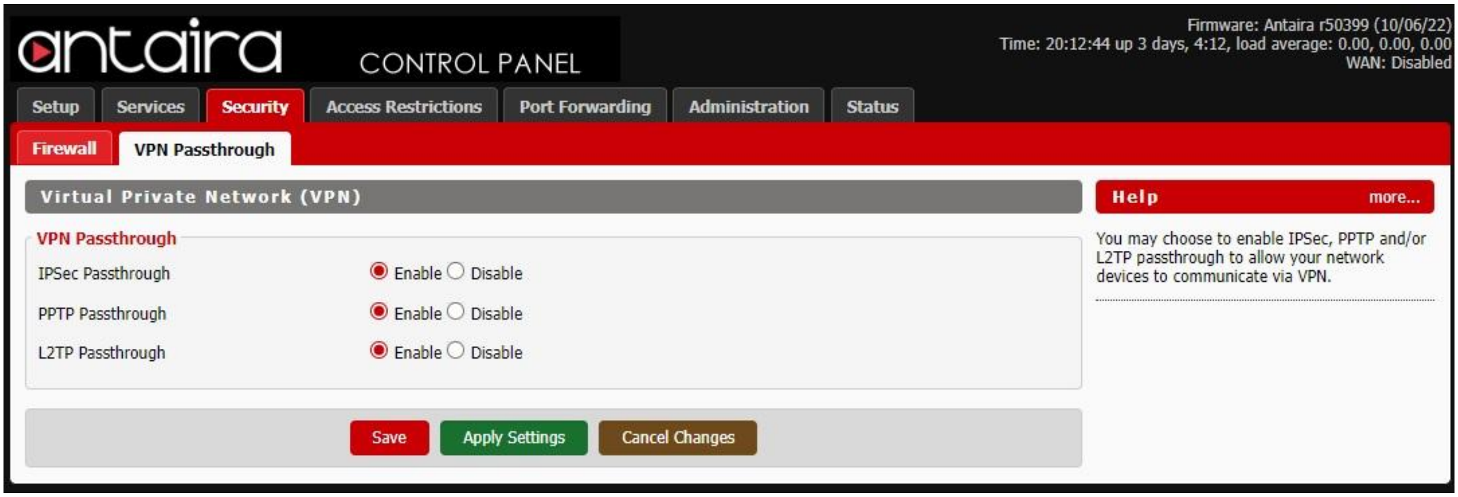
Log Management	Description
Log	To keep activity logs, select **Enable**.
Log Level	Set this to the required amount of information. Set Log Level higher to log more actions.
Dropped	Log Dropped items.
Rejected	Log Rejected items.
Accepted	Log Accepted items.

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.



Virtual Private Network (VPN)

VPN Passthrough

IPSec Passthrough ● Enable ○ Disable

PPTP Passthrough ● Enable ○ Disable

L2TP Passthrough ● Enable ○ Disable

You may choose to enable IPSec, PPTP and/or L2TP passthrough to allow your network devices to communicate via VPN.

Security > Firewall > VPN Passthrough

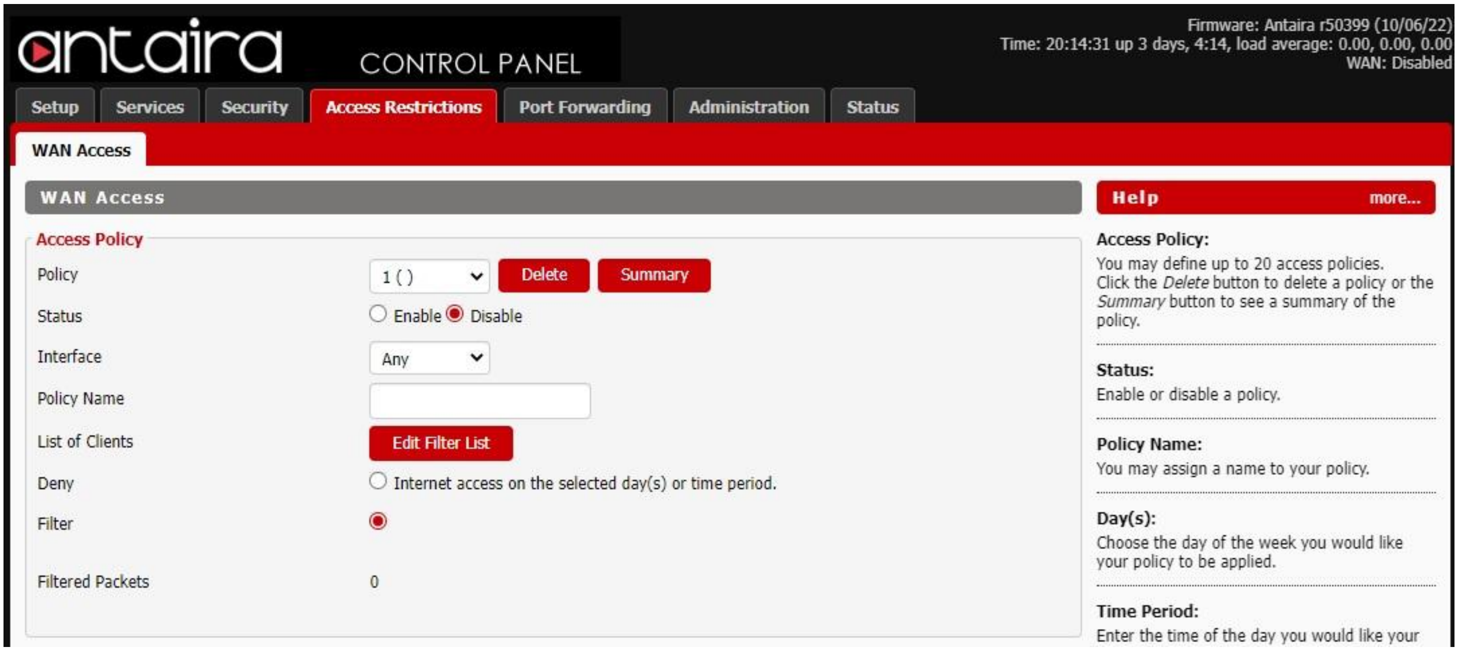
VPN Passthrough	Description
IPSec Passthrough	Allow IPSec.
PPTP Passthrough	Allow PPTP.
L2TP Passthrough	Allow P2TP.

6 Access Restrictions

6.1 WAN Access

6.1.1 Access Policy

Access Policy allows you to restrict access on the basis of time, protocol, or destination. You can create up to 10 sets of rules with each set of rules being referred to as a policy. A policy can contain multiple individual rules, such as filtering a specific machine access to a particular web site, and/or filtering access to certain unwanted P2P protocols. Does not work with Client Bridge Mode.



Firmware: Antaira r50399 (10/06/22)
Time: 20:14:31 up 3 days, 4:14, load average: 0.00, 0.00, 0.00
WAN: Disabled

Access Policy

Policy	1 ( )
Status	○ Enable ● Disable
Interface	Any
Policy Name	
List of Clients	Edit Filter List
Deny	○ Internet access on the selected day(s) or time period.
Filter	●
Filtered Packets	0

Access Policy:
You may define up to 20 access policies. Click the *Delete* button to delete a policy or the *Summary* button to see a summary of the policy.

Status:
Enable or disable a policy.

Policy Name:
You may assign a name to your policy.

Day(s):
Choose the day of the week you would like your policy to be applied.

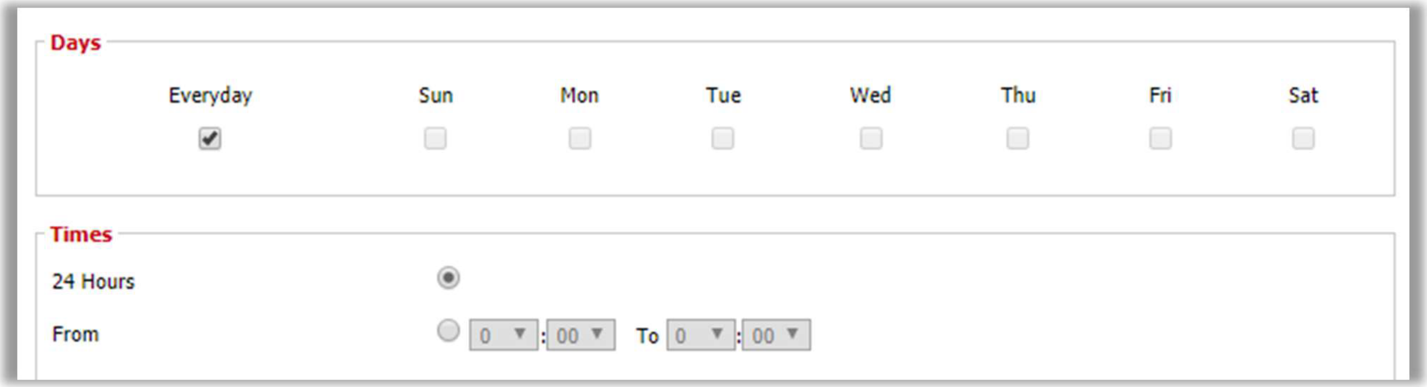
Time Period:
Enter the time of the day you would like your

Access Restriction > WAN Access > Access Policy

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**.

6.1.2 Days and Times

Set the days and time when Internet access will be denied.



Days

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

Times

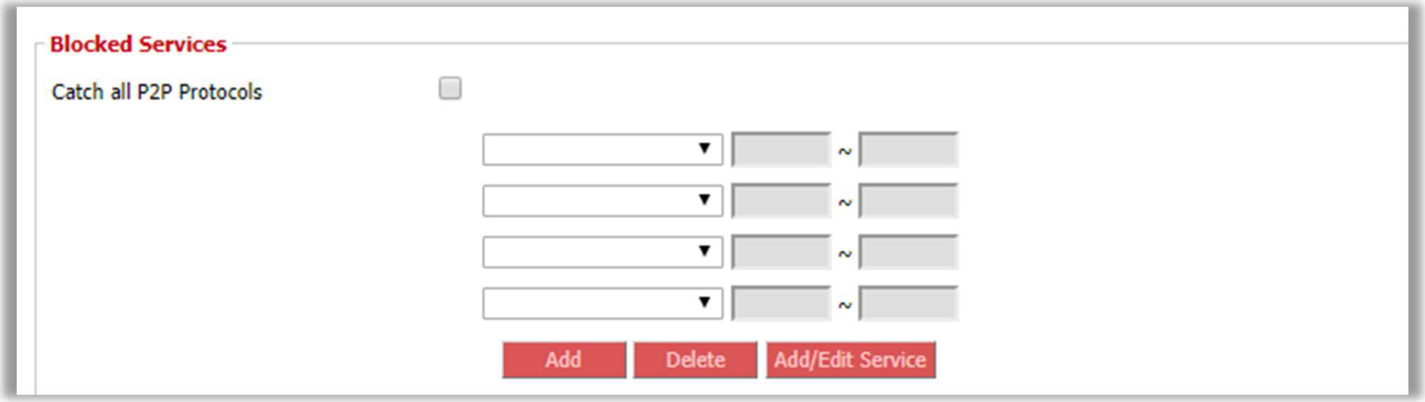
24 Hours ●

From ○ 0 : 00 To 0 : 00

Access Restriction > WAN Access > Days and Times

6.1.3 Blocked Services

Enter the services you wish to block (if any).



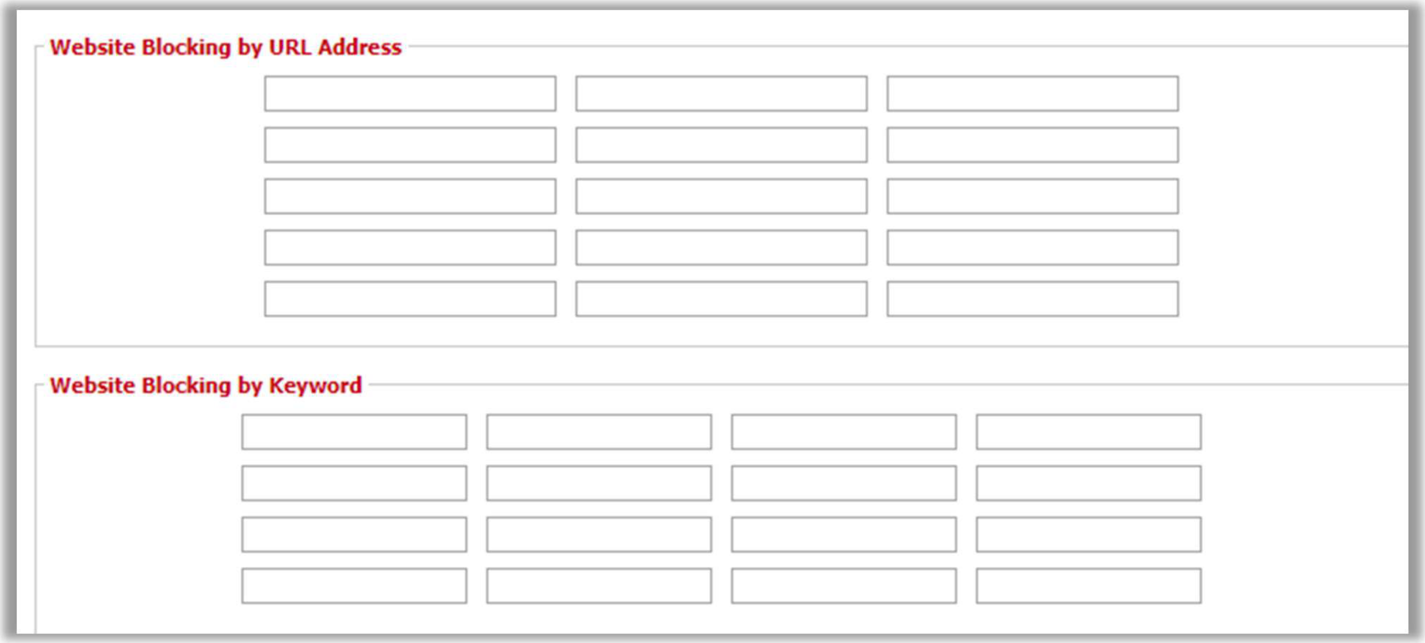
Blocked Services

Catch all P2P Protocols □

Access Restriction > WAN Access > Blocked Services

6.1.4 Website Blocking

Block specific websites by URL or keyword.

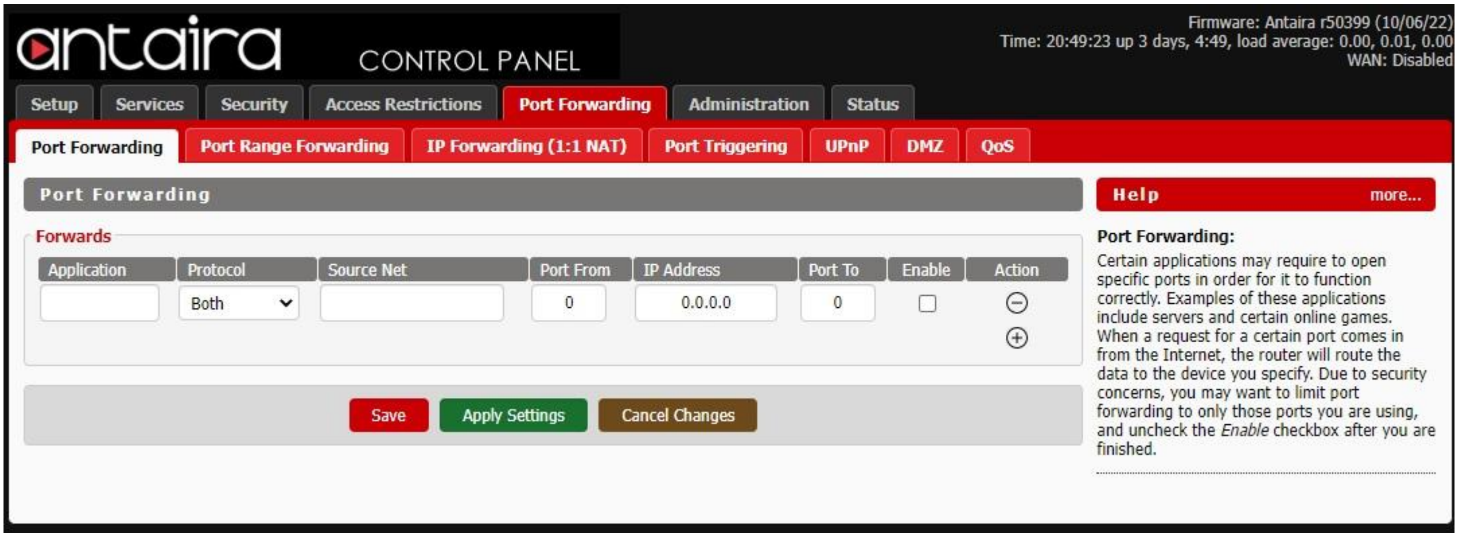


Access Restriction > WAN Access > Website Blocking

7 NAT/QoS

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.



Firmware: Antaira r50399 (10/06/22)
Time: 20:49:23 up 3 days, 4:49, load average: 0.00, 0.01, 0.00
WAN: Disabled

Port Forwarding

Forwards

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

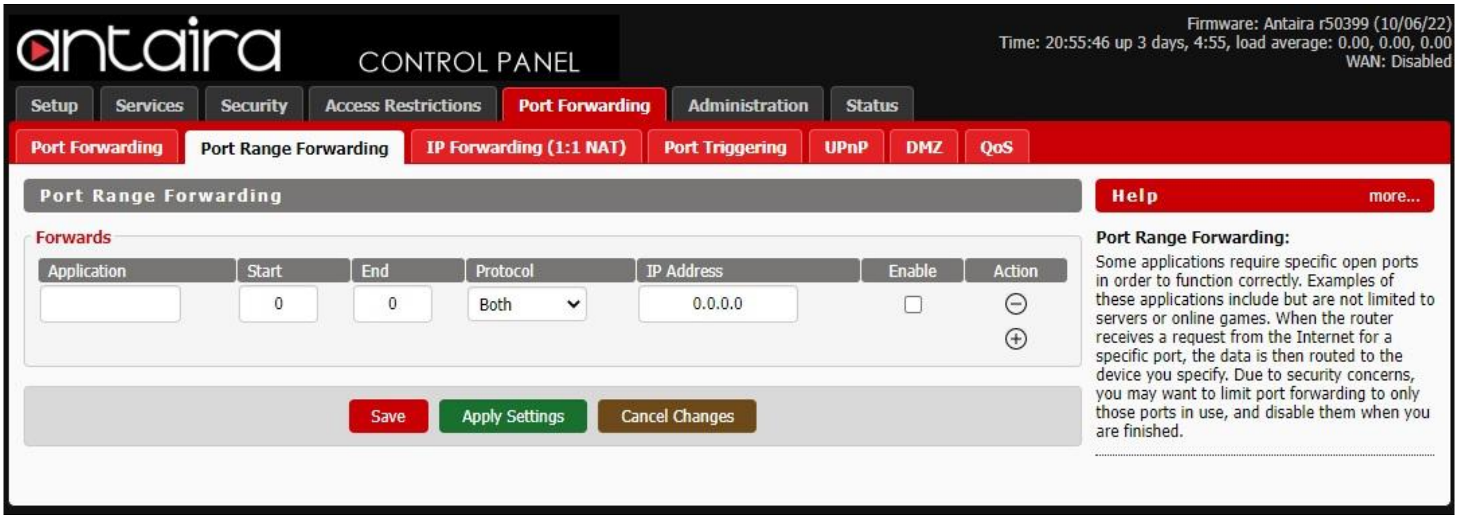
Port Forwarding:
Certain applications may require to open specific ports in order for it to function correctly. Examples of these applications include servers and certain online games. When a request for a certain port comes in from the Internet, the router will route the data to the device you specify. 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.

Port Forwarding > Port Forwarding

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 the 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.



Firmware: Antaira r50399 (10/06/22)
Time: 20:55:46 up 3 days, 4:55, load average: 0.00, 0.00, 0.00
WAN: Disabled

Port Range Forwarding

Forwards

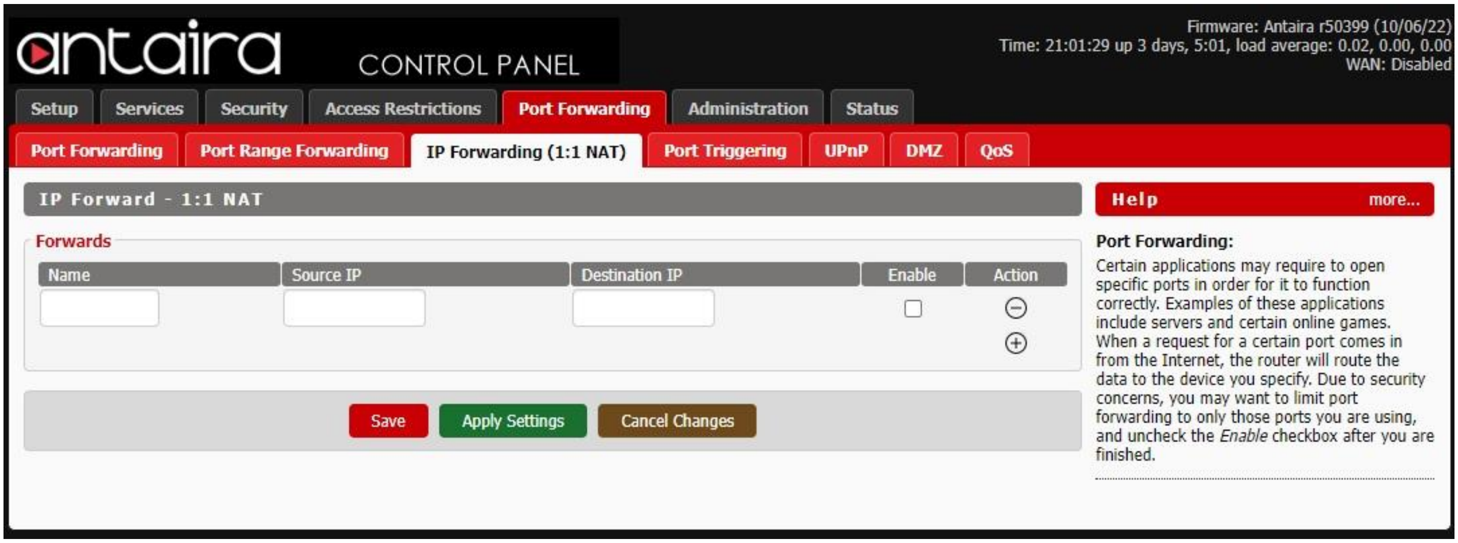
Application	Start	End	Protocol	IP Address	Enable	Action
	0	0	Both	0.0.0.0	□	⊖ ⊕

Port Range Forwarding:
Some applications require specific open ports in order to function correctly. Examples of these applications include but are not limited to servers or online games. When the router receives a request from the Internet for a specific port, the data is then routed to the device you specify. Due to security concerns, you may want to limit port forwarding to only those ports in use, and disable them when you are finished.

Port Forwarding > Port Range Forwarding

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)



Firmware: Antaira r50399 (10/06/22)
Time: 21:01:29 up 3 days, 5:01, load average: 0.02, 0.00, 0.00
WAN: Disabled

IP Forward - 1:1 NAT

Forwards

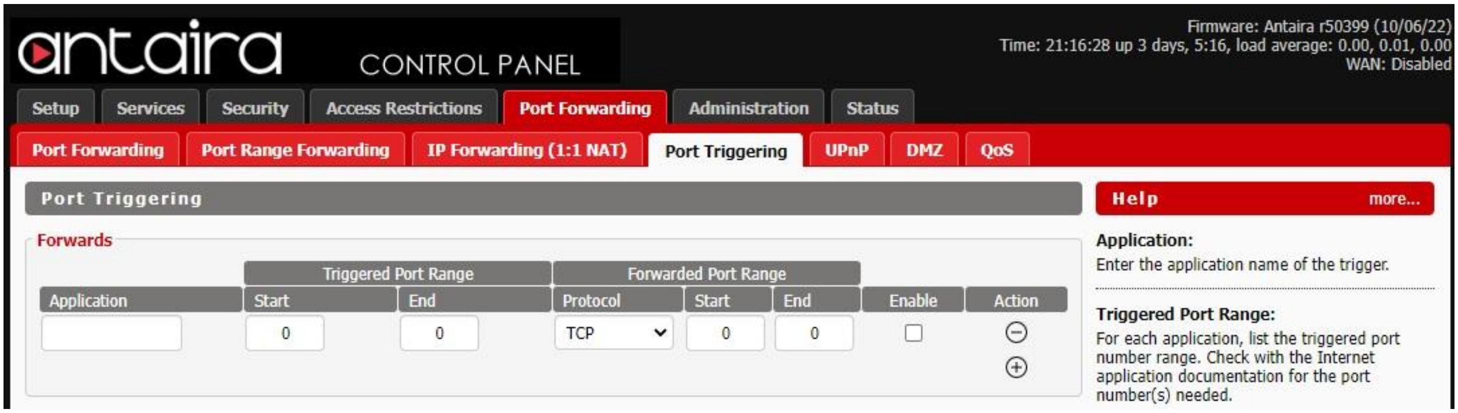
Name	Source IP	Destination IP	Enable	Action
			□	⊖ ⊕

Port Forwards:
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.

Port Forwarding > IP Forwarding (1:1 NAT)

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 specified outgoing port for specific traffic.



Firmware: Antaira r50399 (10/06/22)
Time: 21:16:28 up 3 days, 5:16, load average: 0.00, 0.01, 0.00
WAN: Disabled

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

Application:
Enter the application name of the trigger.

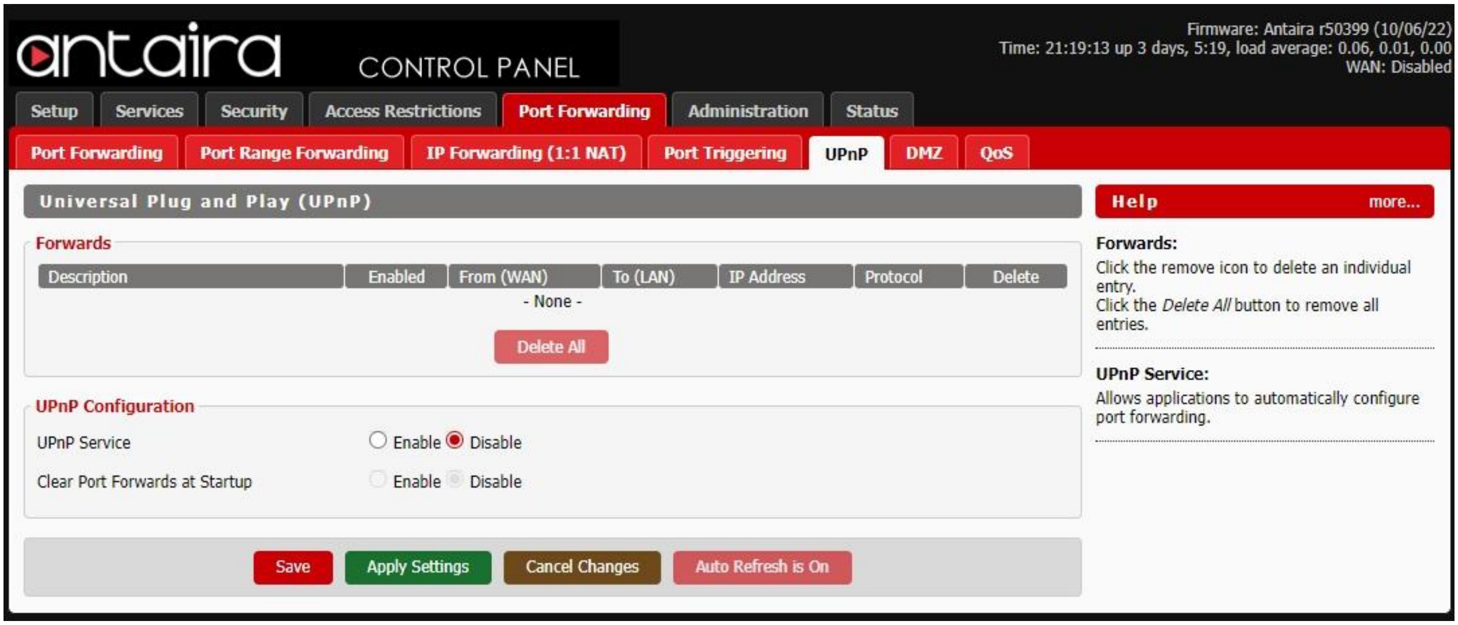
Triggered Port Range:
For each application, list the triggered port number range. Check with the Internet application documentation for the port number(s) needed.

Port Forwarding > Port Triggering

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.



Firmware: Antaira r50399 (10/06/22)
Time: 21:19:13 up 3 days, 5:19, load average: 0.06, 0.01, 0.00
WAN: Disabled

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

Forwards:
Click the remove icon to delete an individual entry.
Click the *Delete All* button to remove all entries.

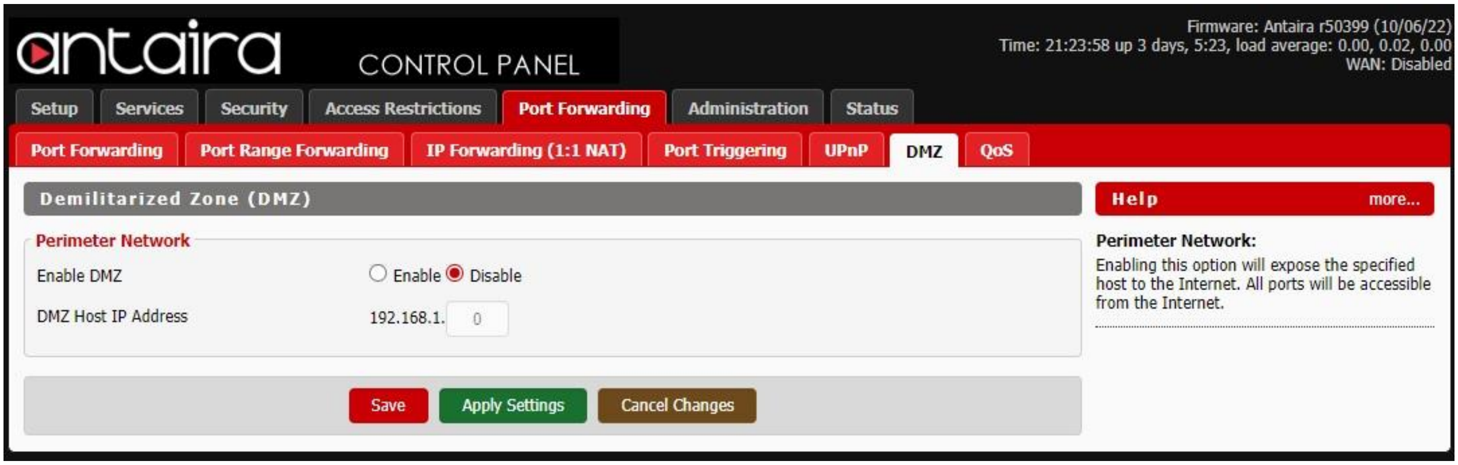
UPnP Service:
Allows applications to automatically configure port forwarding.

Port Forwarding > UPnP

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.



Firmware: Antaira r50399 (10/06/22)
Time: 21:23:58 up 3 days, 5:23, load average: 0.00, 0.02, 0.00
WAN: Disabled

Demilitarized Zone (DMZ)

Perimeter Network

Enable DMZ ○ Enable ● Disable

DMZ Host IP Address 192.168.1. 0

Perimeter Network:
Enabling this option will expose the specified host to the Internet. All ports will be accessible from the Internet.

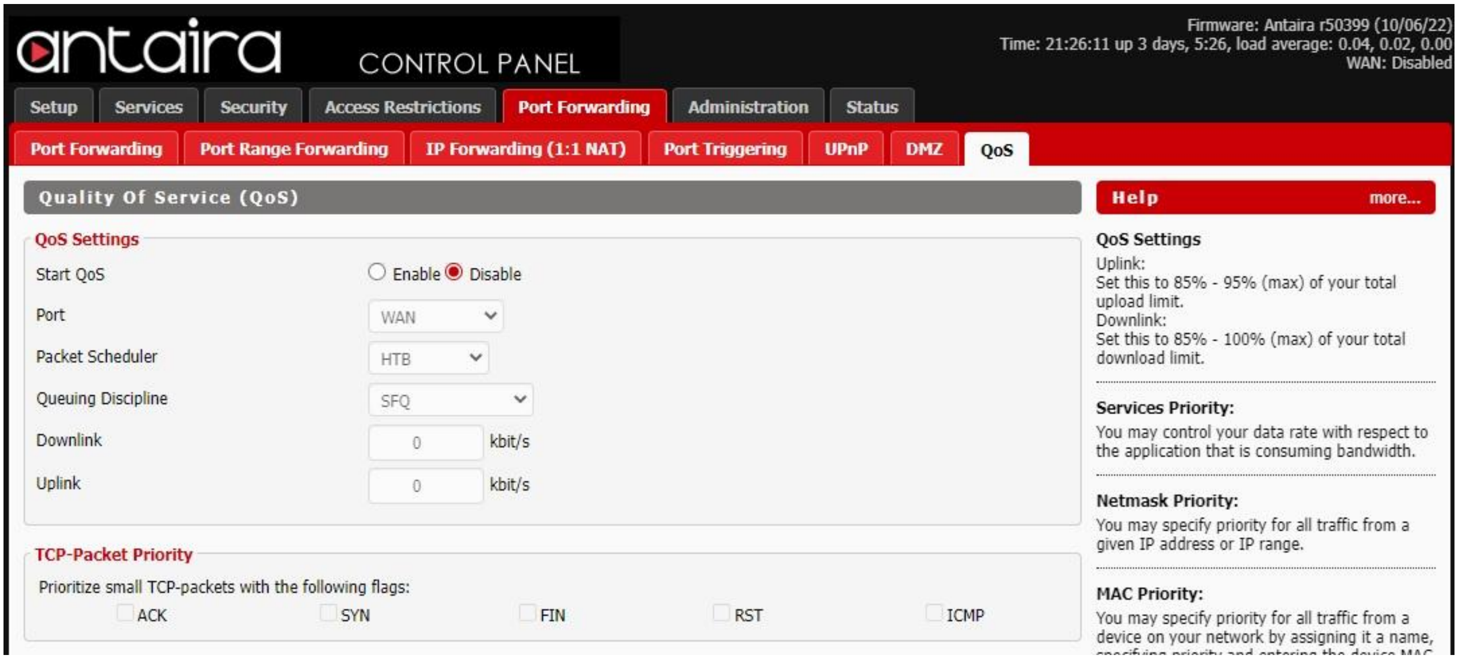
Port Forwarding > DMZ

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 transfer, P2P) gets low priority. The main goal is to allow both types to live side-by-side without unimportant traffic disturbing more critical 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.



Firmware: Antaira r50399 (10/06/22)
Time: 21:26:11 up 3 days, 5:26, load average: 0.04, 0.02, 0.00
WAN: Disabled

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

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

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

Netmask Priority:
You may specify priority for all traffic from a given IP address or IP range.

MAC Priority:
You may specify priority for all traffic from a device on your network by assigning it a name,

Port Forwarding > QoS > QoS Settings

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.

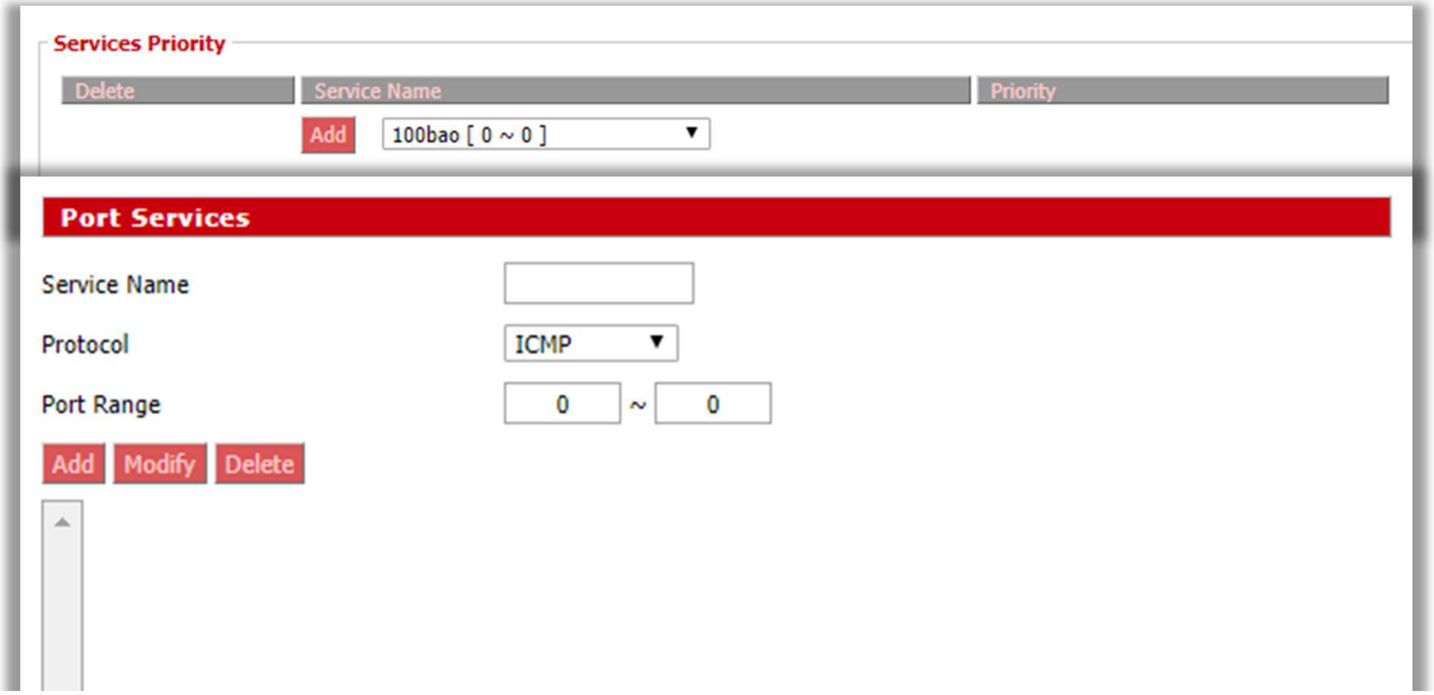
	Priority controls the how long time packets take to get sent out, while bandwidth effects throughput. HTB is a little more resource demanding than HFSC. **HTB**: Hierarchical Token Bucket. HTB helps in controlling the use of the outbound bandwidth on a given link. HTB allows you to use one physical link 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.

7.7.2 Services Priority

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



Services Priority

Delete	Service Name	Priority
	Add 100bao [0 ~ 0] ▼	

Port Services

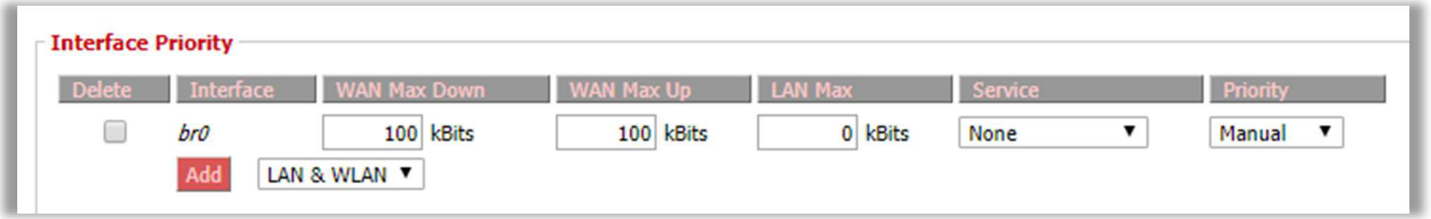
Service Name	
Protocol	ICMP ▼
Port Range	0 ~ 0

Port Forwarding > QoS > Services Priority

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.



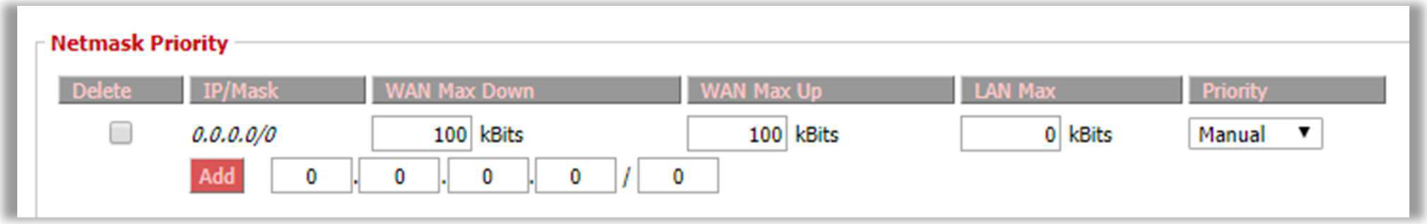
Interface Priority

Delete	Interface	WAN Max Down	WAN Max Up	LAN Max	Service	Priority
□	*br0*	100 kBits	100 kBits	0 kBits	None ▼	Manual ▼
	Add LAN & WLAN ▼					

Port Forwarding > QoS > Interface Priority

7.7.4 Netmask Priority

You may specify priority for all traffic from a given IP address or IP range.



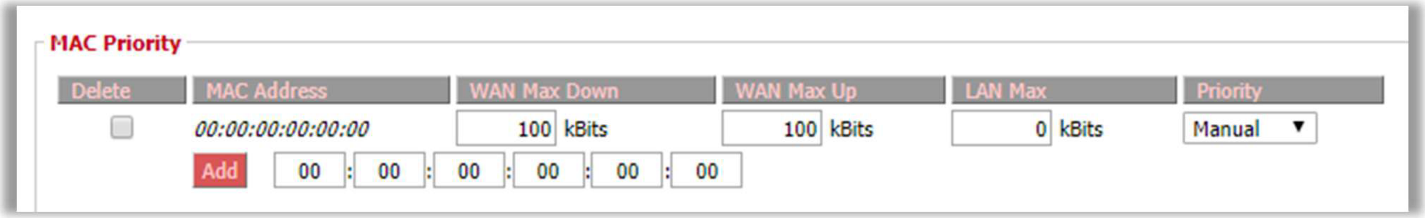
Netmask Priority

Delete	IP/Mask	WAN Max Down	WAN Max Up	LAN Max	Priority
□	0.0.0.0/0	100 kBits	100 kBits	0 kBits	Manual ▼
Add	0 . 0 . 0 . 0 / 0				

Port Forwarding > QoS > Netmask Priority

7.7.5 MAC Priority

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



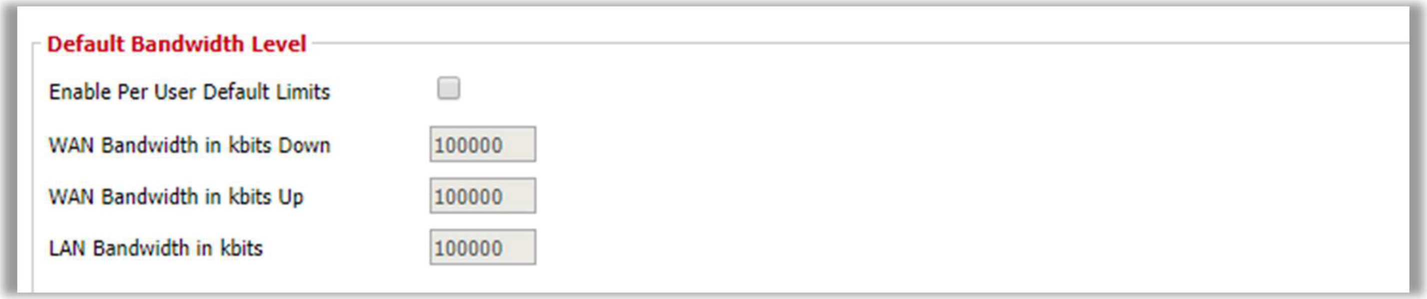
MAC Priority

Delete	MAC Address	WAN Max Down	WAN Max Up	LAN Max	Priority
□	00:00:00:00:00:00	100 kBits	100 kBits	0 kBits	Manual ▼
Add	00 : 00 : 00 : 00 : 00 : 00				

Port Forwarding > QoS > MAC Priority

7.7.6 Default Bandwidth Level

Enable per WAN or LAN default Bandwidth limits.



Default Bandwidth Level

Enable Per User Default Limits	□
WAN Bandwidth in kbits Down	100000
WAN Bandwidth in kbits Up	100000
LAN Bandwidth in kbits	100000

Port Forwarding > QoS > Default Bandwidth Level

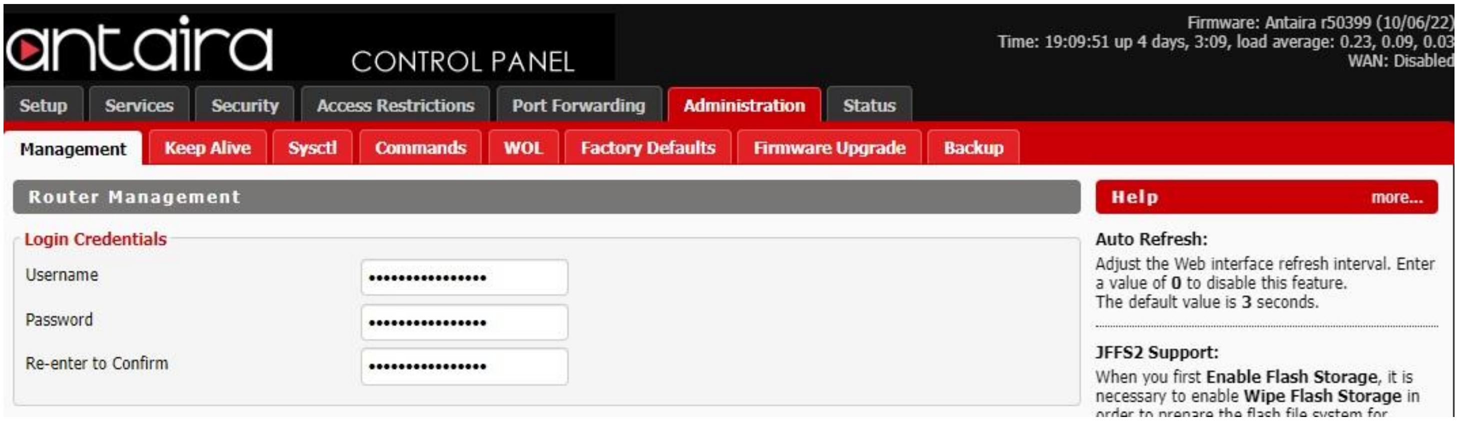
Default Bandwidth Level	Description
Enable Per USer Default Limits	Enable per user default limits.
WAN Bandwidth in kbits Down	Set WAN bandwidth down.
WAN Bandwidth in kbits Up	Set WAN bandwidth up.
LAN Bandwidth in kbits	Set LAN bandwidth.

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 Login Credentials



Firmware: Antaira r50399 (10/06/22)
Time: 19:09:51 up 4 days, 3:09, load average: 0.23, 0.09, 0.03
WAN: Disabled

Login Credentials

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

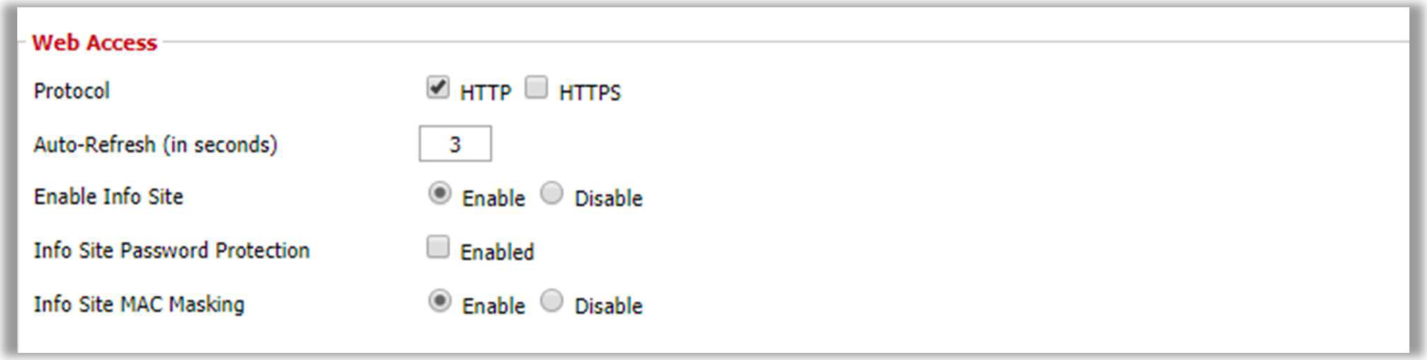
Auto Refresh:
Adjust the Web interface refresh interval. Enter a value of **0** to disable this feature.
The default value is **3** seconds.

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

Administration > Management > Login Credentials

Login Credentials	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 (in seconds)	3
Enable Info Site	● Enable ○ Disable
Info Site Password Protection	☐ Enabled
Info Site MAC Masking	● Enable ○ Disable

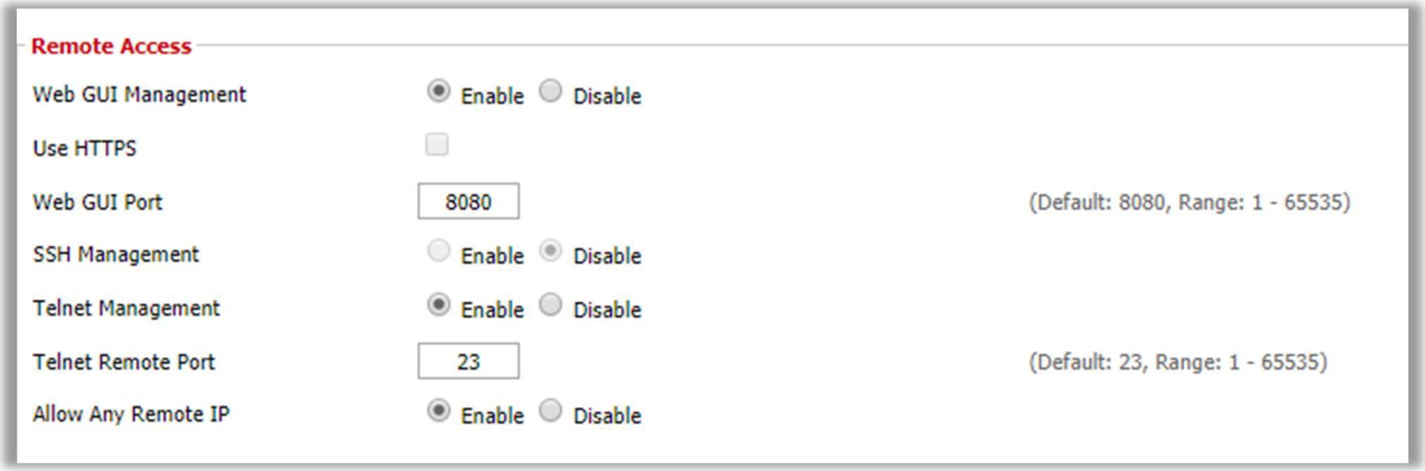
Administration > Management > Web Access

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 site Password Protection	Password to 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 GUI Management ● Enable ○ Disable

Use HTTPS □

Web GUI Port 8080 (Default: 8080, Range: 1 - 65535)

SSH Management ○ Enable ● Disable

Telnet Management ● Enable ○ Disable

Telnet Remote Port 23 (Default: 23, Range: 1 - 65535)

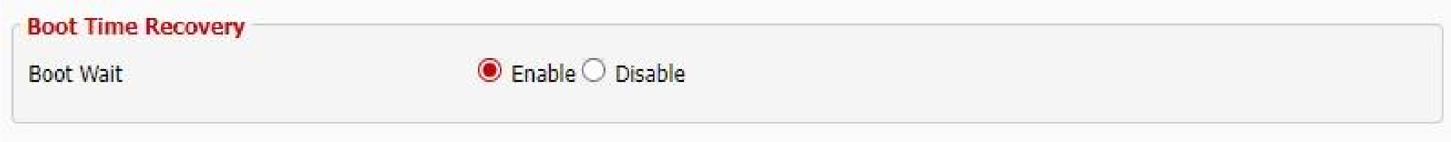
Allow Any Remote IP ● Enable ○ Disable

Administration > Management > Remote Access

Remote Access	Description
Web GUI Management	Enable or disable remote access to 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 Telnet 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 Time Recovery 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.



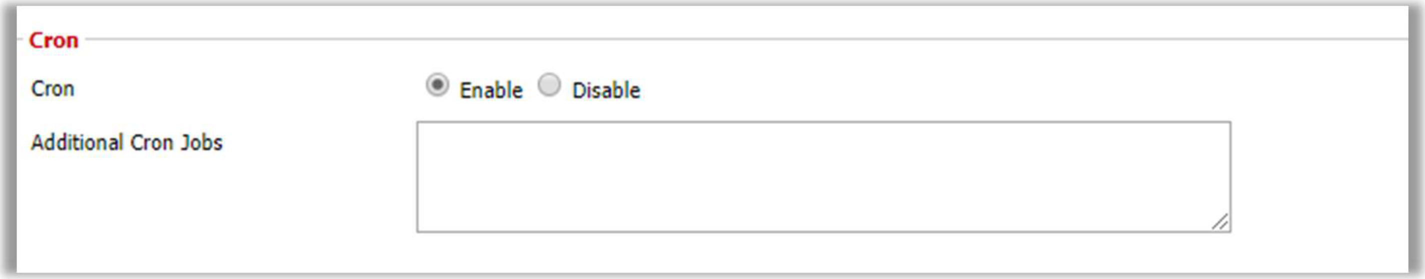
Boot Time Recovery

Boot Wait ● Enable ○ Disable

Administration > Management > Boot Time Recovery

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

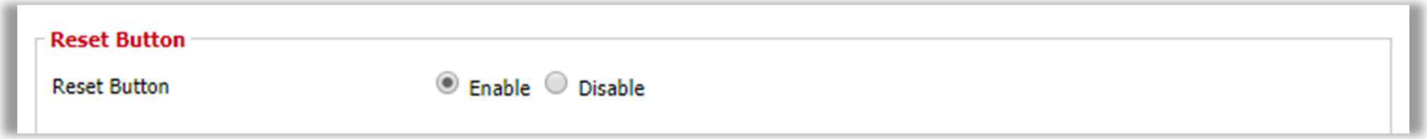
Cron ● Enable ○ Disable

Additional Cron Jobs

Administration > Management > Cron

8.1.6 Reset Button

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



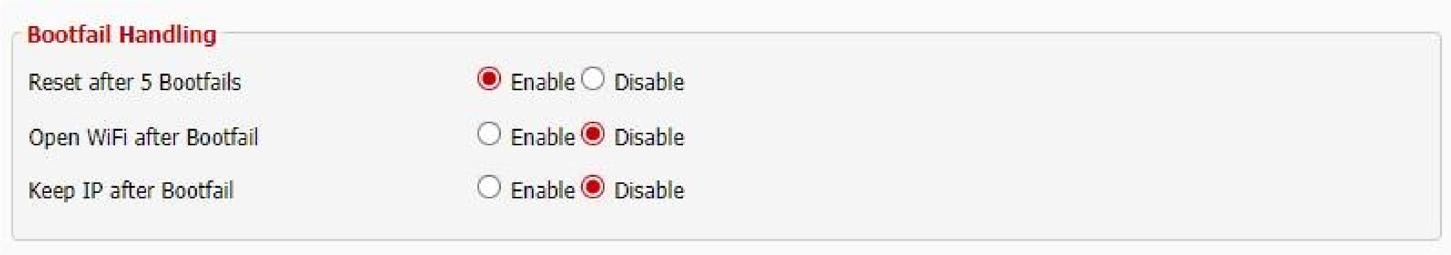
Reset Button

Reset Button ● Enable ○ Disable

Administration > Management > Reset Button

- Short press – Reset the router (reboot)
- Long press (>5s) – Reboot and restore the factory default configuration.

8.1.7 Bootfail Handling



Bootfail Handling

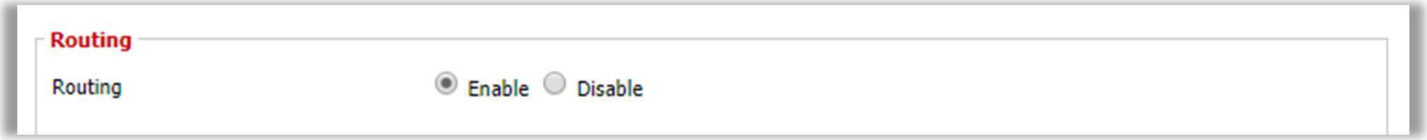
Reset after 5 Bootfails ● Enable ○ Disable

Open WiFi after Bootfail ○ Enable ● Disable

Keep IP after Bootfail ○ Enable ● Disable

Administration > Management > Bootfail Handling

8.1.8 JFFS2 Support



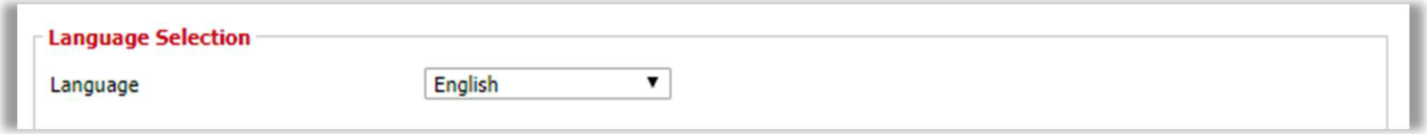
Routing

Routing ● Enable ○ Disable

Administration > Management > JFFS2 Support

8.1.9 Language Selection

Select the language presented on the router.



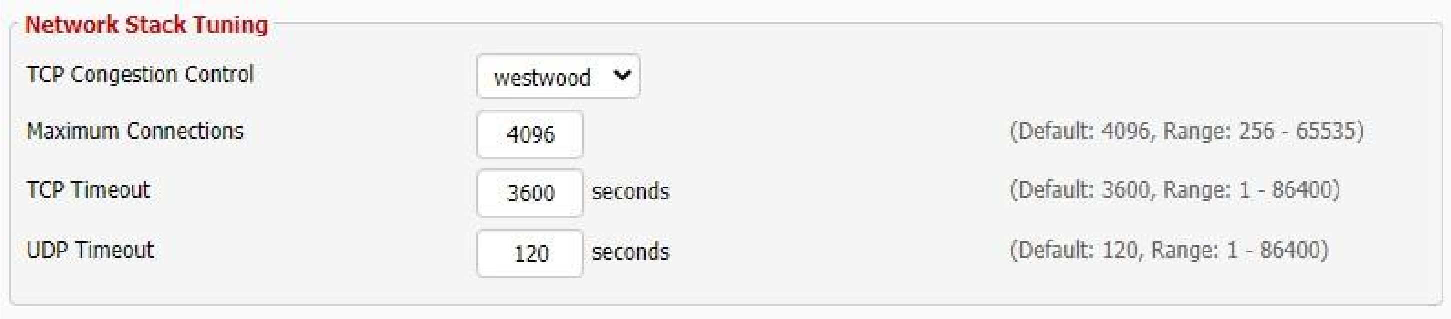
Language Selection

Language: English ▾

Administration > Management > Language Selection

8.1.10 Network Stack Tuning

If you have any peer-to-peer applications running on your network, please increase the maximum ports and lower the TCP/UDP timeouts. This is necessary to maintain router stability because peer-to-peer applications open many connections and do not close them properly.



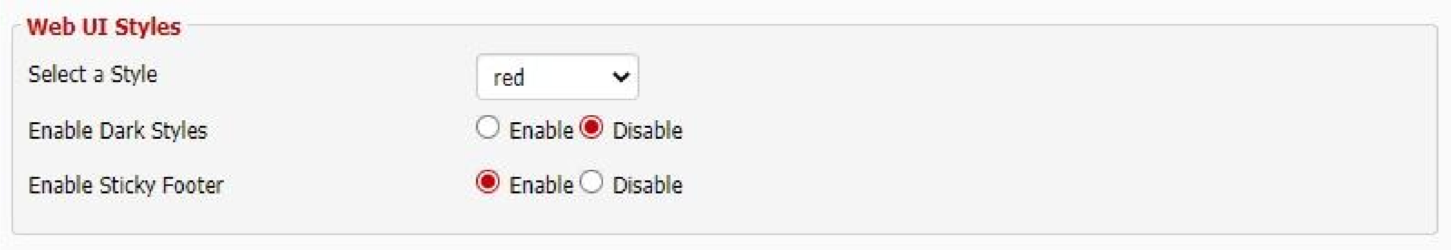
Network Stack Tuning

TCP Congestion Control	westwood ▾	
Maximum Connections	4096	(Default: 4096, Range: 256 - 65535)
TCP Timeout	3600 seconds	(Default: 3600, Range: 1 - 86400)
UDP Timeout	120 seconds	(Default: 120, Range: 1 - 86400)

Administration > Management > Network Stack Tuning

8.1.11 Web UI Styles

Select the graphical style of the web UI.

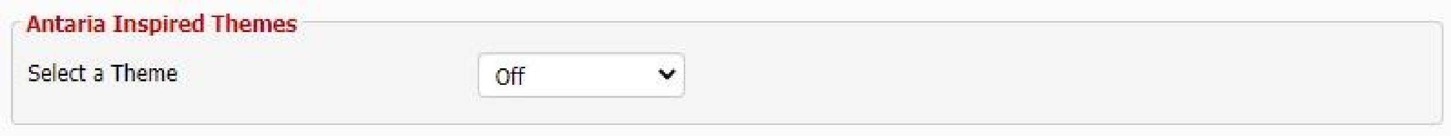


Web UI Styles

Select a Style	red ▾
Enable Dark Styles	○ Enable ● Disable
Enable Sticky Footer	● Enable ○ Disable

Administration > Management > Web UI Styles

8.1.12 Antaira Inspired Themes

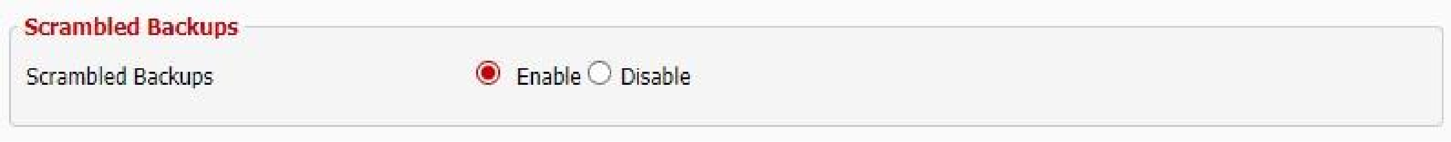


Antaria Inspired Themes

Select a Theme: Off

Administration > Management > Antaira Inspired Themes

8.1.13 Scrambled Backups



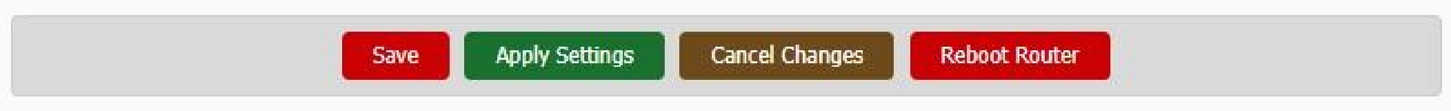
Scrambled Backups

Scrambled Backups: ● Enable ○ Disable

Administration > Management > Scrambled Backups

8.1.14 Router Reboot

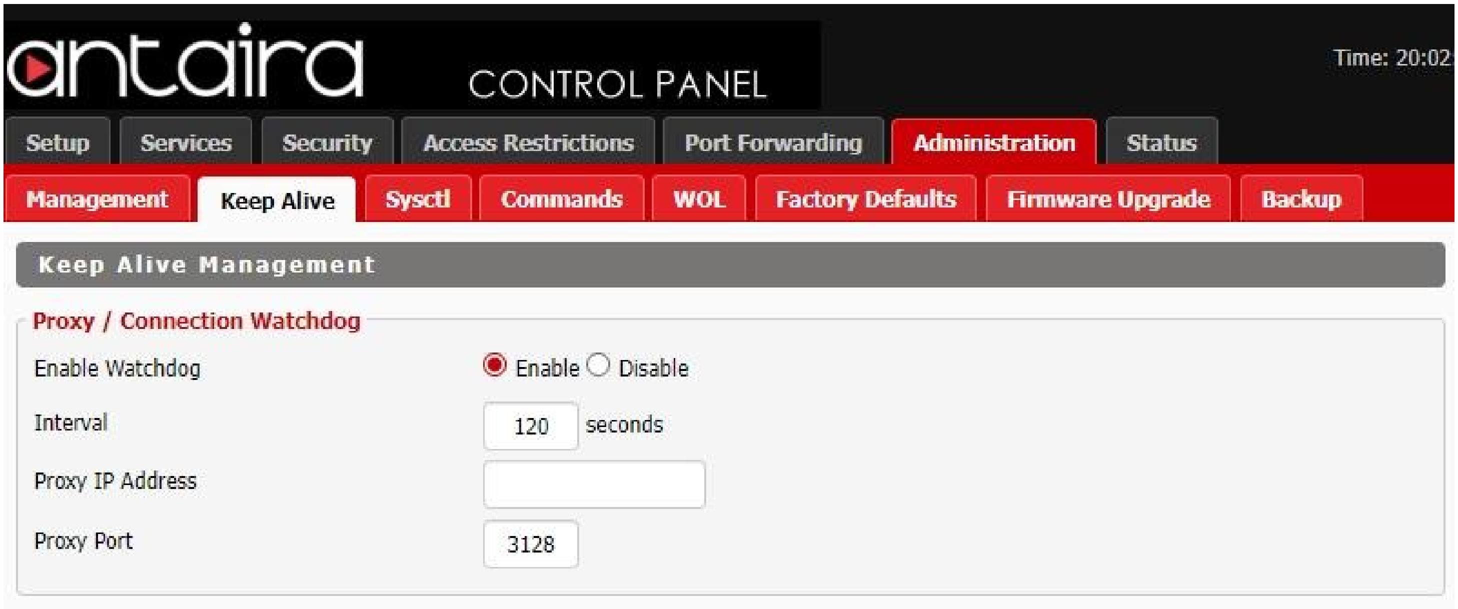
You may reboot the router under this page as well.



Administration > Management > Router Reboot

8.2 Keep Alive

8.2.1 Proxy/Connection Watchdog



Keep Alive Management

Proxy / Connection Watchdog

Enable Watchdog: ● Enable ○ Disable

Interval: 120 seconds

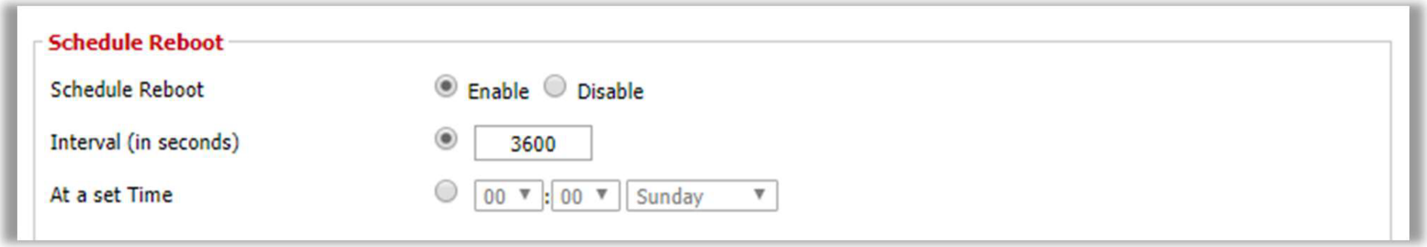
Proxy IP Address:

Proxy Port: 3128

Administration > Keep Alive > Proxy/Connection Watchdog

8.2.2 Schedule Reboot

You can schedule regular reboots for the router after a certain amount of seconds or at a specific date and time each week or everyday.

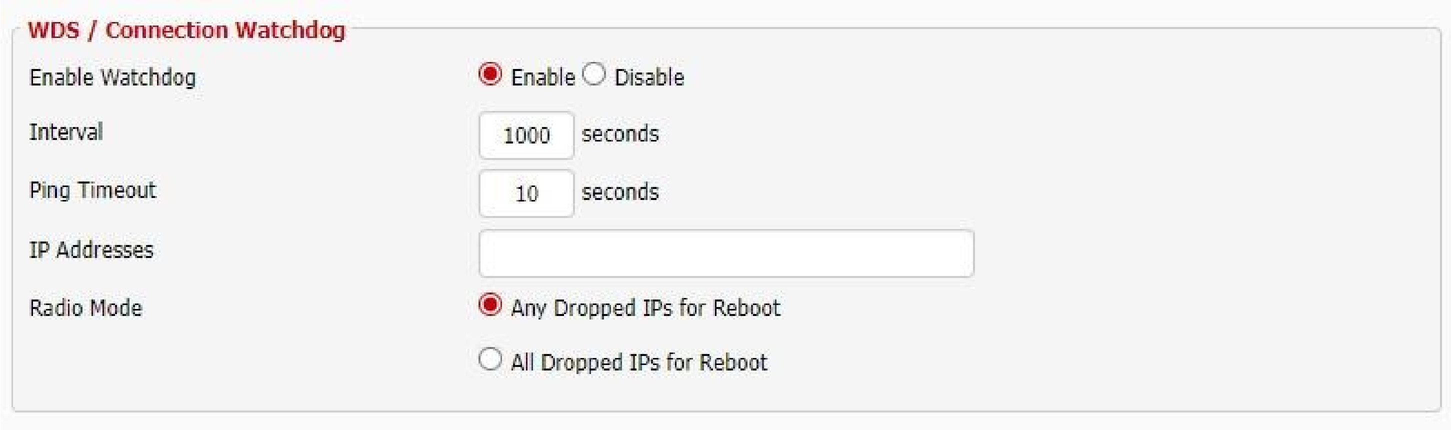


Schedule Reboot

Schedule Reboot	● Enable ○ Disable
Interval (in seconds)	● 3600
At a set Time	○ 00 ▼ : 00 ▼ Sunday ▼

Administration > Keep Alive > Schedule Reboot

8.2.3 WDS/Connection Watchdog



WDS / Connection Watchdog

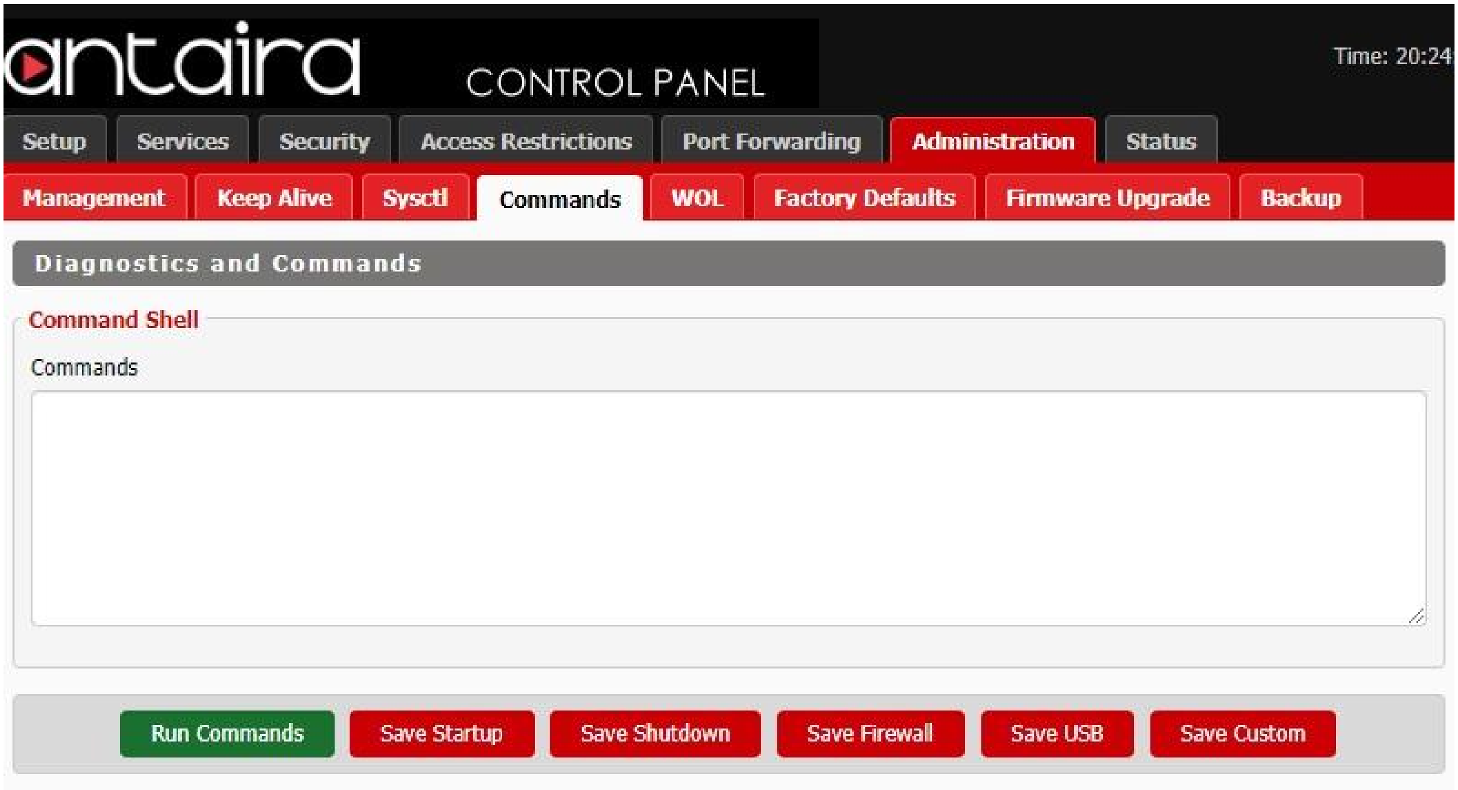
Enable Watchdog	● Enable ○ Disable
Interval	1000 seconds
Ping Timeout	10 seconds
IP Addresses	
Radio Mode	● Any Dropped IPs for Reboot ○ All Dropped IPs for Reboot

Administration > Keep Alive > WDS/Connection Watchdog

8.3 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 specify commands to be executed during the router startup. Fill the text area with commands (*only one command per row*) and click **Save Startup**.

Each time the firewall is started, custom firewall rules can be added to the chain. Fill the text area with additional iptables/ip6tables *commands* (*only one command per row*) and click **Save Firewall**.



Diagnostics and Commands

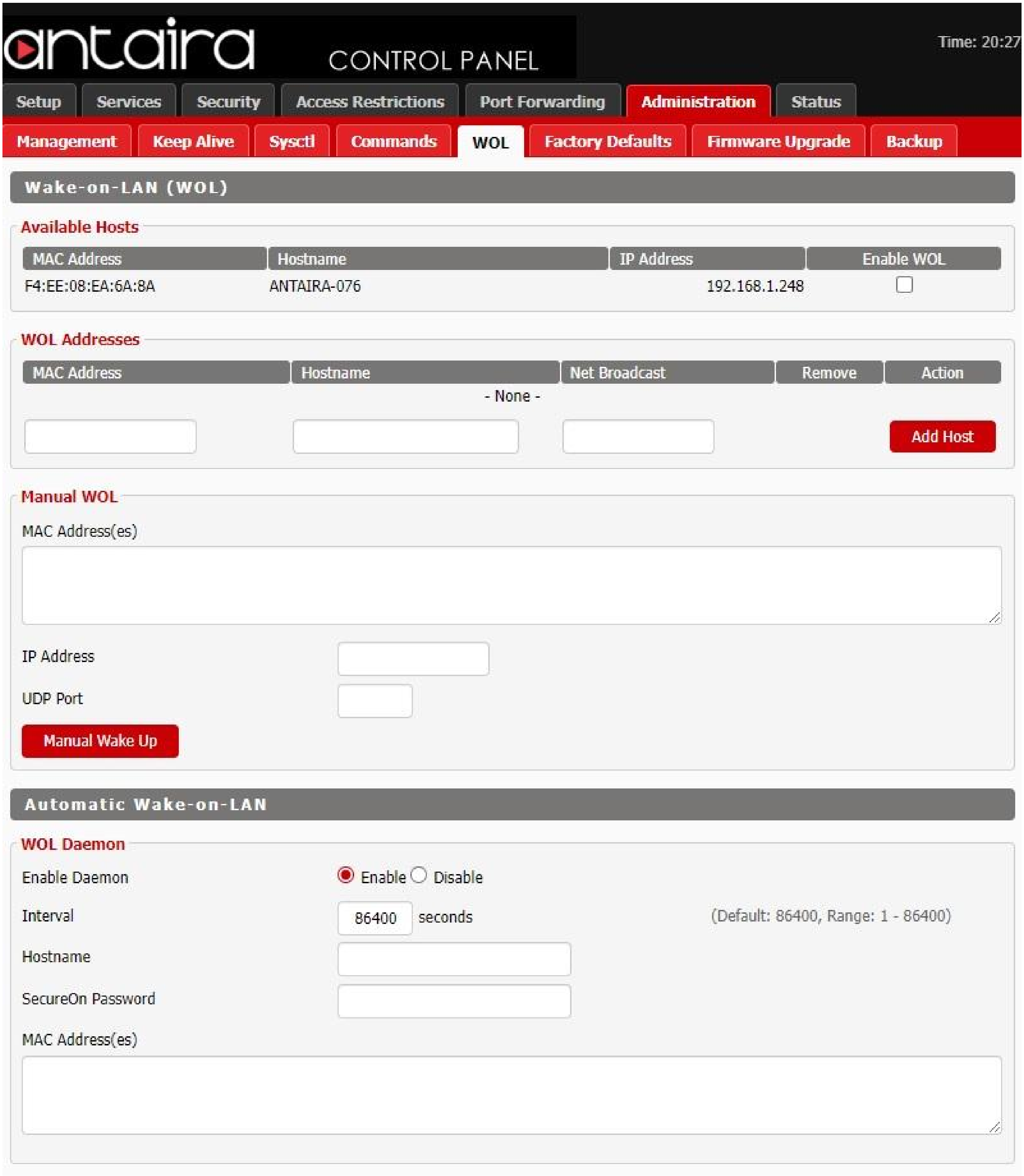
Command Shell

Commands

Administration > Commands

8.4 Wake on LAN (WOL)

This page allows you to Wake Up hosts on your local network.



Wake-on-LAN (WOL)

Available Hosts

MAC Address	Hostname	IP Address	Enable WOL
F4:EE:08:EA:6A:8A	ANTAIRA-076	192.168.1.248	□

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

Interval 86400 seconds (Default: 86400, Range: 1 - 86400)

Hostname

SecureOn Password

MAC Address(es)

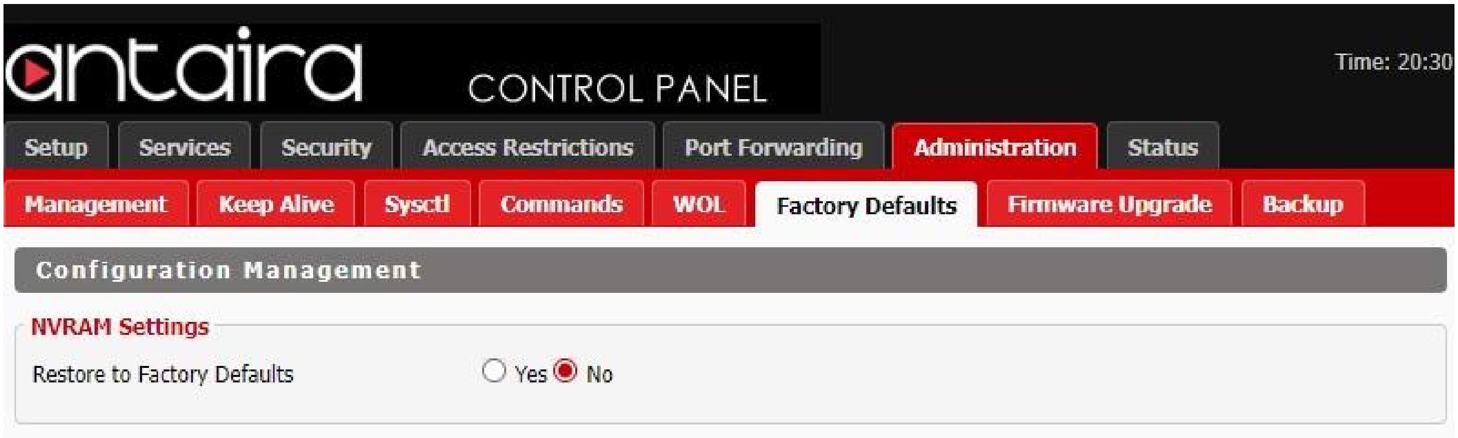
Administration > WOL

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 manual WOL section allows an 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.

8.5 Factory Defaults

If you are having problems with your router, you can restore the factory default configurations here. Any settings you have saved will be lost when the default settings are restored. After restoring the router, it will be accessible under the default IP address **192.168.1.1** and the default password **admin**.



Configuration Management

NVRAM Settings

Restore to Factory Defaults ○ Yes ● No

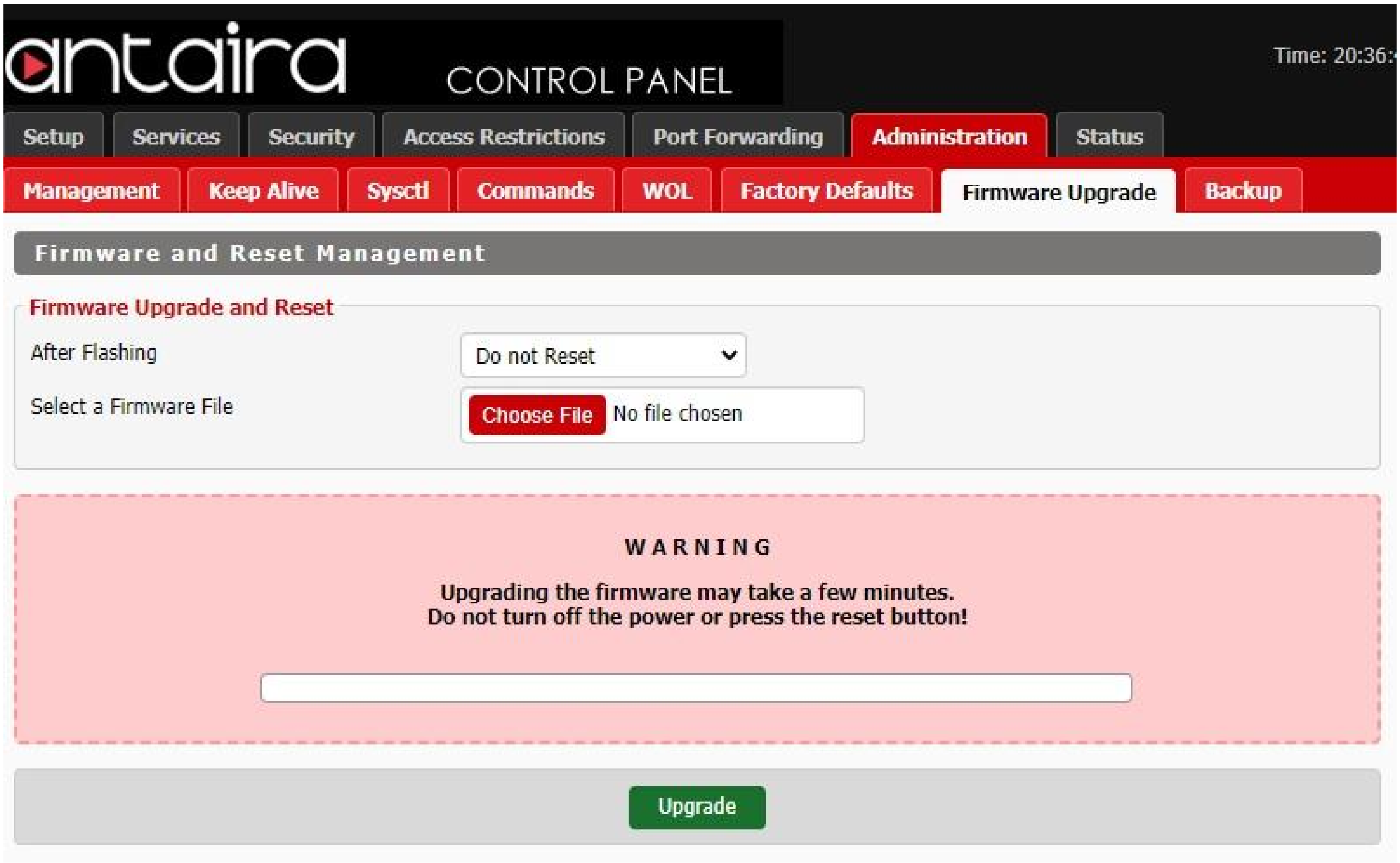
Administration > Factory Defaults

8.6 Firmware Upgrade

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 upgrade 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 interrupt 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.



Firmware and Reset Management

Firmware Upgrade and Reset

After Flashing: Do not Reset

Select a Firmware File: No file chosen

WARNING

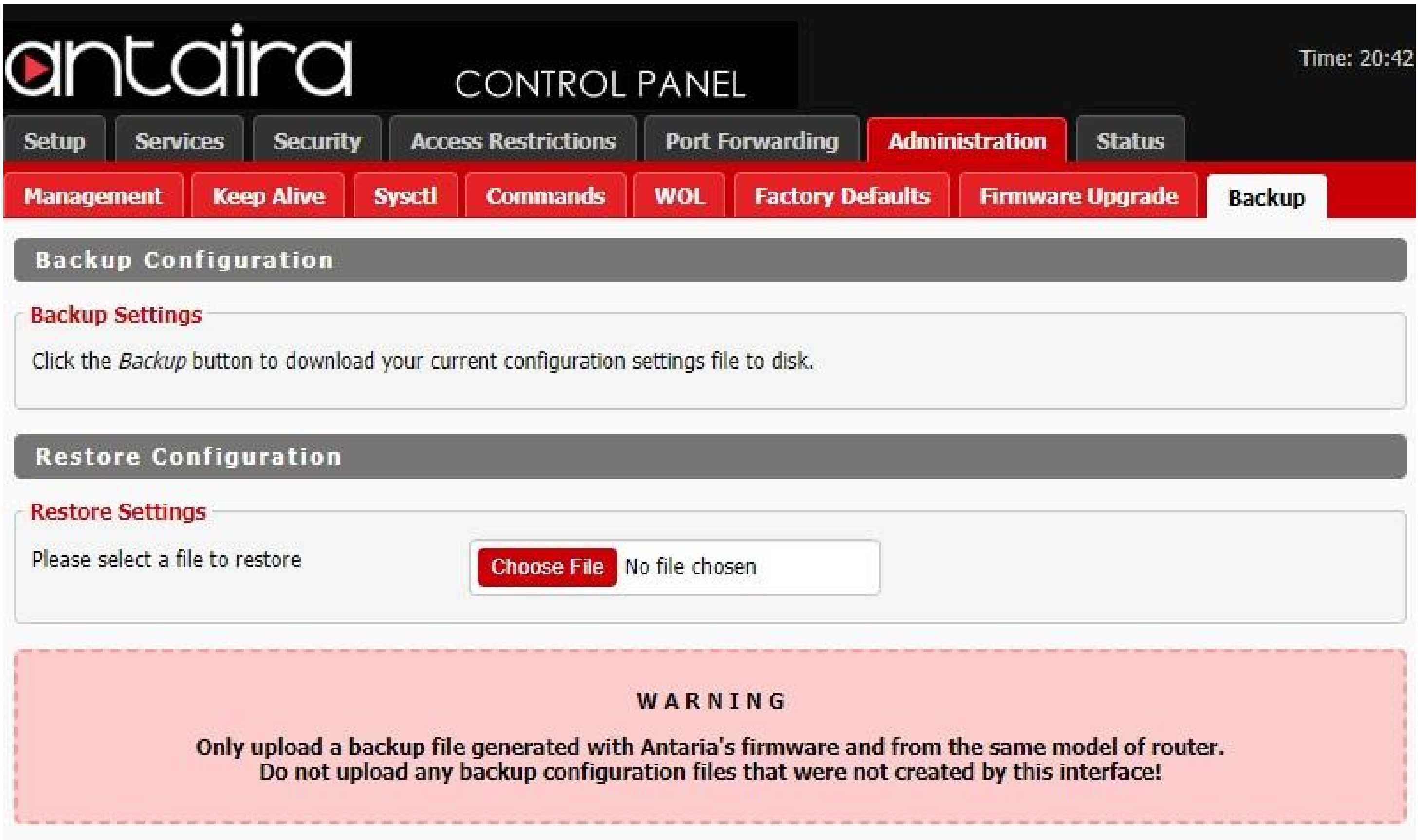
Upgrading the firmware may take a few minutes.
Do not turn off the power or press the reset button!

Administration > Firmware Upgrade

8.7 Backup

You may backup your current configurations in case you need to reset the router back to its factory default settings. Click the Backup button to download your current router configurations to your PC.

To restore settings, click the Choose File button to browse for the configuration file that you saved on your PC. Click Restore to overwrite all current configurations with the ones in the configuration file.



Backup Configuration

Backup Settings

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

Restore Configuration

Restore Settings

Please select a file to restore No file chosen

WARNING

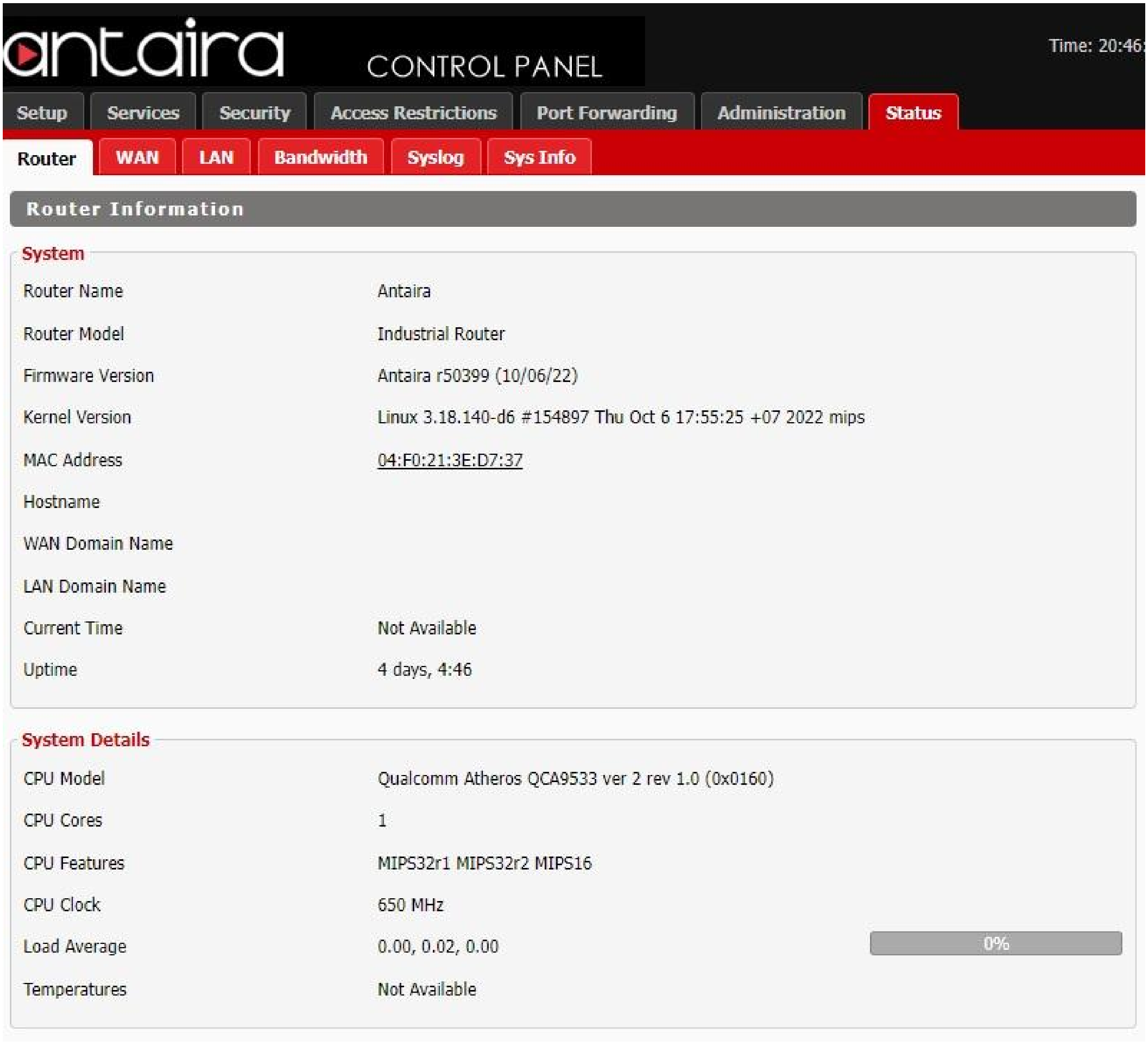
**Only upload a backup file generated with Antaria's firmware and from the same model of router.
Do not upload any backup configuration files that were not created by this interface!**

Administration > Backup

9 Status

9.1 Router

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



Router Information

System

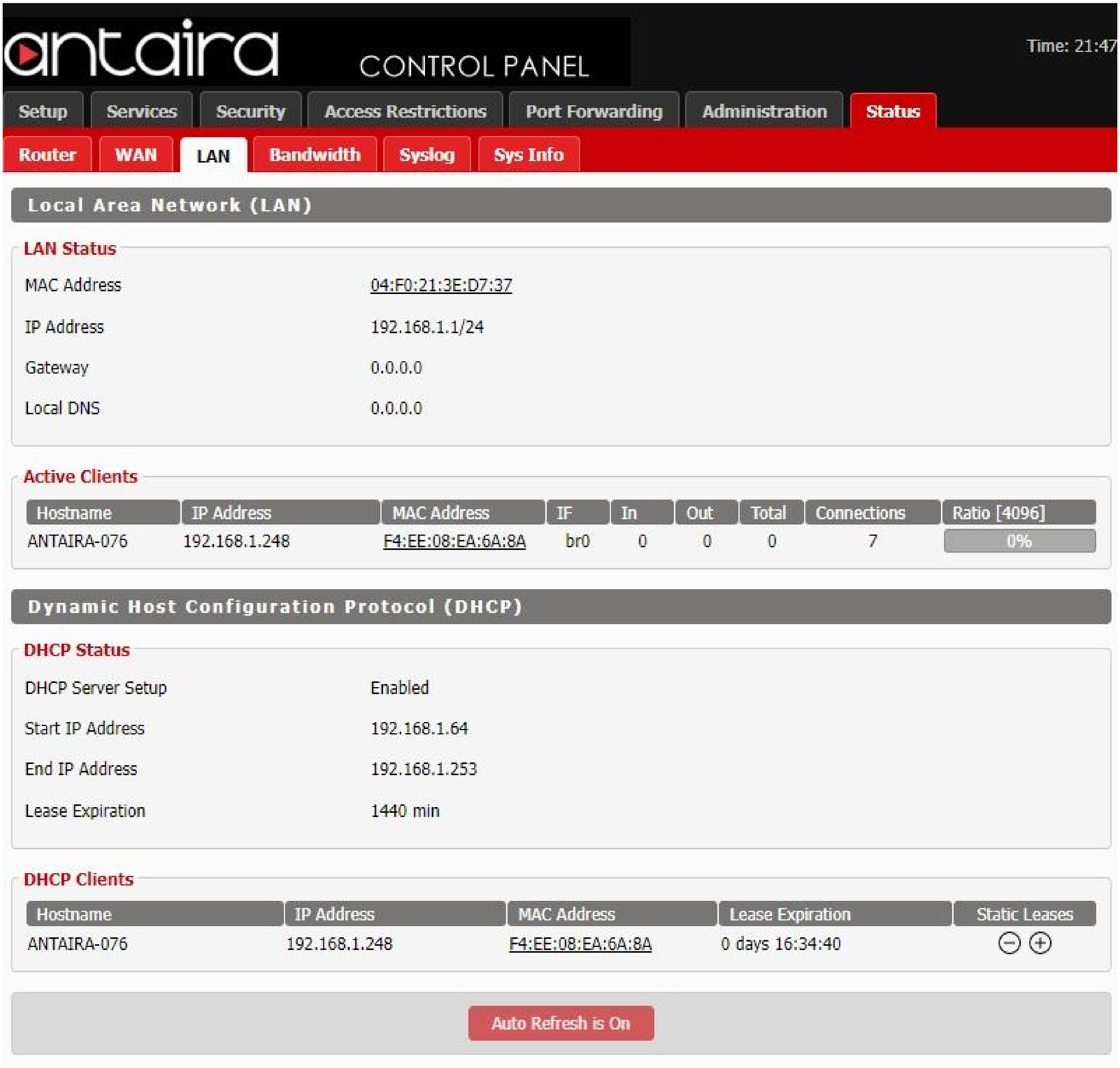
Router Name	Antaira
Router Model	Industrial Router
Firmware Version	Antaira r50399 (10/06/22)
Kernel Version	Linux 3.18.140-d6 #154897 Thu Oct 6 17:55:25 +07 2022 mips
MAC Address	04:F0:21:3E:D7:37
Hostname	
WAN Domain Name	
LAN Domain Name	
Current Time	Not Available
Uptime	4 days, 4:46

System Details

CPU Model	Qualcomm Atheros QCA9533 ver 2 rev 1.0 (0x0160)	
CPU Cores	1	
CPU Features	MIPS32r1 MIPS32r2 MIPS16	
CPU Clock	650 MHz	
Load Average	0.00, 0.02, 0.00	0%
Temperatures	Not Available	

Status > Router > Router Information

9.2 LAN



Local Area Network (LAN)

LAN Status

MAC Address	04:F0:21:3E:D7:37
IP Address	192.168.1.1/24
Gateway	0.0.0.0
Local DNS	0.0.0.0

Active Clients

Hostname	IP Address	MAC Address	IF	In	Out	Total	Connections	Ratio [4096]
ANTAIRA-076	192.168.1.248	F4:EE:08:EA:6A:8A	br0	0	0	0	7	0%

Dynamic Host Configuration Protocol (DHCP)

DHCP Status

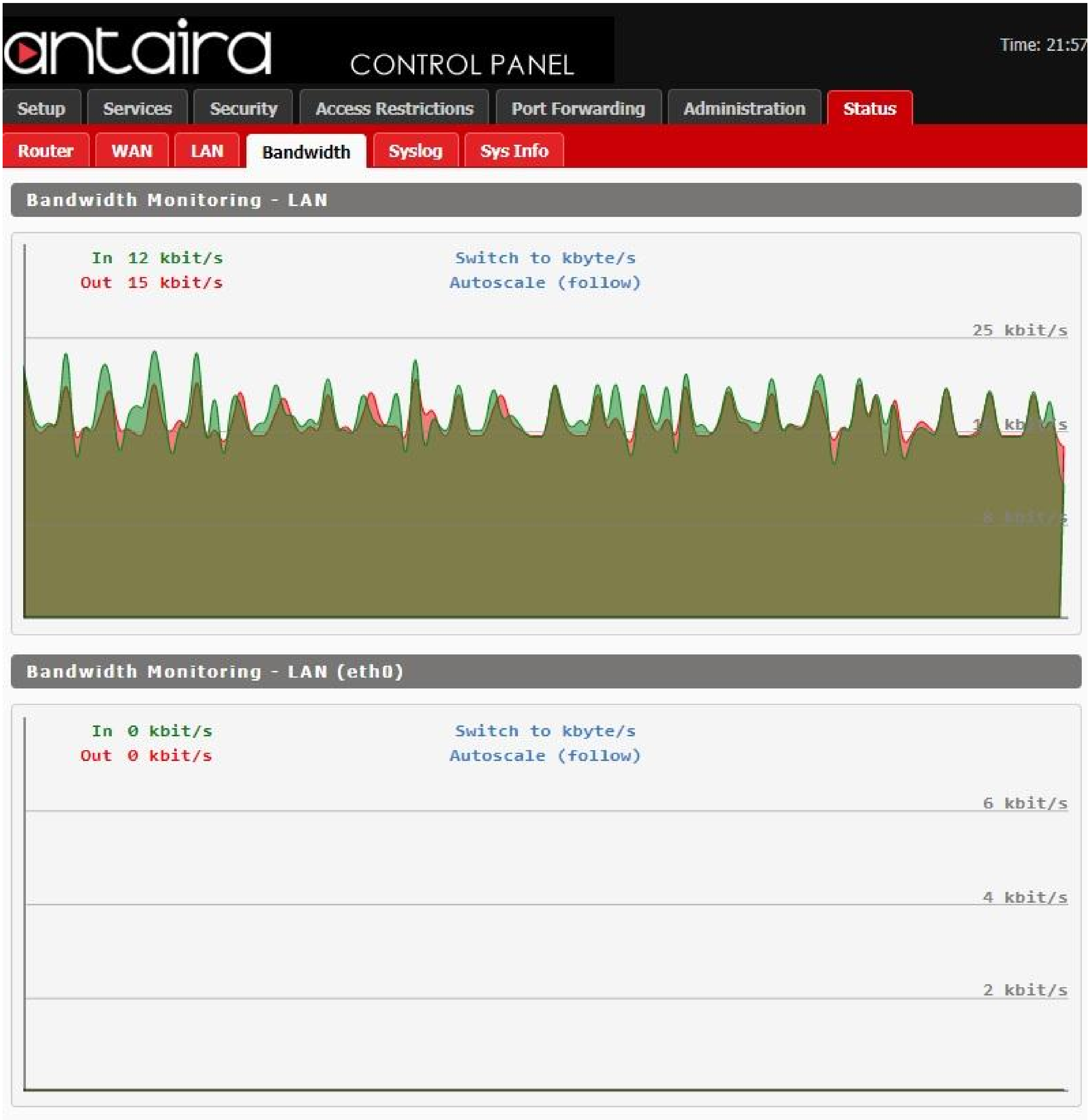
DHCP Server Setup	Enabled
Start IP Address	192.168.1.64
End IP Address	192.168.1.253
Lease Expiration	1440 min

DHCP Clients

Hostname	IP Address	MAC Address	Lease Expiration	Static Leases
ANTAIRA-076	192.168.1.248	F4:EE:08:EA:6A:8A	0 days 16:34:40	⊖ ⊕

Status > LAN

9.3 Bandwidth



Bandwidth Monitoring - LAN

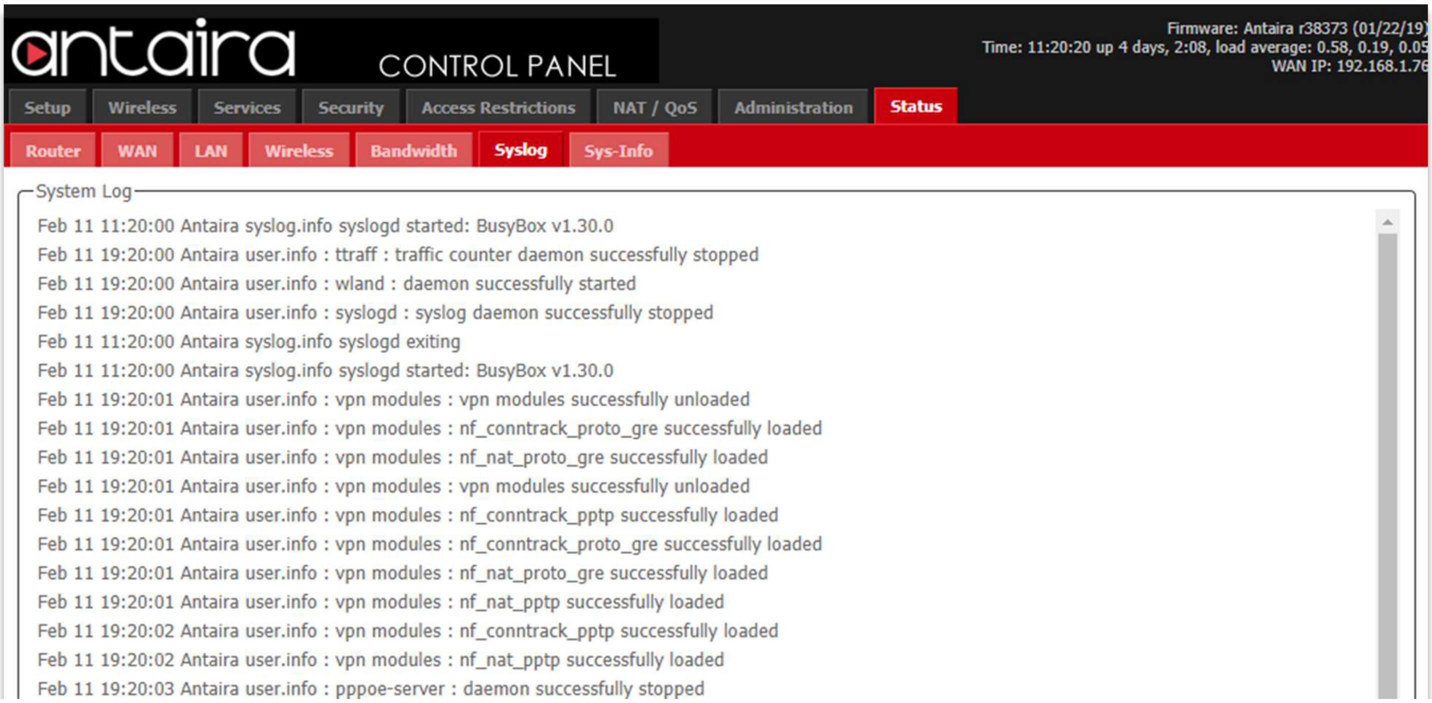
In 12 kbit/s
Out 15 kbit/s

Bandwidth Monitoring - LAN (eth0)

In 0 kbit/s
Out 0 kbit/s

Status > Bandwidth

9.4 Syslog



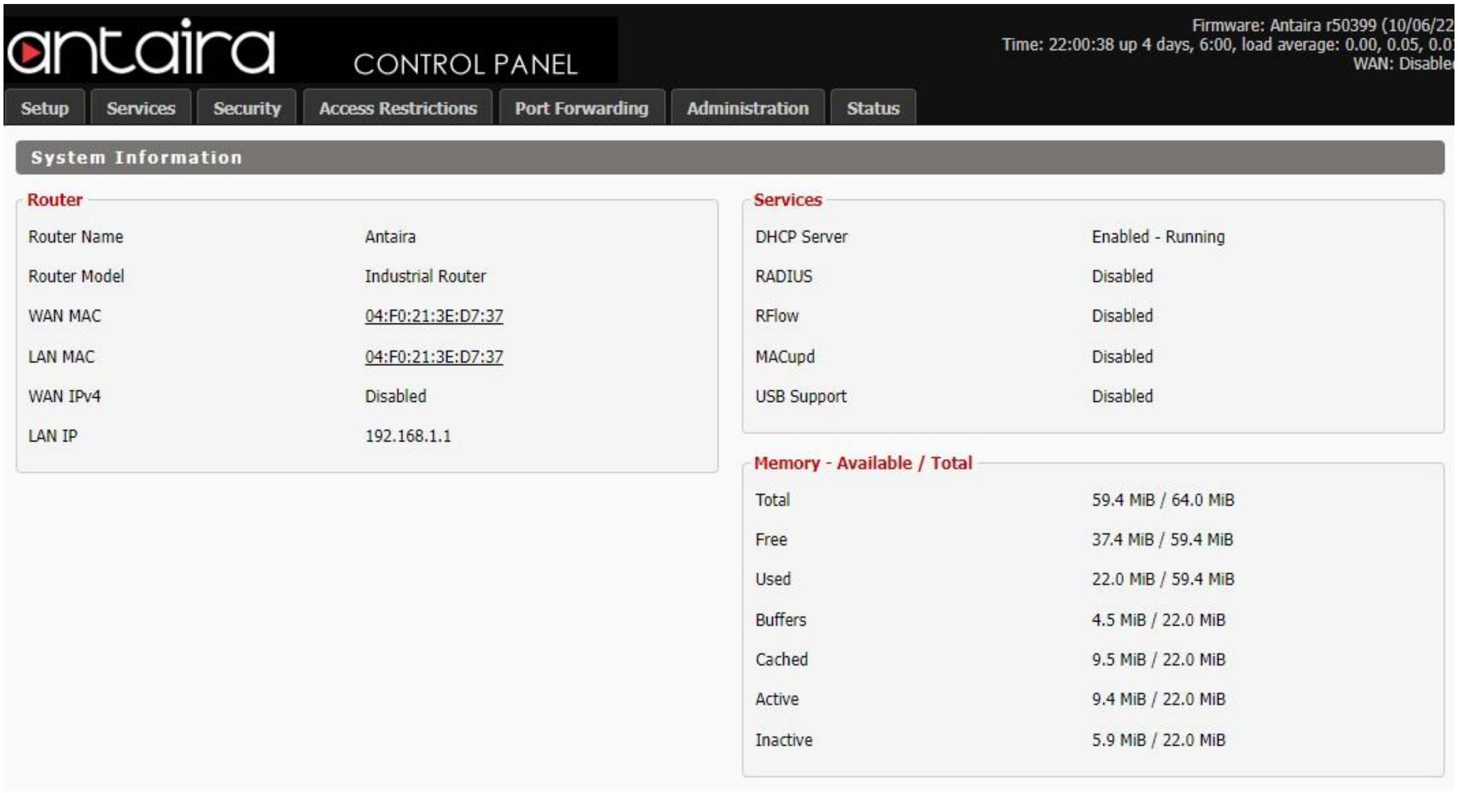
Firmware: Antaira r38373 (01/22/19)
Time: 11:20:20 up 4 days, 2:08, load average: 0.58, 0.19, 0.05
WAN IP: 192.168.1.76

System Log

```
Feb 11 11:20:00 Antaira syslog.info syslogd started: BusyBox v1.30.0
Feb 11 19:20:00 Antaira user.info : ttraff : traffic counter daemon successfully stopped
Feb 11 19:20:00 Antaira user.info : wland : daemon successfully started
Feb 11 19:20:00 Antaira user.info : syslogd : syslog daemon successfully stopped
Feb 11 11:20:00 Antaira syslog.info syslogd exiting
Feb 11 11:20:00 Antaira syslog.info syslogd started: BusyBox v1.30.0
Feb 11 19:20:01 Antaira user.info : vpn modules : vpn modules successfully unloaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_conntrack_proto_gre successfully loaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_nat_proto_gre successfully loaded
Feb 11 19:20:01 Antaira user.info : vpn modules : vpn modules successfully unloaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_conntrack_pptp successfully loaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_conntrack_proto_gre successfully loaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_nat_proto_gre successfully loaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_nat_pptp successfully loaded
Feb 11 19:20:02 Antaira user.info : vpn modules : nf_conntrack_pptp successfully loaded
Feb 11 19:20:02 Antaira user.info : vpn modules : nf_nat_pptp successfully loaded
Feb 11 19:20:03 Antaira user.info : pppoe-server : daemon successfully stopped
```

Status > Syslog

9.5 System Information



Firmware: Antaira r50399 (10/06/22
Time: 22:00:38 up 4 days, 6:00, load average: 0.00, 0.05, 0.0
WAN: Disable

System Information

Router

Router Name	Antaira
Router Model	Industrial Router
WAN MAC	04:F0:21:3E:D7:37
LAN MAC	04:F0:21:3E:D7:37
WAN IPv4	Disabled
LAN IP	192.168.1.1

Services

DHCP Server	Enabled - Running
RADIUS	Disabled
RFlow	Disabled
MACupd	Disabled
USB Support	Disabled

Memory - Available / Total

Total	59.4 MiB / 64.0 MiB
Free	37.4 MiB / 59.4 MiB
Used	22.0 MiB / 59.4 MiB
Buffers	4.5 MiB / 22.0 MiB
Cached	9.5 MiB / 22.0 MiB
Active	9.4 MiB / 22.0 MiB
Inactive	5.9 MiB / 22.0 MiB

Status > System Information

Antaira Customer Service and Support

(Antaira US Headquarter) + 844-268-2472

(Antaira Europe Office) + 48-22-862-88-81

(Antaira Asia Office) + 886-2-2218-9733

Please report any problems to Antaira:

www.antaira.com / support@antaira.com

www.antaira.eu / info@antaira.eu

www.antaira.com.tw / info@antaira.com.tw

Any changes to this material will be announced