



# Wireless Router Software User's Manual

Version 1.1  
(April 2019)

**© Copyright 2019 Antaira Technologies, LLC.**

All Rights Reserved

This document contains information, which is protected by copyright. Reproduction, adaptation or translation without prior permission is prohibited, except as allowed under the copyright laws.

**Trademark Information**

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

**Disclaimer**

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

## FCC Notice

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

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

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

## CE Mark Warning

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

## Industrial Ethernet Wireless APs

Software User Manual

This manual supports the following models:

- ARS-7131-AC
- ARS-7131-AC-T
- ARS-7231-AC
- ARS-7231-AC-T
- ARS-7131
- ARS-7131-T

This manual supports the following software version:

- Release: Antaira r38373 (01/22/19)

Please check our website ([www.antaira.com](http://www.antaira.com)) for any updated manual or contact us by e-mail ([support@antaira.com](mailto:support@antaira.com)).

## Table of Contents

<b>1.</b>	<b>Access with Web Browser .....</b>	<b>7</b>
1.1	Web GUI Login .....	7
1.2	Operation Modes .....	8
1.2.1	Access Point .....	8
1.2.2	Client Mode .....	9
1.2.3	Client Bridge Mode .....	10
1.2.4	Ad Hoc Mode .....	11
1.2.5	WDS Station/WDS Access Point....	12
1.2.6	Repeater Mode .....	13
<b>2.</b>	<b>Setup .....</b>	<b>14</b>
2.1	Basic Setup .....	14
2.1.1	WAN Setup .....	15
2.1.2	Optional Settings.....	16
2.1.3	Router IP .....	17
2.1.4	Network Address Server Settings (DHCP)	18
2.1.5	Time Settings .....	19
2.2	IPv6 .....	20
2.3	DDNS .....	22
2.4	MAC Address Clone .....	23
2.5	Advanced Routing .....	24
2.5.1	Gateway .....	25
2.5.2	BGP .....	27
2.5.3	RIP2 Router .....	29
2.5.4	OSPF Router .....	30
2.5.5	OSPF & RIP2 Router .....	32
2.5.6	OLSR Router .....	33
2.5.7	Router .....	36
2.6	Networking .....	37
2.6.1	VLAN Tagging .....	37
2.6.2	Bridging .....	38

2.6.3	IP Virtual Server.....	39
2.6.4	Create Virtual Server .....	39
2.6.5	Port Setup .....	40
2.6.6	DHCPD .....	40
2.7	Tunnels.....	41
2.7.1	Ethernet and IP Tunneling.....	41
<b>3.</b>	<b>Wireless</b>	<b>43</b>
3.1	Basic Settings.....	43
3.1.1	Wireless Site Survey.....	43
3.1.2	Wireless Mode .....	44
3.1.3	Wireless Network Mode .....	45
3.1.4	Channel Width .....	46
3.1.5	Wireless Network Name (SSID) .....	47
3.1.6	Advanced Settings.....	48
3.1.7	Radio Time Restrictions .....	50
3.1.8	Virtual Interfaces .....	51
3.1.9	Advanced Settings .....	51
3.1.10	Network Configuration .....	52
3.2	Wireless Security.....	53
3.2.1	WPA.....	54
3.2.2	RADIUS .....	55
3.2.3	WEP .....	56
3.2.4	802.1x/EAP .....	58
3.3	MAC Filter .....	59
3.3.1	Edit MAC Filter List .....	60
3.4	WDS.....	61
<b>4.</b>	<b>Services</b>	<b>62</b>
4.1	Services.....	62
4.1.1	DHCP Client .....	62
4.1.2	DHCP Server .....	63
4.1.3	Dnsmasq.....	64
4.1.4	Lighttpd Webserver.....	65
4.1.5	Mikrotik MAC Telnet .....	65
4.1.6	PPPoE Relay .....	66

4.1.7	SES/AOSS/EZ-SETUP/WPS Button	66
4.1.8	RFlow/MACUpd.....	66
4.1.9	SNMP.....	67
4.1.10	Secure Shell.....	68
4.1.11	System Log.....	68
4.1.12	Telnet.....	69
4.1.13	The Onion Router Project.....	69
4.1.14	WAN Traffic Counter.....	70
4.2	FreeRadius.....	71
4.3	PPPoE Server.....	73
4.4	VPN.....	74
4.4.1	PPTP Server.....	75
4.4.2	PPTP Client.....	77
4.4.3	OpenVPN Server.....	78
4.4.4	OpenVPN Client.....	81
4.4.5	SoftEther VPN.....	83
4.5	USB.....	84
4.6	Hotspot.....	85
4.7	Adblocking.....	86
<b>5.</b>	<b>Security</b>	<b>87</b>
5.1	Firewall.....	87
5.1.1	Security.....	87
5.1.2	Block WAN Request.....	88
5.1.3	Impede WAN DoS/Bruteforce.....	89
5.1.4	Connection Warning Notifier.....	90
5.1.5	Log Management.....	91
5.2	VPN Passthrough.....	92
<b>6.</b>	<b>Access Restrictions</b> .....	<b>93</b>
6.1	WAN Access.....	93
6.1.1	Access Policy.....	93
6.1.2	Days and Times.....	94
6.1.3	Blocked Services.....	94
6.1.4	Website Blocking.....	95
<b>7.</b>	<b>NAT/QoS</b>	<b>95</b>

7.1	Port Forwarding .....	95
7.2	Port Range Forwarding .....	96
7.3	Port Triggering.....	98
7.4	UPnP .....	99
7.5	DMZ.....	100
7.6	QoS .....	101
7.6.1	QoS Settings.....	101
7.6.2	Services Priority .....	103
7.6.3	Interface Priority.....	104
7.6.4	Netmask Priority .....	104
7.6.5	MAC Priority.....	105
7.6.6	Default Bandwidth Level.....	105
<b>8.</b>	<b>Administration .....</b>	<b>106</b>
8.1	Management .....	106
8.1.1	Router Password .....	106
8.1.2	Web Access .....	107
8.1.3	Remote Access.....	107
8.1.4	Boot Wait .....	108
8.1.5	Cron .....	108
8.1.6	802.1x .....	109
8.1.7	Reset Button .....	109
8.1.8	Routing .....	109
8.1.9	JFFS2 Support.....	110
8.1.10	Language Selection .....	110
8.1.11	IP Filter Settings .....	110
8.1.12	Router GUI Style.....	111
8.1.13	Router Reboot .....	111
8.2	Keep Alive .....	111
8.2.1	Proxy/Connection Watchdog .....	111
8.2.2	Schedule Reboot .....	112
8.2.3	WDS/Connection Watchdog .....	112
8.3	Commands .....	112
8.4	Wake on LAN (WOL).....	114
8.5	Factory Defaults .....	115

	8.6	Firmware Upgrade.....	116
	8.7	Backup .....	117
<b>9.</b>		<b>Status</b>	<b>118</b>
	9.1	Router.....	118
	9.2	WAN .....	119
	9.3	LAN .....	121
	9.4	Wireless.....	122
	9.5	Bandwidth.....	126
	9.6	Syslog.....	127
	9.7	Sys-Info .....	128



# 1. Access with Web Browser

## 1.1 Web GUI Login

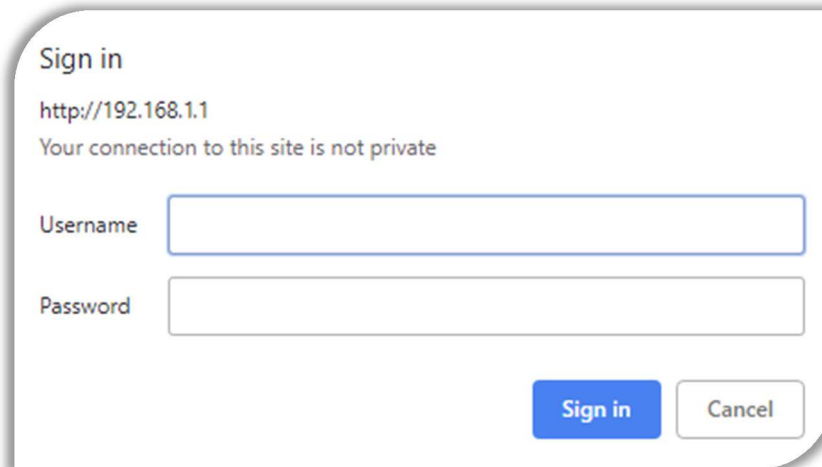
All of Antaira's industrial managed devices are embedded with HTML web GUI interfaces. They provide user-friendly management features through its design and allows users to manage the devices from anywhere on the network through a web browser.

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

**Step 2:** The default WEB GUI login:

Username: root

Password: admin



Sign in

http://192.168.1.1

Your connection to this site is not private

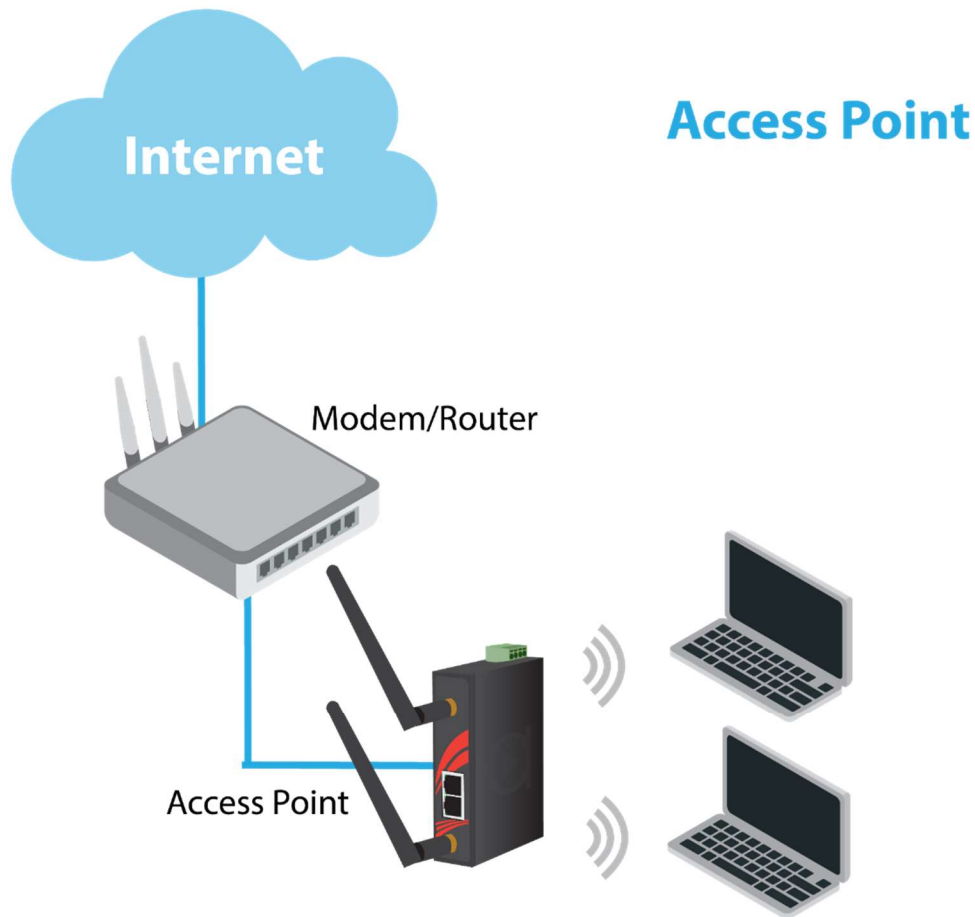
Username

Password

## 1.2 Operation Modes

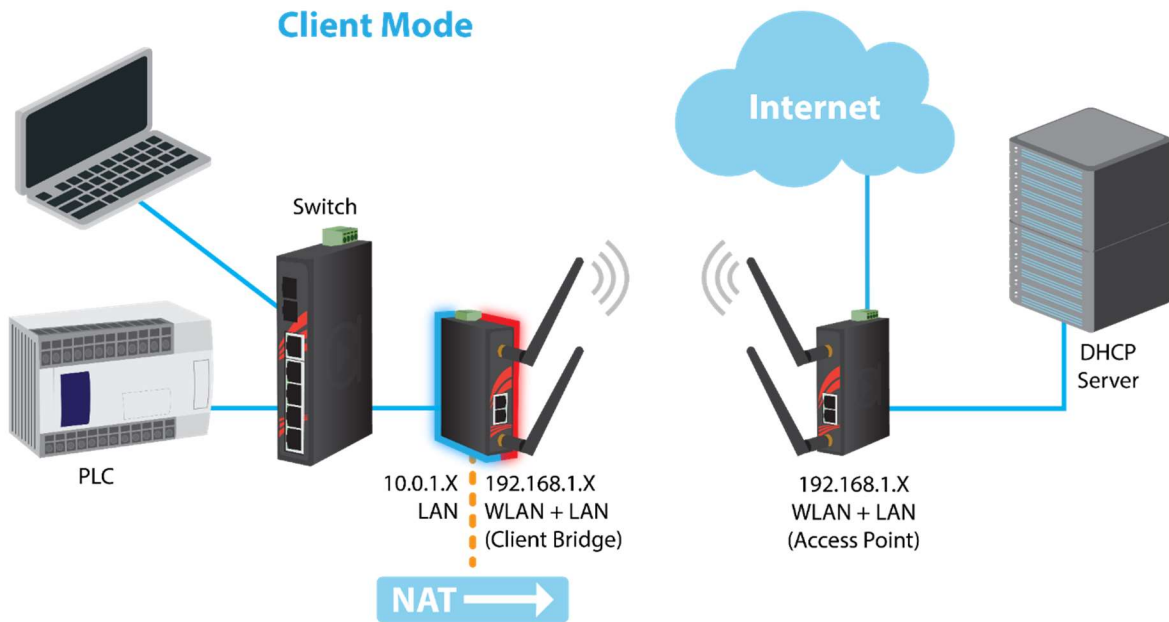
### 1.2.1 Access Point

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



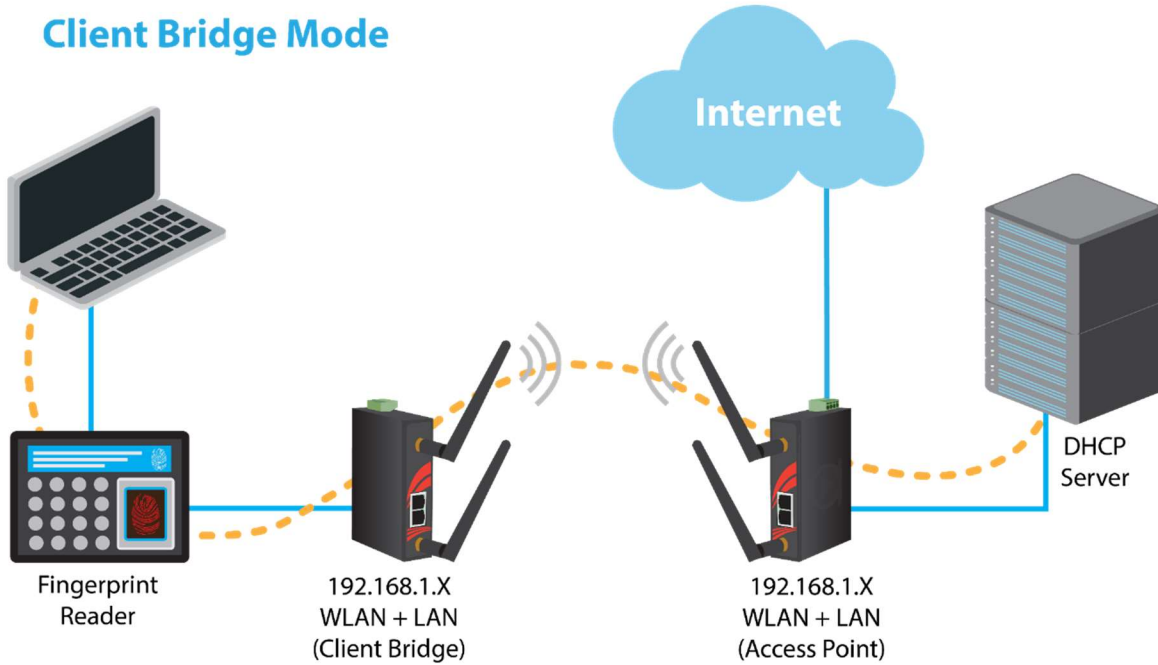
### 1.2.2 Client Mode

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



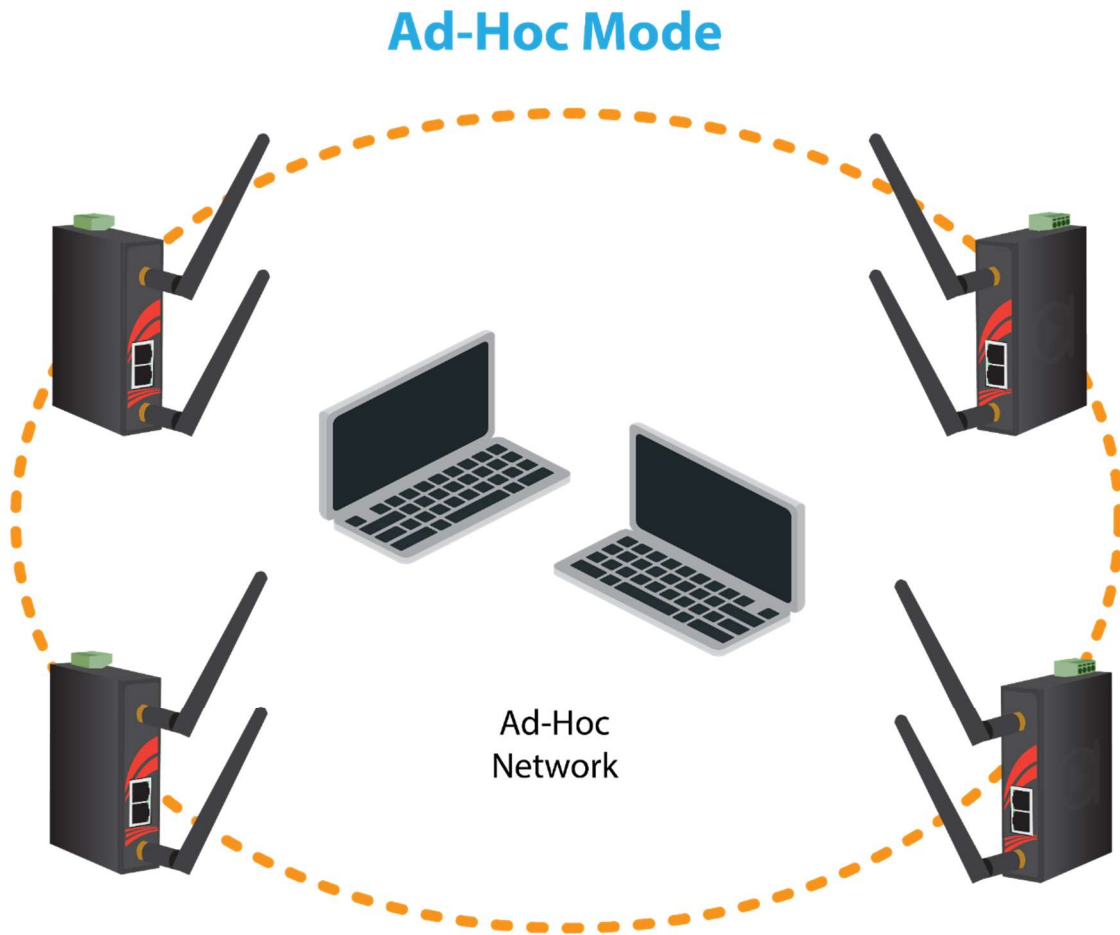
### 1.2.3 Client Bridge Mode

Client Bridge Mode is much like Client Mode, except the WLAN and LAN are on the same subnet. Consequently, NAT is no longer used and services such as DHCP will be able to work on the bridged network. Just as in client mode, the router will not accept wireless clients.



### 1.2.4 Ad Hoc Mode

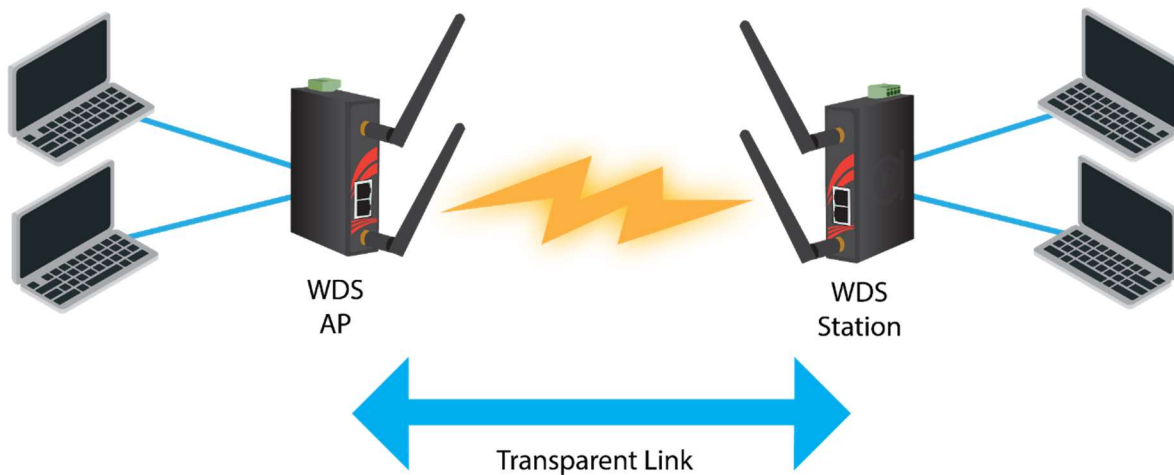
Ad Hoc Mode allows the router to connect to other wireless devices that are also in ad hoc configuration. Think of this mode as a Client Mode that does not connect to infrastructure networks, but rather to other ad hoc configured devices. Ad hoc networks lack the central management that is typical of infrastructure-type networks.



### 1.2.5 WDS Station/WDS Access Point

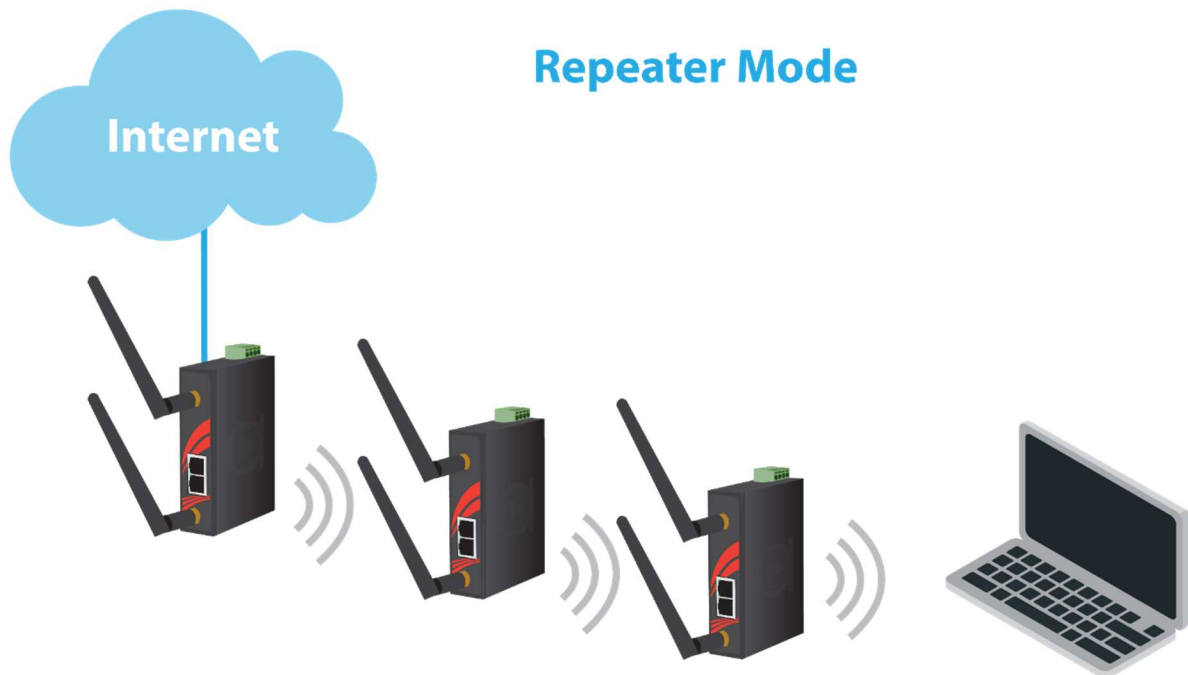
In a typical Access Point to Station/Client connection, whenever traffic is passed through the AP, the MAC address of the client packet changes to the MAC address of the AP. This can add overhead and latency. A Wireless Distribution System (WDS) allows one or more access points to connect wirelessly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

#### WDS AP/Client Mode



## 1.2.6 Repeater Mode

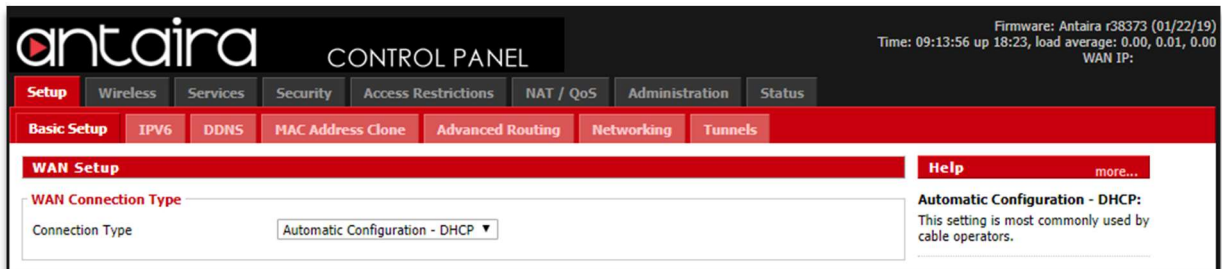
In Repeater Mode, the access point will act as a relay for another wireless signal. Repeater Mode takes an existing signal from a wireless AP or wireless router and rebroadcasts it. This mode is beneficial for extending the wireless range and coverage. The drawback is that the re-transmitted signal throughput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



## 2. Setup

### 2.1 Basic Setup

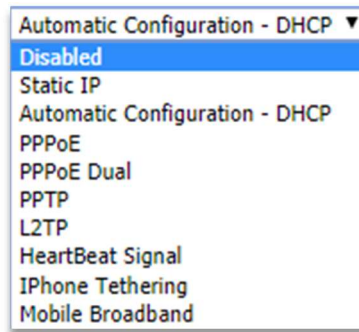
The Setup Screen is the first screen you will see when accessing the router. After you have configured and made changes to these settings, it is recommended to set a new password for the router. This will increase security by protecting the router from unauthorized changes. All users who try to access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



[Setup > Basic Setup](#)



## 2.1.1 WAN Setup



[Setup > Basic Setup > WAN Setup](#)

WAN Connection Type	Description
<b>Disabled</b>	Disable the WAN port.
<b>Static IP</b>	A static IP address is used. <b>Required:</b> IP address, subnet mask, gateway, and server to be entered manually.
<b>Automatic Configuration -DHCP</b>	The WAN port will obtain its IP address from a DHCP server.
<b>PPPoE</b>	Configure as PPPoE Client. <b>Required:</b> Username and Password. <b>Advanced Options:</b> Service Name, T-Online VLAN 7 Support, PPP Compression, MPPE Encryption, Single Line Multi Link, and Connection Strategy.
<b>PPPoE Dual</b>	Allows users to set multiple paths of the WAN.
<b>PPTP</b>	Establishes a connection via PPTP. <b>Required:</b> Gateway, Username, Password, and encryption information.
<b>L2TP</b>	Establishes a connection via L2TP. <b>Required:</b> Gateway, Username, Password, and encryption information.
<b>HeartBeat Signal</b>	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.
<b>iPhone Tethering</b>	Establishes a connection via iPhone tethering.
<b>Mobile Broadband</b>	Establishes a connection via mobile broadband.

## 2.1.2 Optional Settings

**Optional Settings**

Router Name

Hostname

Domain Name

MTU

Shortcut Forwarding Engine  Enable  Disable

STP  Enable  Disable

[Setup > Basic Setup > Optional Settings](#)

Optional Settings	Description
<b>Router Name</b>	The desired name to appear for the router.
<b>Hostname</b>	Necessary for some ISPs and can be provided by the ISP.
<b>Domain Name</b>	Necessary for some ISPs and can be provided by the ISP.
<b>MTU</b>	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.
<b>Shortcut Forwarding Engine</b>	Enable or disable this feature.
<b>STP</b>	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				
<b>Router IP</b>				
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)

**Network Address Server Settings (DHCP)**

DHCP Type: DHCP Server ▼

DHCP Server:  Enable  Disable

Start IP Address: 192.168.11. 100

Maximum DHCP Users: 50

Client Lease Time: 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 DHCP:

Use DNSMasq for DNS:

DHCP-Authoritative:

Recursive DNS Resolving (Unbound):

Forced DNS Redirection:

[Setup > Basic Setup > Network Address Server Settings](#)

Network Address Server Settings	Description
<b>DHCP Type</b>	<p><b>Server:</b> This device will function as the DHCP server. If there is already a DHCP server on the network, select <b>Disable</b>.</p> <p><b>Forwarder:</b> 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.</p>
<b>DHCP Server</b>	<p><b>Enable</b> if you want this router to provide DHCP addressing. Disable if there is an existing DHCP server on the network.</p>
<b>Start IP Address</b>	<p>A numerical value for the DHCP server to start its addressing with when assigning IP addresses. ****Do not start with the routers IP address. ****</p>
<b>Maximum DHCP Users</b>	<p>The maximum number of devices the router will assign</p>

	IP address through DHCP.
<b>Client Lease Time</b>	The lease time of an IP address given by the DHCP server before it expires.
<b>Static DNS #</b>	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.
<b>WINS</b>	Windows Internet Naming Services: Manages the PC's interaction with the internet.

### 2.1.5 Time Settings

**Time Settings**

NTP Client  Enable  Disable

Time Zone

Server IP/Name

Manual assign

[Setup > Basic Setup > Time Settings](#)

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

## 2.2 IPv6

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

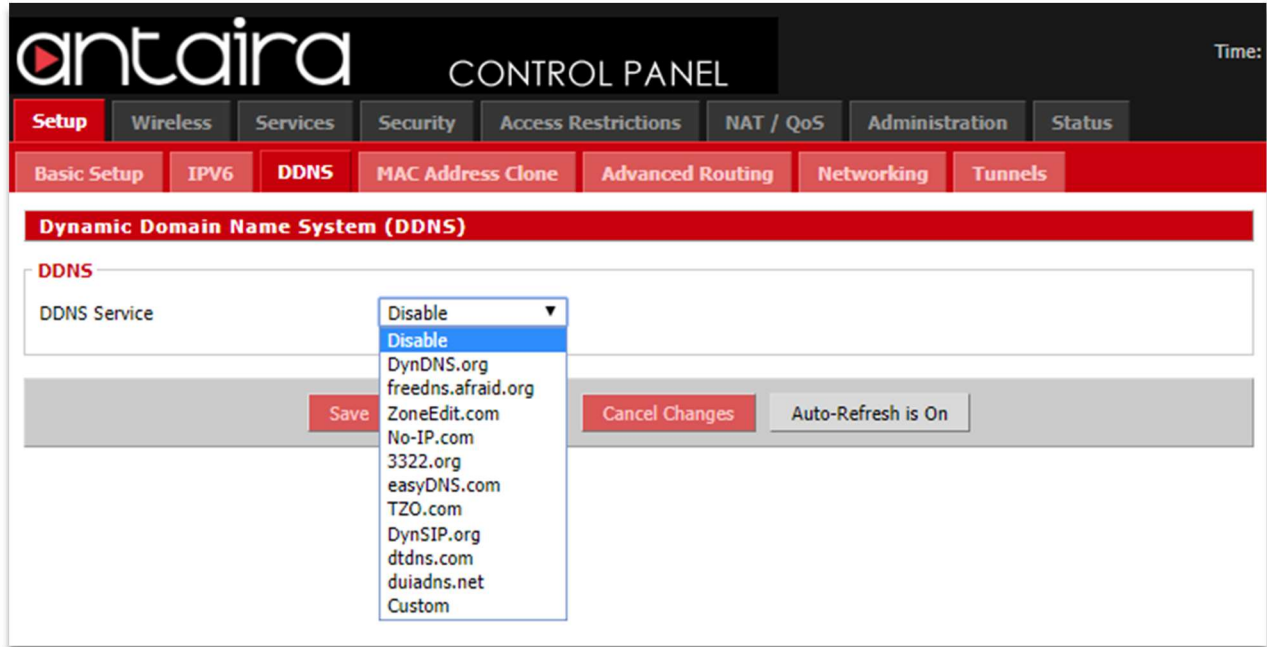
[Setup > IPv6](#)

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

<b>Dhcp6c custom</b>	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.
<b>Dhcp6s</b>	This option provides IPv6 addresses and prefix assignment administrative policy and configuration information for DHCPv6 clients.
<b>Radvd</b>	Linux IPv6 Router Advertisement Daemon
<b>Radvd custom</b>	Custom options for radvd configuration.

## 2.3 DDNS

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



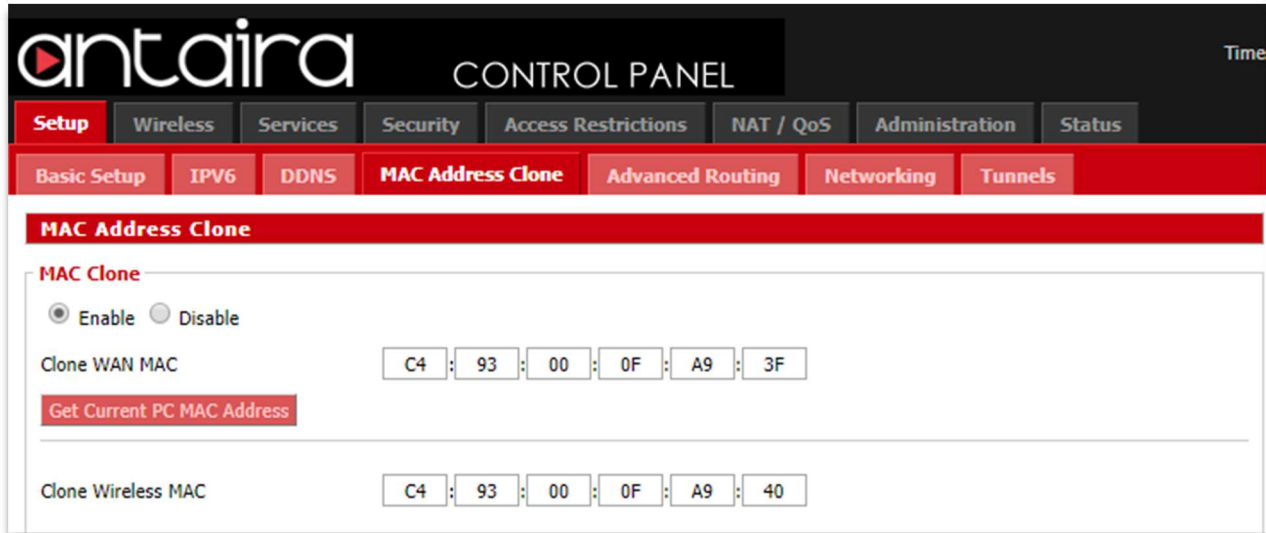
[Setup > DDNS](#)

DDNS Settings	Description
<b>DDNS Service</b>	Sign up for a DDNS service through a DDNS service provider.
<b>Username</b>	Setup a Username through the DDNS service provider.
<b>Password</b>	Setup a Password through the DDNS service provider.
<b>Hostname</b>	Setup a Hostname through the DDNS service provider.
<b>Type</b>	<b>Dynamic:</b> Allows a hostname (chosen by the user through the DDNS service provider) to point to the users IP address.
	<b>Static:</b> Like Dynamic service, but the DNS host will not expire after 35 days without updates.
	<b>Custom:</b> Creates a managed primary DNS that provides the user more control over the DNS.
<b>Wildcard</b>	Enabling the Wildcard feature allows the user's host to be aliased to the same IP address and the DNS server.
<b>External IP Check</b>	Allows the DDNS function to pick up the WAN IP from the router instead of checking on an external site.
<b>Force Update Interval</b>	The number represents how often (in days) an update will be performed.



## 2.4 MAC Address Clone

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

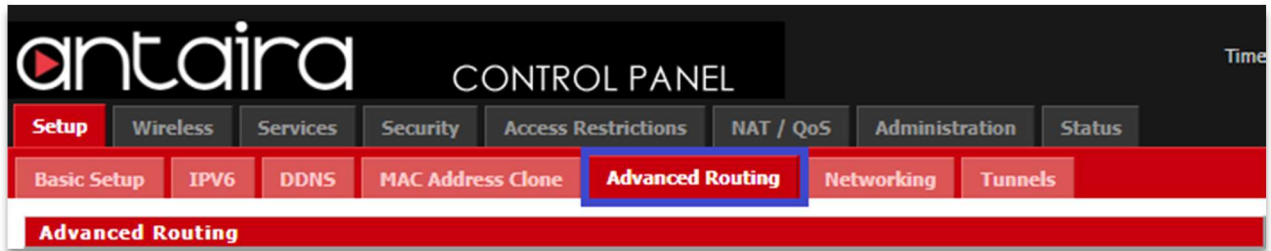


### [Setup > MAC Address Clone](#)

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

## 2.5 Advanced Routing

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



[Setup > Advanced Routing](#)

## 2.5.1 Gateway

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

The screenshot shows the Antaira Control Panel with the following configuration details:

- Operating Mode:** Gateway
- Dynamic Routing Interface:** Disable
- Static Routing:**
  - Select set number: 1 (Delete)
  - Route Name: (empty)
  - Metric: 0
  - Masquerade Route (NAT):
  - Destination LAN NET: 0.0.0.0
  - Subnet Mask: 0.0.0.0
  - Gateway: 0.0.0.0
  - Interface: LAN & WLAN

[Setup > Advanced Routing > Operating Mode > Gateway](#)

Gateway	Description
Operating Mode	<b>Gateway:</b> If the router is hosting the Internet connection, the router will perform NAT in Gateway mode.
	<b>BGP:</b> Boarder Gateway Protocol.
	<b>RIP2 Router:</b> Routing Information Protocol.
	<b>OSPF Router:</b> Open Shortest Path First.
	<b>OSPF &amp; RIP2 Router:</b> Uses a combination of RIP and OSPF.

	<b>OLSR Router:</b> Optimized Link State Routing Protocol.
	<b>Router:</b> Static routes.
<b>Dynamic Routing – Interface</b>	Tells the end user if the destination IP address is on the LAN & WAN, WAN or Loopback.
<b>Select Set Number</b>	A unique router number. You can set up to 50 routes.
<b>Route Name</b>	The name assigned to a specific route number.
<b>Metric</b>	Enter a metric number.
<b>Masquerade Route (NAT)</b>	Enable or disable masquerading (NAT).
<b>Destination LAN Net</b>	The remote host assigned to the static route.
<b>Subnet Mask</b>	Enter a subnet mask.
<b>Gateway</b>	Enter a gateway IP address.
<b>Interface</b>	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.

The screenshot shows the Antaira Control Panel interface. The top navigation bar includes 'Setup', 'Wireless', 'Services', 'Security', 'Access Restrictions', 'NAT / QoS', 'Administration', and 'Status'. Below this, a secondary navigation bar highlights 'Basic Setup', 'IPV6', 'DDNS', 'MAC Address Clone', 'Advanced Routing', 'Networking', and 'Tunnels'. The 'Advanced Routing' section is active and contains the following configuration options:

- Operating Mode:** A dropdown menu set to 'BGP'.
- BGP Settings:**
  - BGP Own AS#: An empty text input field.
  - Neighbor IP: Four individual input fields, each containing '0'.
  - Neighbor AS#: An empty text input field.
- Zebra Configuration:** Radio buttons for 'GUI' (unselected) and 'Vtysh' (selected).
- Static Routing:**
  - Select set number: A dropdown menu showing '1 ( )' and a 'Delete' button.
  - Route Name: An empty text input field.
  - Metric: An input field containing '0'.
  - Destination LAN NET: Four input fields, each containing '0'.
  - Subnet Mask: Four input fields, each containing '0'.
  - Gateway: Four input fields, each containing '0'.
  - Interface: A dropdown menu set to 'LAN & WLAN'.

A 'Show Routing Table' button is located at the bottom right of the Static Routing section.

[Setup > Advanced Routing > Operating Mode > BGP](#)

BGP	Description
BGP Own AS#	Autonomous System Number.

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

[Setup > Advanced Routing > Operating Mode > RIP2 Router](#)

RIP2 Router	Description
<b>RIP2 Config Style</b>	Sets the configuration style for RIP2.
<b>Zebra Config Style</b>	Sets the Zebra configuration style.
<b>Select Set Number</b>	Select the Route set (1-64).
<b>Route Name</b>	Give the route a name.
<b>Metric</b>	An integer giving weight to the cost of the route.
<b>Destination LAN NET</b>	Network address of destination LAN.

<b>Subnet Mask</b>	Subnet mask of destination LAN.
<b>Gateway</b>	Gateway IP address.
<b>Interface</b>	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.



[Setup > Advanced Routing > Operating Mode > OSPF Router](#)

OSPF Router	Description
<b>OSPF Config Style</b>	Sets the configuration style for OSPF.
<b>Zebra Config Style</b>	Sets the Zebra configuration style.
<b>Select Set Number</b>	Select the Route set (1-64).
<b>Route Name</b>	Give the route a name.
<b>Metric</b>	An integer giving weight to the cost of the route.
<b>Destination LAN NET</b>	Network address of destination LAN.
<b>Subnet Mask</b>	Subnet mask of destination LAN.
<b>Gateway</b>	Gateway IP address.
<b>Interface</b>	Select the interface for the path of the route.

## 2.5.5 OSPF & RIP2 Router

**antaira CONTROL PANEL**

Time

**Setup** | Wireless | Services | Security | Access Restrictions | NAT / QoS | Administration | Status

Basic Setup | IPV6 | DDNS | MAC Address Clone | **Advanced Routing** | Networking | Tunnels

**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

**Static Routing**

Select set number: 1 ( ) ▼

Route Name:

Metric:

Destination LAN NET:  .  .  .

Subnet Mask:  .  .  .

Gateway:  .  .  .

Interface: LAN & WLAN ▼

[Setup > Advanced Routing > Operating Mode > OSPF & RIP2 Router](#)

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

<b>Destination LAN NET</b>	Network address of destination LAN.
<b>Subnet Mask</b>	Subnet mask of destination LAN.
<b>Gateway</b>	Gateway IP address.
<b>Interface</b>	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.

**antaira** CONTROL PANEL Time

**Setup** | Wireless | Services | Security | Access Restrictions | NAT / QoS | Administration | Status

Basic Setup | IPV6 | DDNS | MAC Address Clone | **Advanced Routing** | Networking | Tunnels

---

**Advanced Routing**

**Operating Mode**

Operating Mode:

---

**OLSR Routing (Optimized Link State Routing)**

Gateway Mode:  Enable  Disable

Host Net Announce:

Poll Rate:

TC Redundancy:

MPR Coverage:

Link Quality Fish Eye:  Enable  Disable

Link Quality Aging:

Smart Gateway:  Enable  Disable

Link Quality Level:

Hysteresis:  Enable  Disable

New Interface:

---

**Static Routing**

Select set number:

Route Name:

Metric:

Destination LAN NET:

Subnet Mask:

Gateway:

Interface:

[Setup > Advanced Routing > Operating Mode > OLSR Router](#)

<b>OLSR Router</b>	<b>Description</b>
<b>Gateway Mode</b>	Enable or disable feature.
<b>Host Net Announce</b>	Enter a host net announce.
<b>Poll Rate</b>	Set the poll rate interval.
<b>TC Redundancy</b>	Set the TC Redundancy.
<b>MPR Coverage</b>	Set the MPR Coverage.
<b>Link Quality Fish Eye</b>	Enable or disable this feature.
<b>Link Quality Aging</b>	Set the link quality aging.
<b>Smart Gateway</b>	Enable or disable this feature.
<b>Link Quality Level</b>	Set the link quality level.
<b>Hysteresis</b>	Enable or disable this feature.
<b>New Interface</b>	Add a new interface.
<b>Select Set Number</b>	Select the Route set (1-64).
<b>Route Name</b>	Give the route a name.
<b>Metric</b>	An integer giving weight to the cost of the route.
<b>Destination LAN NET</b>	Network address of destination LAN.
<b>Subnet Mask</b>	Subnet mask of destination LAN.
<b>Gateway</b>	Gateway IP address.
<b>Interface</b>	Select the interface for the path of the route.

## 2.5.7 Router

Router Mode allows users to set static routes.

The screenshot shows the Antaira Control Panel interface. At the top, there's a navigation bar with tabs for Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, Administration, and Status. Below this is a sub-navigation bar with tabs for Basic Setup, IPV6, DDNS, MAC Address Clone, Advanced Routing (selected), Networking, and Tunnels. The main content area is titled 'Advanced Routing' and contains two sections: 'Operating Mode' with a dropdown menu set to 'Router', and 'Static Routing' with several input fields: 'Select set number' (1), 'Route Name' (empty), 'Metric' (0), 'Destination LAN NET' (0.0.0.0), 'Subnet Mask' (0.0.0.0), 'Gateway' (0.0.0.0), and 'Interface' (LAN & WLAN). A 'Delete' button is next to the set number, and a 'Show Routing Table' button is at the bottom right of the static routing section.

[Setup > Advanced Routing > Operating Mode > Router](#)

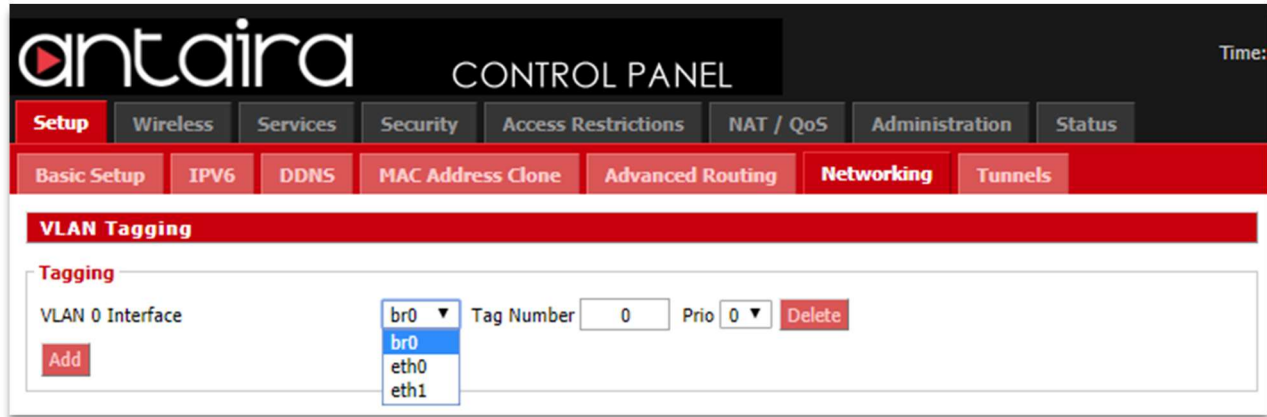
Router	Description
<b>Select Set Number</b>	This is the unique router number. You may set up to 50 routes.
<b>Route Name</b>	Enter the name you would like to assign to this route.
<b>Metric</b>	
<b>Destination LAN NET</b>	This is the remote host to which you would like to assign the static route.
<b>Subnet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

## 2.6 Networking

### 2.6.1 VLAN Tagging

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

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



[Setup > Networking > VLAN Tagging](#)

## 2.6.2 Bridging

Bridging

**Create Bridge**

Name	STP	IGMP Snooping	Prio	MTU	Root MAC	
br0	Off ▼	Off ▼	32768 ▼	1500	04:F0:21:41:AF:AE	Delete

Add

**Assign to Bridge**

Assignment	Interface	STP	Prio	Path Cost	Hairpin Mode	
none ▼	eth0 ▼	Off ▼	128 ▼	100	<input type="checkbox"/>	Delete

Add

**Current Bridging Table**

Bridge Name	STP	Interface
br0	no	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
<b>Add</b>	Create a new network bridge.
<b>STP</b>	Spanning Tree Protocol. Turn on or off.
<b>IGMP Snooping</b>	Turn on or off IGMP Snooping.
<b>Prio</b>	Sets the bridge priority order. (Lower numbers are higher priority.)
<b>MTU</b>	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.
<b>Root MAC</b>	The Root MAC address.

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

Assign to Bridge	Description
<b>Assignment</b>	Assign any valid interface to a network bridge.
<b>Interface</b>	Select the interface to assign to the bridge.
<b>STP</b>	Spanning Tree Protocol. Turn on or off.
<b>Prio</b>	Sets the priority order (Lower numbers are higher priority).



<b>Path Cost</b>	Set the path cost.
<b>Hairpin Mode</b>	Enables Hairpin routing.

### 2.6.3 IP Virtual Server

[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

[Setup > Networking > Create Virtual Server](#)

Create Virtual Server	Description
<b>Server Name</b>	Enter a server name.
<b>Source IP</b>	Enter a source IP address.
<b>Source Port</b>	Enter a source port.
<b>Protocol</b>	Choose between TCP, UDP, or SIP protocol.
<b>Scheduler</b>	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
<b>WAN Port Assignment</b>	Select a WAN Port.
<b>MAC Address</b>	MAC Address of the configured WAN port.
<b>Label</b>	Input a label if desired.
<b>TX Queue Length</b>	Set the TX-queue length.
<b>Bridge Assignment</b>	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  Max  Leasetime  Delete

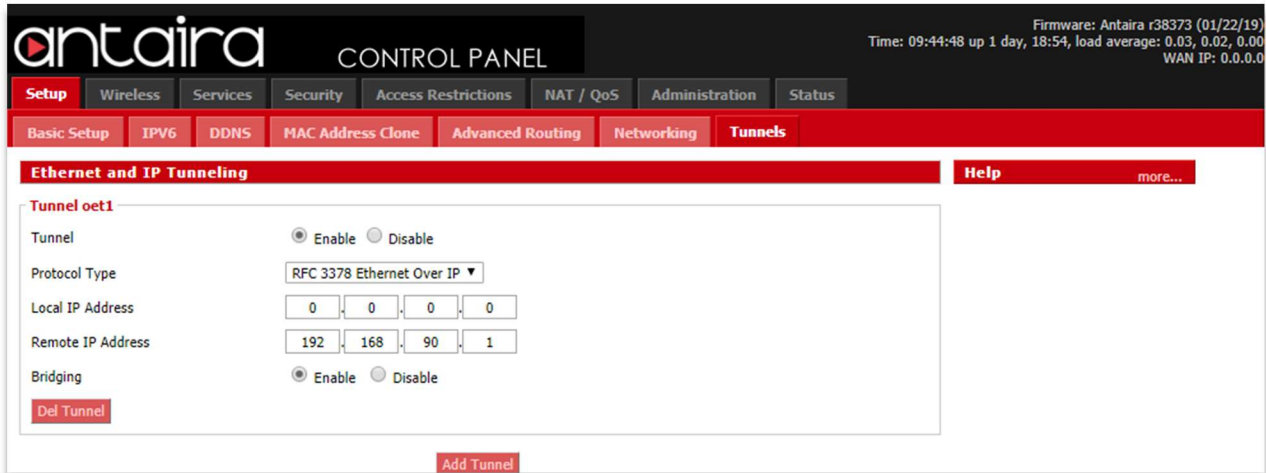
Add

[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.



[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

Del Tunnel

[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 ▼

Local Port  

Generate Key

Local Public Key  

Add Peer

IP Address 1 . 2 . 3 . 4

Subnet Mask 255 . 255 . 255 . 255

Del Tunnel

[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.

## 3. Wireless

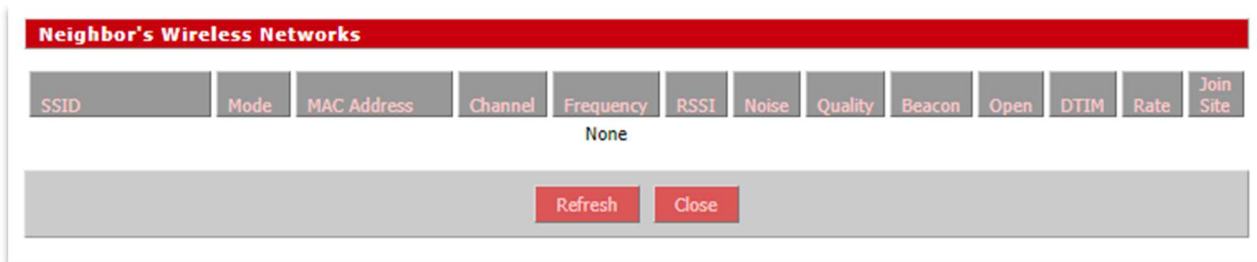
### 3.1 Basic Settings

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

#### 3.1.1 Wireless Site Survey

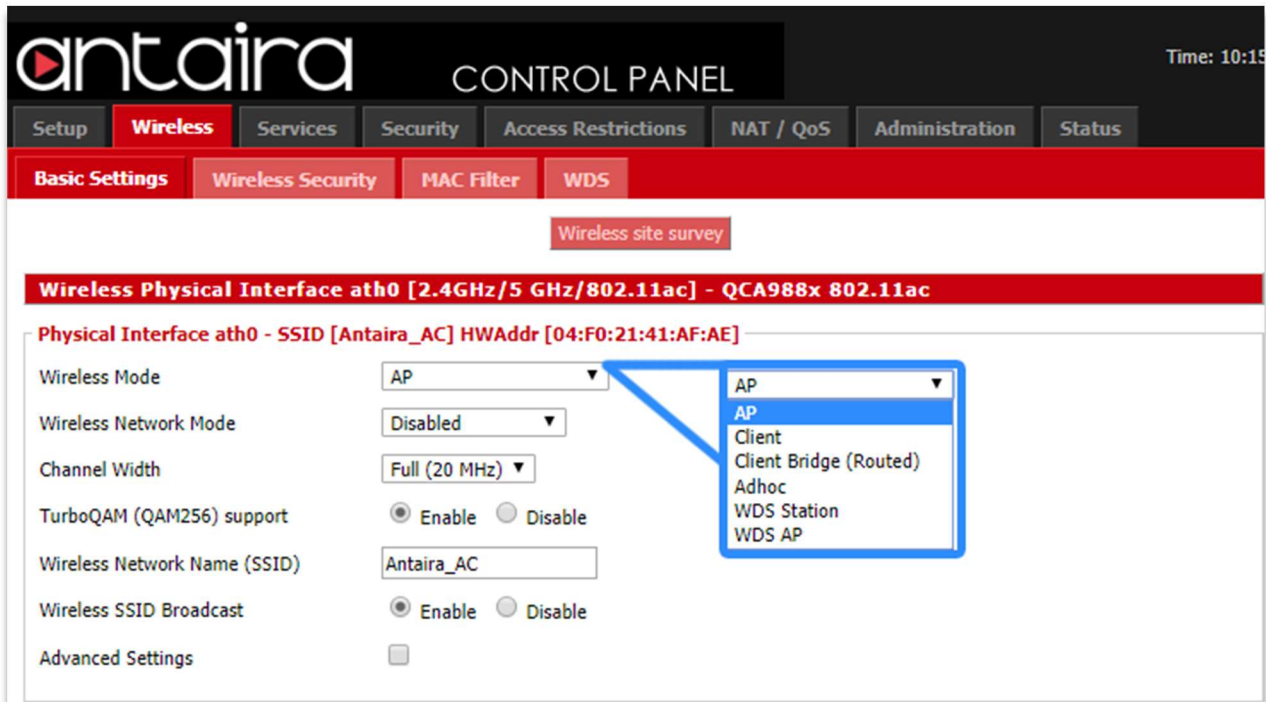


#### [Wireless > Basic Settings](#)



#### [Wireless > Basic Settings > Wireless Site Survey](#)

### 3.1.2 Wireless Mode



[Wireless > Basic Settings > Wireless Mode](#)

Basic Settings	Description
<b>Wireless Mode</b>	<b>AP:</b> The default settings. Access Point Mode will allow the router to act as a connection point for wireless client devices to connect with.
	<b>Client:</b> The radio interface is used to connect the Internet-facing side of the router (the WAN) as a client to a remote access point. NAT or routing are performed between WAN and LAN. Use this mode if your Internet connection is provided by a remote access point and you want to attach a subnet of your own to it.
	<b>Client Bridge (Routed):</b> The radio interface is used to connect the LAN side of the router to an access point. The LAN and access point will be in the same subnet (bridging two network segments). The WAN side of the router is unused and can be disabled. Use this mode to make the router act as a WLAN adapter for a device connected to one of its LAN Ethernet ports.
	<b>Adhoc:</b> A point-to-point communication that does not use access points. Devices in Adhoc Mode communicate directly with each other.

	<p><b>WDS Station:</b> Used to connect with a WDS AP. WDS Station functions like a Client, but multiple layer 2 devices can be connected to the WDS Station device.</p>
	<p><b>WDS AP:</b> Functions as an access point that only WDS Station devices can connect to.</p>

### 3.1.3 Wireless Network Mode

[Wireless > Basic Settings > Wireless Network Mode](#)

Basic Settings	Description
<b>Wireless Network Mode</b>	<b>Disabled:</b> Disables the wireless network mode.
	<b>Mixed:</b> If you have mixed b/g/n devices on your network.
	<b>B-Only:</b> IEEE 802.11b allows a maximum data rate of 11Mbps/s through 2.4GHz wireless connections. If only B-type wireless devices are on the network, use this mode.
	<b>G-Only:</b> IEEE 802.11g allows a maximum data rate of

54Mbps/s through 2.4GHz wireless connections. If only G-type wireless devices are on the network, use this mode.
<b>BG-Mixed:</b> If B and G-type wireless devices are on the network, use this mode.
<b>A-Only:</b> IEEE 802.11a allows a maximum data rate of 54Mbps/s through 5GHz wireless connections. If only A-type devices are on the network, use this mode.
<b>NG-Mixed:</b> Mix band of 802.11b/g/b modes.
<b>N-Only (2.4GHz):</b> N-Only wireless network mode.
<b>NA-Mixed:</b> Mix band of 802.11n/a modes.
<b>N-Only (5GHz):</b> Improved throughput for 5GHz devices.
<b>AC/N-Mixed:</b> Mix band of 802.11ac/n modes.
<b>AC-Only:</b> AC-Only wireless network mode.

### 3.1.4 Channel Width

The screenshot shows the 'Wireless Physical Interface ath0 [2.4GHz/5 GHz/802.11ac] - QCA988x 802.11ac' configuration page. The 'Channel Width' dropdown menu is expanded, showing the following options: Full (20 MHz), Full (20 MHz), Dynamic (20/40 MHz), Wide HT40 (40 MHz), and VHT80 (80 MHz). The 'Full (20 MHz)' option is currently selected.

[Wireless > Basic Settings > Channel Width](#)



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

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

### 3.1.5 Wireless Network Name (SSID)

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

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

### 3.1.6 Advanced Settings

By selecting the *Advanced Settings* box, the following options will become available.

Advanced Settings	<input checked="" type="checkbox"/>	
Regulatory Domain	UNITED_STATES	
TX Power	20	dBm
Antenna Gain	0	dBi
Noise Immunity	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Protection Mode	None	
RTS Threshold	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Short Preamble	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Short GI	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
TX Antenna Chains	1+2	
RX Antenna Chains	1+2	
AP Isolation	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Beacon Interval	100	
DTIM Interval	2	
Airtime Fairness	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Frame Compression	Disabled	
WMM Support	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Radar Detection	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
ScanList	default	
Sensitivity Range (ACK Timing)	2000	(Default: 2000 meters)
Max Associated Clients	256	(Default: 256 Clients)
<b>Drop Clients with Low Signal</b>		
Minimum Signal for authenticate	-128	
Minimum Signal for connection	-128	
Poll Time for signal lookup	10	
Amount of allowed low signals	3	
Network Configuration	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Bridged

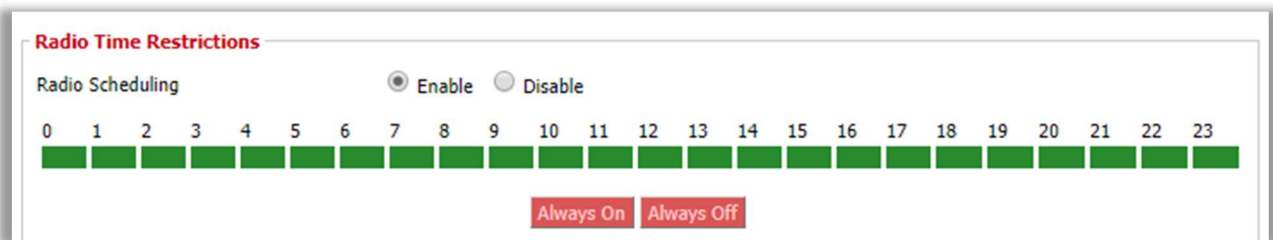
[Wireless > Basic Settings > Advanced Settings](#)

Basic Settings	Description
<b>Regulatory Domain</b>	Select a regulatory domain from the drop-down menu.
<b>TX Power</b>	Enter a value for the transmit power is dBm.
<b>Antenna Gain</b>	The antenna's ability to direct radio frequency energy.

<b>Noise Immunity</b>	Enable or disable this feature.
<b>Protection Mode</b>	CTS (Clear to Send) protection allows multiple client devices to send data simultaneously to a single access point. The CTS protection is able to set an order of what device gets to transmit, preventing the access point from discarding packets.
<b>RTS Threshold</b>	Specifies the maximum size for a packet before data is fragmented into multiple packets.
<b>Short Preamble</b>	Default is Long Preamble. A short preamble can be used but communication issues might occur when communicating with IEEE 802.11b devices.
<b>Short GI</b>	Enable or disable this feature.
<b>TX Antenna Chains</b>	Used based on external antennas to provide optimum performance.
<b>RX Antenna Chains</b>	Used based on external antennas to provide optimum performance.
<b>AP Isolation</b>	Disabled by default. If enabled, wireless clients are isolated and access to and from other wireless clients is stopped.
<b>Beacon Interval</b>	Set the beacon interval.
<b>DTIM Interval</b>	Set the STIM interval.
<b>Airtime Fairness</b>	Enable or disable this feature.
<b>Frame Compression</b>	Enable or disable this feature.
<b>WMM Support</b>	Enable or disable this feature.
<b>Radar Detection</b>	Looks for airport or military pulses from radars to prevent unintended interference between equipment.
<b>ScanList</b>	
<b>Sensitivity Range (ACK Timing)</b>	Default is 2000 meters. The sensitivity range is a timing adjustment based on the distance between linking devices. When the time needed to transmit is greater than the amount of time sender waits before resending the same packet. Typically, the ACK time should be 2 times the distance between devices (measured in meters). If the ACK time is too low, information can be lost. 0 disables ACK timing completely.
<b>Max Associated Clients</b>	Number of clients that can be connected to the access point.
<b>Minimum Signal for Authenticate</b>	Set the minimum signal for authentication.
<b>Minimum Signal for</b>	Set the minimum signal for connection.

<b>Connection</b>	
<b>Poll Time for Signal Lookup</b>	Set the poll time for signal lookup.
<b>Amount of Allowed Low Signals</b>	Set the amount of allowed low signals.
<b>Network Configuration</b>	<b>Bridged</b> shares the wireless interface and LAN port (same network). <b>Unbridged</b> allows the separation between the Wireless interface and LAN.

### 3.1.7 Radio Time Restrictions



[Wireless > Basic Settings > Radio Time Restrictions](#)

### 3.1.8 Virtual Interfaces

**Virtual Interfaces**

**Virtual Interfaces ath0.1 SSID [antaira\_vap]**

Wireless Mode AP ▼

Wireless Network Name (SSID) antaira\_vap

Wireless SSID Broadcast  Enable  Disable

Advanced Settings

[Wireless > Basic Settings > Virtual Interfaces](#)

Basic Settings	Description
<b>Wireless Mode</b>	Choose between Access Point or WDS Access Point for the wireless mode of the virtual interface.
<b>Wireless Network Name (SSID)</b>	Enter a SSID for the virtual interface.
<b>Wireless SSID Broadcast</b>	Enable or disable broadcasting of the SSID.

### 3.1.9 Advanced Settings

Advanced Settings

Protection Mode None ▼

RTS Threshold  Enable  Disable

Frame Compression Disabled ▼

WMM Support  Enable  Disable

AP Isolation  Enable  Disable

Max Associated Clients 256 (Default: 256 User)

DTIM Interval 2

**Drop Clients with Low Signal**

Minimum Signal for authenticate -128

Minimum Signal for connection -128

Poll Time for signal lookup 10

Amount of allowed low signals 3

[Wireless > Basic Settings > Virtual Interfaces > Advanced Settings](#)

Basic Settings	Description
Protection Mode	Choose between None, CTS, RTS/CTS
RTS Threshold	Specifies the maximum size for a packet before data is fragmented into multiple packets.
Frame Compression	Enable or disable this feature.
WMM Support	Enable or disable this feature.
AP Isolation	Disabled by default. If enabled, wireless clients are isolated and access to and from other wireless clients is stopped.
Max Associated Clients	Number of clients that can be connected to the access point. Default max is 256 users.
DTIM Interval	Set the DTIM interval.
Minimum Signal for Authenticate	Set the minimum signal for authentication.
Minimum Signal for Connection	Set the minimum signal for connections.
Poll Time for Signal Lookup	Set the poll time for signal lookup.
Amount of Allowed Low Signals	Set the amount of allowed low signals.

### 3.1.10 Network Configuration

Network Configuration  Unbridged  Bridged

Multicast forwarding  Enable  Disable

Masquerade / NAT  Enable  Disable

Net Isolation  Enable  Disable

Forced DNS Redirection  Enable  Disable

IP Address

Subnet Mask

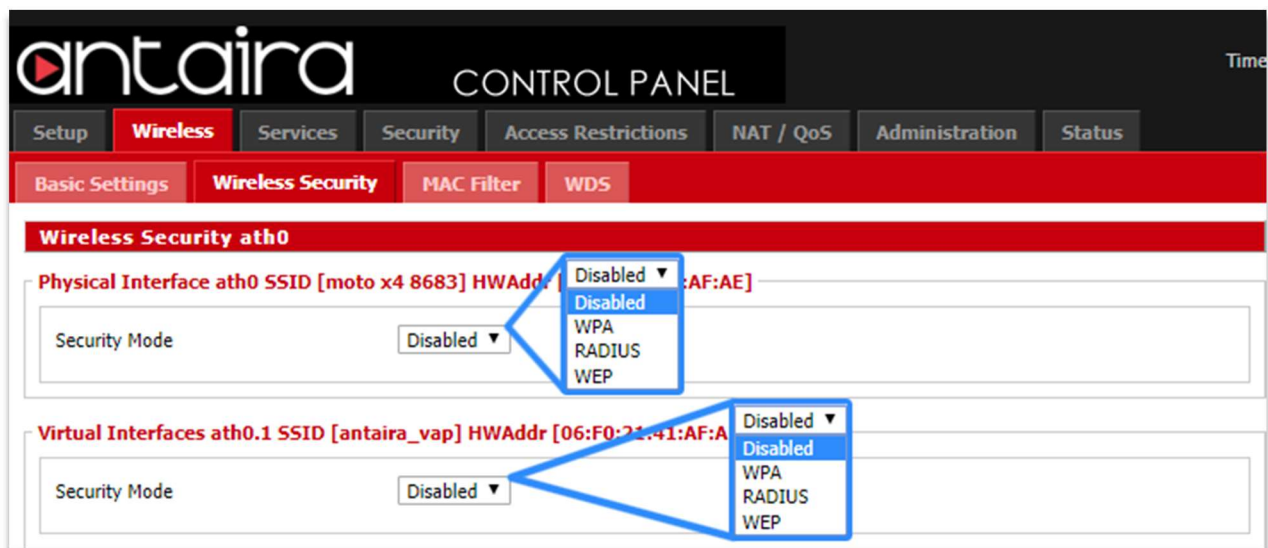
[Wireless > Basic Settings > Virtual Interfaces > Advanced Settings > Network Configuration](#)

Basic Settings	Description
Network Configuration	<b>Bridged</b> shares the Wireless interface and LAN port (same network). <b>Unbridged</b> allows the separation between the Wireless interface and LAN.

<b>Multicast Forwarding</b>	Enable or disable Multicast forwarding.
<b>Masquerade/NAT</b>	Enable or disable NAT.
<b>Net Isolation</b>	Enable or disable Net Isolation.
<b>Forced DNS Redirection</b>	Enable or disable Forced-DNS-Redirection.
<b>IP Address</b>	Enter an IP Address.
<b>Subnet Mask</b>	Enter a Subnet Mask.

### 3.2 Wireless Security

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



[Wireless > Wireless Security > Security Mode](#)

Wireless Security	Description
<b>Security Mode</b>	<b>Disabled:</b> Uses no wireless security.
	<b>WPA:</b> Uses WPA for wireless security. Additional options and settings will appear when selected.
	<b>RADIUS:</b> Uses RADIUS for wireless security. Additional options and settings will appear when selected.
	<b>WEP:</b> Uses WEP for wireless security. Additional options and settings will appear when selected.

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

### 3.2.1 WPA

The screenshot shows the Antaira Control Panel interface. The top navigation bar includes 'Setup', 'Wireless', 'Services', 'Security', 'Access Restrictions', 'NAT / QoS', 'Administration', and 'Status'. Below this, there are sub-tabs for 'Basic Settings', 'Wireless Security', 'MAC Filter', and 'WDS'. The main content area is titled 'Wireless Security ath0' and 'Virtual Interfaces ath0.1'. Each section has a 'Physical Interface ath0 SSID [moto x4 8683] HWAddr [04:F0:21:41:AF:AE]' and 'Virtual Interfaces ath0.1 SSID [antaira\_vap] HWAddr [06:F0:21:41:AF:AE]' header. Under each header, there is a 'Security Mode' dropdown menu set to 'WPA'. Below the dropdown are two columns of options: 'Network Authentication' and 'WPA Algorithms'. The 'Network Authentication' column includes: WPA Personal, WPA2 Personal, WPA2 Personal with SHA256, WPA3 Personal, WPA Enterprise, WPA2 Enterprise, WPA2 Enterprise with SHA256, and WPA3 Enterprise. The 'WPA Algorithms' column includes: CCMP-128 (AES) and TKIP. All options are currently unchecked.

[Wireless > Wireless Security > Security Mode > WPA](#)



Wireless Security	Description
<b>Network Authentication</b>	Choose the network authentication method.

### WPA Algorithms

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

### 3.2.2 RADIUS

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

The screenshot shows the 'Wireless Security ath0' configuration page. The 'Security Mode' is set to 'RADIUS'. The 'MAC Format' is 'aabbcc-ddeeff'. The 'Radius Auth Server Address' is '0.0.0.0'. The 'Radius Auth Server Port' is '1812'. The 'Radius Auth Shared Secret' field is empty with an 'Unmask' checkbox. The 'Force Client IP' is '0.0.0.0'.

[Wireless > Wireless Security > Security Mode > RADIUS](#)

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

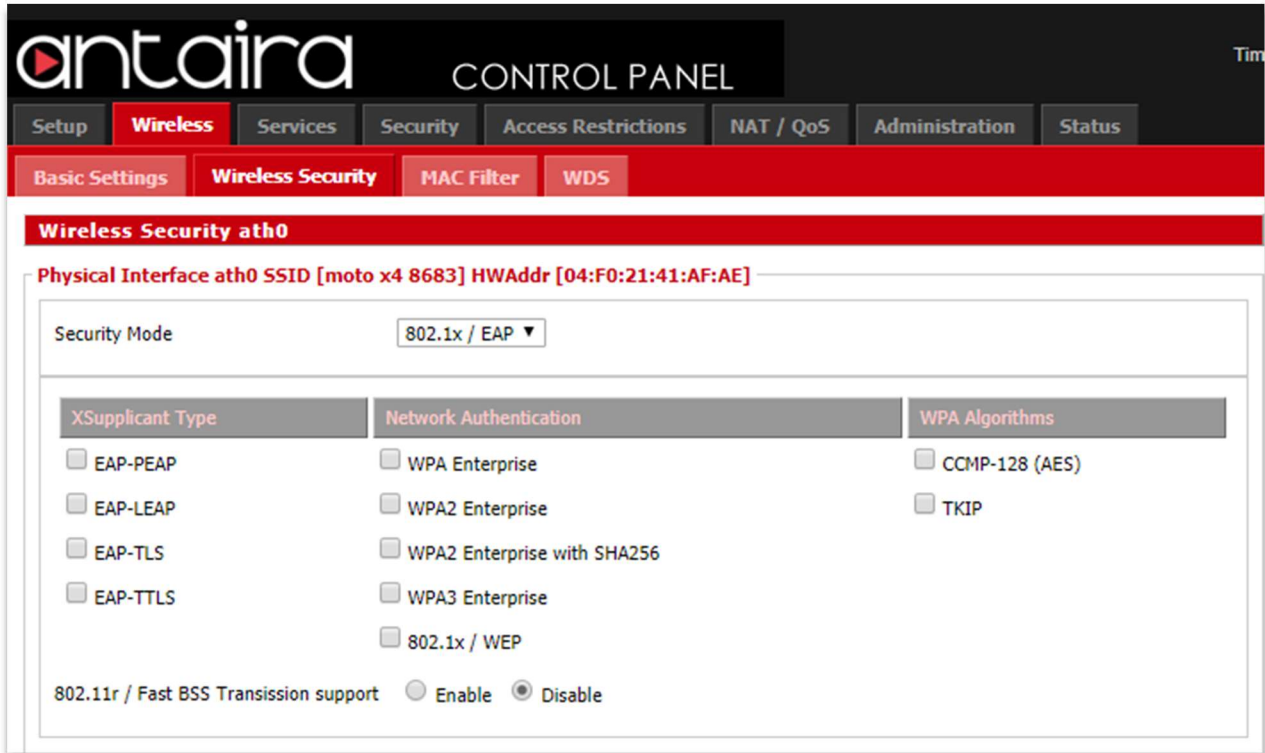
### 3.2.3 WEP

The screenshot shows the 'Wireless Security ath0' configuration page. At the top, the 'Wireless' tab is selected. Below it, the 'Wireless Security' sub-tab is active. The configuration for 'Physical Interface ath0 SSID [moto x4 8683] HWAddr [04:F0:21:41:AF:AE]' is shown. The 'Security Mode' is set to 'WEP'. Under 'Authentication Type', 'Open' is selected. 'Default Transmit Key' is set to '1'. 'Encryption' is set to '64 bits 10 hex digits'. There is a 'Passphrase' field with a 'Generate' button. Below are four 'Key' input fields (Key 1 through Key 4).

[Wireless > Wireless Security > Security Mode > WEP](#)

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

### 3.2.4 802.1x/EAP

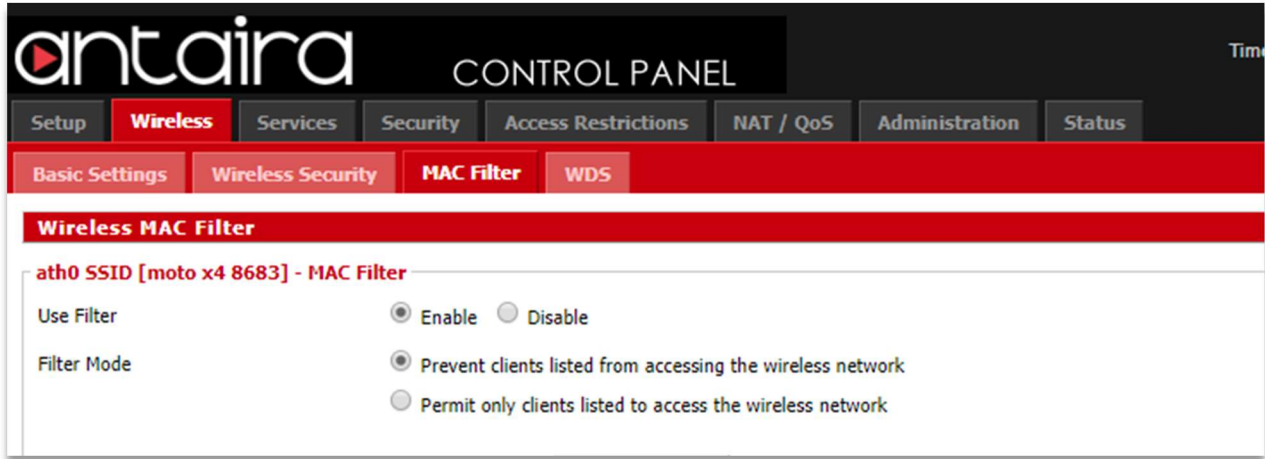


[Wireless > Wireless Security > Security Mode > 802.1x/EAP](#)

Wireless Security	Description
<b>XSupplicant Type</b>	Select a XSupplicant type: EAP-PEAP, EAP-LEAP, EAP-TLS, EAP-TTLS.
<b>Network Authentication</b>	Select a Network Authentication method: WPA Enterprise, WPA2 Enterprise, WPA2 Enterprise with SHA256, WPA3 Enterprise, 802.1x/WEP.
<b>WPA Algorithms</b>	Select a WPA Algorithm: CCMP-128(AES), TKIP.
<b>802.11r/Fast BSS Transmission Support</b>	Enable or disable 802.11r/Fast BSS Transmission Support.

### 3.3 MAC Filter

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



[Wireless > MAC Filter](#)

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

### 3.3.1 Edit MAC Filter List

**MAC Address Filter List**

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

Wireless Client MAC List

Table 1		Table 2	
MAC 001 :	<input type="text"/>	MAC 065 :	<input type="text"/>
MAC 002 :	<input type="text"/>	MAC 066 :	<input type="text"/>
MAC 003 :	<input type="text"/>	MAC 067 :	<input type="text"/>
MAC 004 :	<input type="text"/>	MAC 068 :	<input type="text"/>
MAC 005 :	<input type="text"/>	MAC 069 :	<input type="text"/>
MAC 006 :	<input type="text"/>	MAC 070 :	<input type="text"/>
MAC 007 :	<input type="text"/>	MAC 071 :	<input type="text"/>
MAC 008 :	<input type="text"/>	MAC 072 :	<input type="text"/>
MAC 009 :	<input type="text"/>	MAC 073 :	<input type="text"/>
MAC 010 :	<input type="text"/>	MAC 074 :	<input type="text"/>
MAC 011 :	<input type="text"/>	MAC 075 :	<input type="text"/>
MAC 012 :	<input type="text"/>	MAC 076 :	<input type="text"/>
MAC 013 :	<input type="text"/>	MAC 077 :	<input type="text"/>
MAC 014 :	<input type="text"/>	MAC 078 :	<input type="text"/>
MAC 015 :	<input type="text"/>	MAC 079 :	<input type="text"/>
MAC 016 :	<input type="text"/>	MAC 080 :	<input type="text"/>
MAC 017 :	<input type="text"/>	MAC 081 :	<input type="text"/>
MAC 018 :	<input type="text"/>	MAC 082 :	<input type="text"/>
MAC 019 :	<input type="text"/>	MAC 083 :	<input type="text"/>
MAC 020 :	<input type="text"/>	MAC 084 :	<input type="text"/>
MAC 021 :	<input type="text"/>	MAC 085 :	<input type="text"/>
MAC 022 :	<input type="text"/>	MAC 086 :	<input type="text"/>
MAC 023 :	<input type="text"/>	MAC 087 :	<input type="text"/>
		MAC 129 :	<input type="text"/>
		MAC 130 :	<input type="text"/>
		MAC 131 :	<input type="text"/>
		MAC 132 :	<input type="text"/>
		MAC 133 :	<input type="text"/>
		MAC 134 :	<input type="text"/>
		MAC 135 :	<input type="text"/>
		MAC 136 :	<input type="text"/>
		MAC 137 :	<input type="text"/>
		MAC 138 :	<input type="text"/>
		MAC 139 :	<input type="text"/>
		MAC 140 :	<input type="text"/>
		MAC 141 :	<input type="text"/>
		MAC 142 :	<input type="text"/>
		MAC 143 :	<input type="text"/>
		MAC 144 :	<input type="text"/>
		MAC 145 :	<input type="text"/>
		MAC 146 :	<input type="text"/>
		MAC 147 :	<input type="text"/>
		MAC 148 :	<input type="text"/>
		MAC 149 :	<input type="text"/>
		MAC 150 :	<input type="text"/>
		MAC 151 :	<input type="text"/>
		MAC 193 :	<input type="text"/>
		MAC 194 :	<input type="text"/>
		MAC 195 :	<input type="text"/>
		MAC 196 :	<input type="text"/>
		MAC 197 :	<input type="text"/>
		MAC 198 :	<input type="text"/>
		MAC 199 :	<input type="text"/>
		MAC 200 :	<input type="text"/>
		MAC 201 :	<input type="text"/>
		MAC 202 :	<input type="text"/>
		MAC 203 :	<input type="text"/>
		MAC 204 :	<input type="text"/>
		MAC 205 :	<input type="text"/>
		MAC 206 :	<input type="text"/>
		MAC 207 :	<input type="text"/>
		MAC 208 :	<input type="text"/>
		MAC 209 :	<input type="text"/>
		MAC 210 :	<input type="text"/>
		MAC 211 :	<input type="text"/>
		MAC 212 :	<input type="text"/>
		MAC 213 :	<input type="text"/>
		MAC 214 :	<input type="text"/>
		MAC 215 :	<input type="text"/>

[Wireless > MAC Filter > Edit MAC Filter List](#)

### 3.4 WDS

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

**antaira CONTROL PANEL** Time: 14:38

Setup **Wireless** Services Security Access Restrictions NAT / QoS Administration Status

Basic Settings Wireless Security MAC Filter **WDS**

**Wireless Distribution System**

**WDS Settings**

Wireless MAC 04:F0:21:41:AF:AE

Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	
Disable	00	:	00	:	00	:	00	:	00	:	00	:	00	

**Extra Options**

Lazy WDS  Enable  Disable (Default: Disable)

WDS Subnet  Enable  Disable

NAT Disable

IP Address 0 0 0 0

Subnet Mask 255 255 255 0

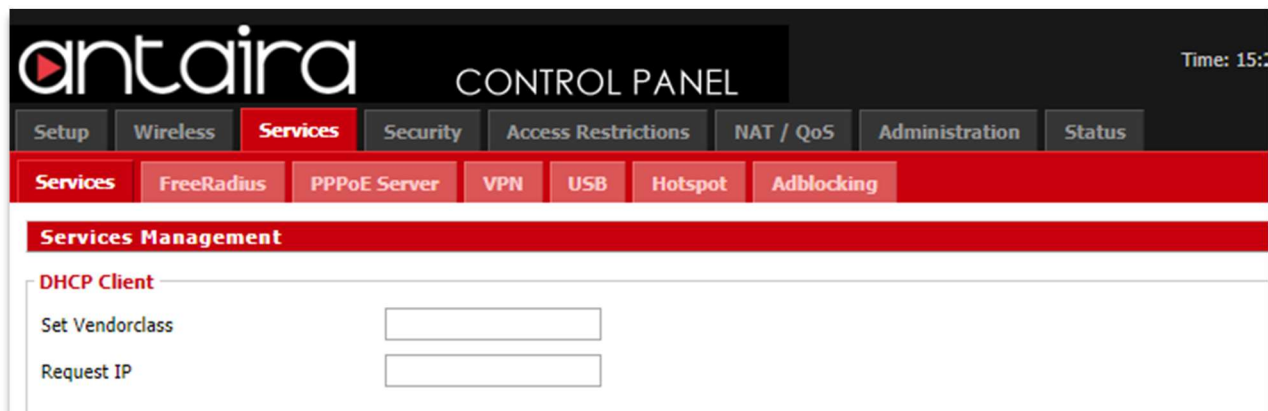
[Wireless > WDS](#)

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

## 4. Services

### 4.1 Services

#### 4.1.1 DHCP Client



[Services > Services > DHCP Client](#)

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**

Use JFFS2 for client lease DB *(Not mounted)*

Use NVRAM for client lease DB

Used Domain WAN ▼

LAN Domain

Additional DHCPd Options

---

**Static Leases**

MAC Address	Hostname	IP Address	Client Lease Time
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 50%;" type="text"/> min
<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 100%;" type="text"/>	<input style="width: 50%;" type="text"/> min

[Services > Services > DHCP Server](#)

DHCP Server	Description
<b>Use NVRAM for Client Lease DB</b>	Enable or disable this feature.
<b>Used Domain</b>	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.
<b>LAN Domain</b>	Define your local LAN domain here. This is used as the local domain for dnsmasq and DHCP service if chosen above.
<b>Additional DHCPd Options</b>	Enter any additional DHCPd options here.
<b>Static Leases</b>	If you want to assign certain hosts a specific address then you can define them here. This is also the way to add hosts with a fixed address to the router's local DNS service (dnsmasq).

### 4.1.3 Dnsmasq

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

**Dnsmasq**

Dnsmasq  Enable  Disable

Encrypt DNS  Enable  Disable

DNSCrypt Resolver

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.

<b>Additional Dnsmasq Options</b>	Enter any additional options here.
-----------------------------------	------------------------------------

#### 4.1.4 Lighttpd Webserver

**Lighttpd Webserver**

**Lighttpd**

Lighttpd  Enable  Disable

HTTPS Port

HTTP Port

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.

#### 4.1.5 Mikrotik MAC Telnet

**Mikrotik MAC Telnet**

MAC Telnet  Enable  Disable

Password

[Services > Services > Mikrotik MAC Telnet](#)

### 4.1.6 PPPoE Relay

**PPPoE Relay**

Relay  Enable  Disable

[Services > Services > PPPoE Relay](#)

### 4.1.7 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](#)

### 4.1.8 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

Port  (Default: 2055)

MACupd  Enable  Disable

Server IP

Port  (Default: 2056)

Interface

Interval (in seconds)

[Services > Services > RFlow/MACupd](#)

RFlow/MACupd	Description
RFlow	Enable or disable this feature.

<b>Server IP</b>	Enter the Server IP address.
<b>Port</b>	Enter a port number. Default is port 2055.
<b>MACUpd</b>	Enable or disable MACUpd.
<b>Server IP</b>	Enter the server IP address.
<b>Port</b>	Enter a port number. Default is port 2056.
<b>Interface</b>	Select an interface.
<b>Interval</b>	Set the interval in seconds.

### 4.1.9 SNMP

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



[Services > Services > SNMP](#)

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

### 4.1.10 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  (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 <i>root</i> ).
Port	Change the SSH port. Default is port 22.
Authorized Keys	Enter authorized keys is applicable.

### 4.1.11 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.

<b>Klogd</b>	Enable or disable Klogd.
<b>Remote Server</b>	Enter the remote server IP address to receive syslogs.

### 4.1.12 Telnet

Enable or disable Telnet.

**Telnet**

Telnet  Enable  Disable

[Services > Services > Telnet](#)

### 4.1.13 The Onion Router Project

**The Onion Router Project**

Tor  Enable  Disable

DNS Name or External IP

Nickname / ID

Bandwidth Rate  KB/s

Bandwidth Burst  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
<b>Tor</b>	Enable or disable this feature.
<b>DNS Name or External IP</b>	Enter the DNS name or external IP address.
<b>Nickname/ID</b>	Enter a nickname/ID.
<b>Bandwidth Rate</b>	Set the bandwidth rate.
<b>Bandwidth Burst</b>	Set the bandwidth burst.
<b>Relay Mode</b>	Enable or disable this feature.
<b>Directory Mirror</b>	Enable or disable this feature.

<b>Tor Bridge Mode</b>	Enable or disable this feature.
<b>Transparent Proxy</b>	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 widely deployed RADIUS. FreeRADIUS can be used to authenticate WLAN clients using WPA/WPA2 Enterprise.

The screenshot shows the Antaira Control Panel interface for configuring FreeRadius. The top navigation bar includes 'Setup', 'Wireless', 'Services', 'Security', 'Access Restrictions', 'NAT / QoS', 'Administration', and 'Status'. The 'Services' menu is expanded to show 'FreeRadius', 'PPPoE Server', 'VPN', 'USB', 'Hotspot', and 'Adblocking'. The 'FreeRadius' section is active and contains the following configuration options:

- FreeRadius:** A radio button selection for 'Enable' (selected) and 'Disable'.
- Server Certificate:** Fields for 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, with a default of 365), and Passphrase (none). A 'Gen Cert' button is located below these fields.
- Certificate Status:** A progress indicator showing 'generating 0%, this may take a long time'.
- Settings:** A field for Radius Port (1812, with a default of 1812).
- Clients:** A table with columns for IP/NET, Shared key, and an 'Add' button.
- Users:** A table with columns for Username, Password, Downspeed, Upspeed, Expires (Days), and Enabled, with an 'Add' button.

[Services > FreeRadius](#)

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

**antaira CONTROL PANEL**

Setup | Wireless | **Services** | Security | Access Restrictions | NAT / QoS | Administration | Status

Services | FreeRadius | **PPPoE Server** | VPN | USB | Hotspot | Adblocking

**PPPoE Server**

**PPPoE Server**

RP-PPPoE Server Daemon  Enable  Disable

**RP-PPPoE Server Options**

RP-PPPoE 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
		0.0.0.0	<input type="checkbox"/>

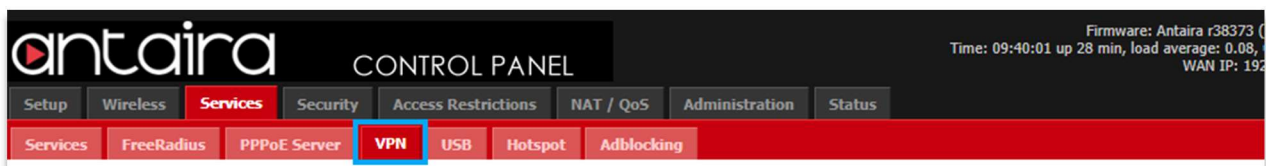
Add Remove

[Services > PPPoE Server](#)

PPPoE Server	Description
<b>RP-PPPoE Server Daemon</b>	Enable or disable this feature.
<b>RP-PPPoE Server Interface</b>	Select the interface.
<b>IP Range</b>	Set the IP range.
<b>Max Associated Clients</b>	Set the maximum associated clients allowed.
<b>Deflate Compression</b>	Enable or disable this feature.
<b>BSD Compression</b>	Enable or disable this feature.
<b>LZS Stac Compression</b>	Enable or disable this feature.
<b>MPPC Compression</b>	Enable or disable this feature.
<b>MPPE Encryption</b>	Enable or disable this feature.
<b>Session Limit per MAC</b>	Set a session limit per MAC address. Default is 0.
<b>LCP Echo Interval</b>	Set the LCP Echo Interval. Default is 5.
<b>LCP Echo Failure</b>	Set the LCP Echo Failure. Default is 12.
<b>Client Idle Time</b>	
<b>MTU/MRU</b>	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.
<b>Authentication</b>	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.



[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).

[Services > VPN > PPTP Server](#)

PPTP Server	Description
PPTP Server	Enable or disable PPTP Server option.
Broadcast Support	When <b>Disabled</b> , PPTP-Server does set <i>proxy-arp</i> which works for broadcasting in most cases. When <b>Enabled</b> ,

	<i>bcrelay</i> will relay all broadcast messages to the default bridge network. This will increase cpu load. Disabled by default.
<b>MPPE Encryption</b>	Forces clients to use encryption with 128bit. When encryption is disabled, encryption to clients is allowed, but not forced.
<b>DNS1 &amp; 2</b>	Add your local/WAN DNS Server. Setting DNS2 is optional.
<b>WINS1 &amp; 2</b>	Add your local WINS server. This setting is optional.
<b>MTU/MRU</b>	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.
<b>Server IP</b>	Enter a LAN IP Address ( <i>An IP from your network that is not used by any device or the router</i> ). Example: ( <i>Assuming the router's LAN address is 192.168.1.1</i> ) Server IP = 192.168.1.2. The default port for pptp is 1723.
<b>Client IP(s)</b>	The client IP range. Leaving it blank will not work. ( <i>Input in format like: 192.168.1.100-199</i> ). 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.
<b>Max Associated Clients</b>	Max allowed concurrent clients.
<b>Authentication</b>	RADIUS or CHAP Secrets.

## 4.4.2 PPTP Client

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

[Services > VPN > PPTP Client](#)

PPTP Client	Description
<b>PPTP Client Options</b>	Enable or disable PPTP Client options.
<b>Server IP or DNS Name</b>	The IP address of the VPN server.
<b>Remote Subnet</b>	Use the Network Address for the Remote Network ( <i>10.20.1.0 for example</i> ).
<b>Remote Subnet Mask</b>	Use the Subnet Mask appropriate for the Remote Network ( <i>255.255.255.0 for example</i> ).
<b>MPPE Encryption</b>	The type of security to use for the connection. If you are connecting to another router, you need ( <i>Example: mppe required</i> ). But if you are connecting to a Windows VPN server you need ( <i>Example: mppe required, no40, no56, stateless</i> ) or ( <i>Example: mppe required, no40, no56, stateful</i> ).
<b>MTU/MRU</b>	Needs to match the server's MTU/MRU settings.
<b>NAT</b>	Recommended to leave enabled.

<b>Username</b>	Your Remote PPTP Network Domain/Username. (Example: YOURCOMPANY\johndoe)
<b>Password</b>	Your Remote PPTP Network Password.
<b>Additional PPTP Options</b>	Additional options for PPTP connections.

### 4.4.3 OpenVPN Server

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

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

Netmask

Port  (Default: 1194)

Tunnel Protocol  (Default: UDP)

Encryption Cipher

Hash Algorithm

Advanced Options  Enable  Disable

Public Server Cert

CA Cert

Private Server Key

DH PEM

Additional Config

TLS Auth Key

Certificate Revoke List



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. <b>TUN</b> : Routing (layer 3) <b>TAP</b> : Bridging networks (Layer 2, can be used for routing, but not common)
Network	Network to use for the tunnel (Only in routing mode).
Netmask	Netmask of the network for the tunnel.
Port	The port which OpenVPN server listens on. Default is port 1194.
Tunnel Protocol	The sub-protocol the connection will use. Default is UDP.
Encryption Cipher	The encryption algorithm that will be used for the tunnel. Blowfish: fastest to AES512: safest.
Hash Algorithm	The hash algorithm that will be used. MD4: fastest to SHA512.
Advanced Options	Refer to the Advanced Options table below.
Public Server Cert	Server certificate issued by CA for this particular router (usually server.crt). Only part between 'BEGIN' and 'END' is required.
CA Cert	Certificate of OpenVPN CA in pem form (usually ca.crt). Only part between (and including) -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- is necessary.
Private Server Key	Key associated with Public Server Cert (usually server.key). This should be kept secret as anyone with this key can successfully authenticate client certificates.
DH PEM	Diffie Hellman parameters generated for the OpenVPN server (usually dh1024.pem).
Additional Config	Any additional configurations you want to define for the VPN connection.
TLS Auth Key	The static key OpenVPN should use for generating HMAC send/receive Keys.
Certificate Revoke List	Enter certificates to be revoked, if desired.

<b>Advanced Options (Server Side)</b>	<b>Description</b>
<b>TLS Cipher</b>	What encryption algorithm OpenVPN should use for encrypting its control channel. Default is disabled.
<b>LZO Compression</b>	Enables compression over VPN. This may speed up the connection.
<b>Redirect Default Gateway</b>	Force the clients to use the tunnel as the default gateway. Default is disabled.
<b>Allow Client to Client</b>	Allows clients to see each other. Default is disabled.
<b>Allow Duplicate cn</b>	Allow the use of one client certification for multiple clients. (This poses a security risk of sharing certifications). Default is disabled.
<b>Tunnel MTU Setting</b>	Set the mtu of the tunnel. Default is 1500.
<b>Tunnel UDP Fragment</b>	Set mss-fix and fragmentation across the tunnel.
<b>Tunnel UDP MSS-Fix</b>	Equal to value of Fragment. Only used with udp. Should be set on one side of the connection only.
<b>CCD-Dir DEFAULT File</b>	Enter CCD-dir default file here.
<b>Client Connect Script</b>	Enter a client connect script here.
<b>Static Key</b>	Enter the static key here.
<b>PKCS12 Key</b>	Used for peer-to-peer links. No pki needed.

### 4.4.4 OpenVPN Client

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

OpenVPN Client

**OpenVPN Client**

Start OpenVPN Client  Enable  Disable

Server IP/Name

Port  (Default: 1194)

Tunnel Device  ▼

Tunnel Protocol  ▼

Encryption Cipher  ▼

Hash Algorithm  ▼

User Pass Authentication  Enable  Disable

Advanced Options  Enable  Disable

CA Cert

Public Client Cert

Private Client Key

[Services > VPN > OpenVPN Client](#)

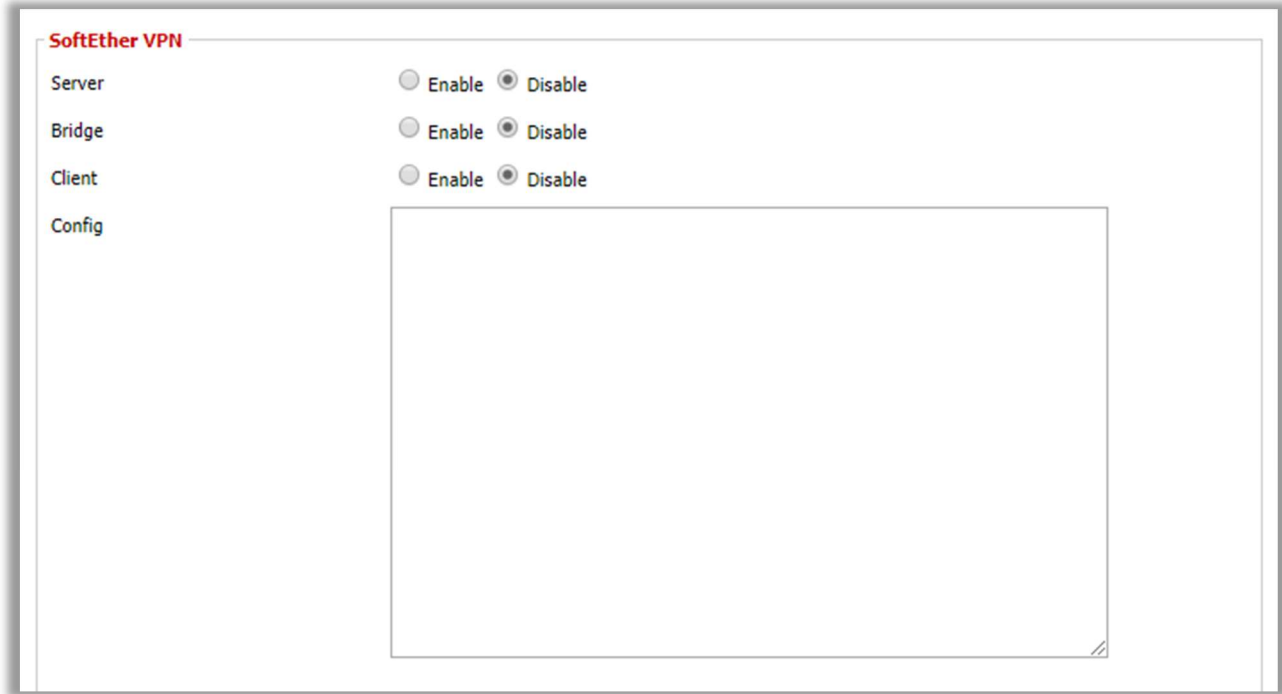
OpenVPN	Description
<b>Start OpenVPN Client</b>	Enable or disable OpenVPN client options.
<b>Server IP/Name</b>	IP address/hostname of the OpenVPN server you wish to connect to.
<b>Port</b>	The port which OpenVPN server is listening on. Default is port 1194.
<b>Tunnel Device</b>	The mode of tunneling. <b>TUN:</b> Routing (layer 3). <b>TAP:</b> Bridging (layer 2, can be used for routing, but not common).
<b>Tunnel Protocol</b>	The sub-protocol the connection will use. Default is UDP.
<b>Encryption Cipher</b>	The encryption algorithm that will be used for the tunnel. Blowfish is fastest, while AES512 is safest.
<b>Hash Algorithm</b>	The hash algorithm that will be used. MD4: fastest to

	SHA512.
<b>User Pass Authentication</b>	Enable or Disable this feature.
<b>Advanced Options</b>	Refer to the Advanced Options table below.
<b>CA Cert</b>	CA certificate. Only part between 'BEGIN' and 'END' is required.
<b>Public Client Cert</b>	Client certificate issued by CA.
<b>Private Client Key</b>	Key associated with the Public Client Cert. This should be kept secret because anyone with this key can successfully authenticate as this client.

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

## 4.4.5 SoftEther VPN

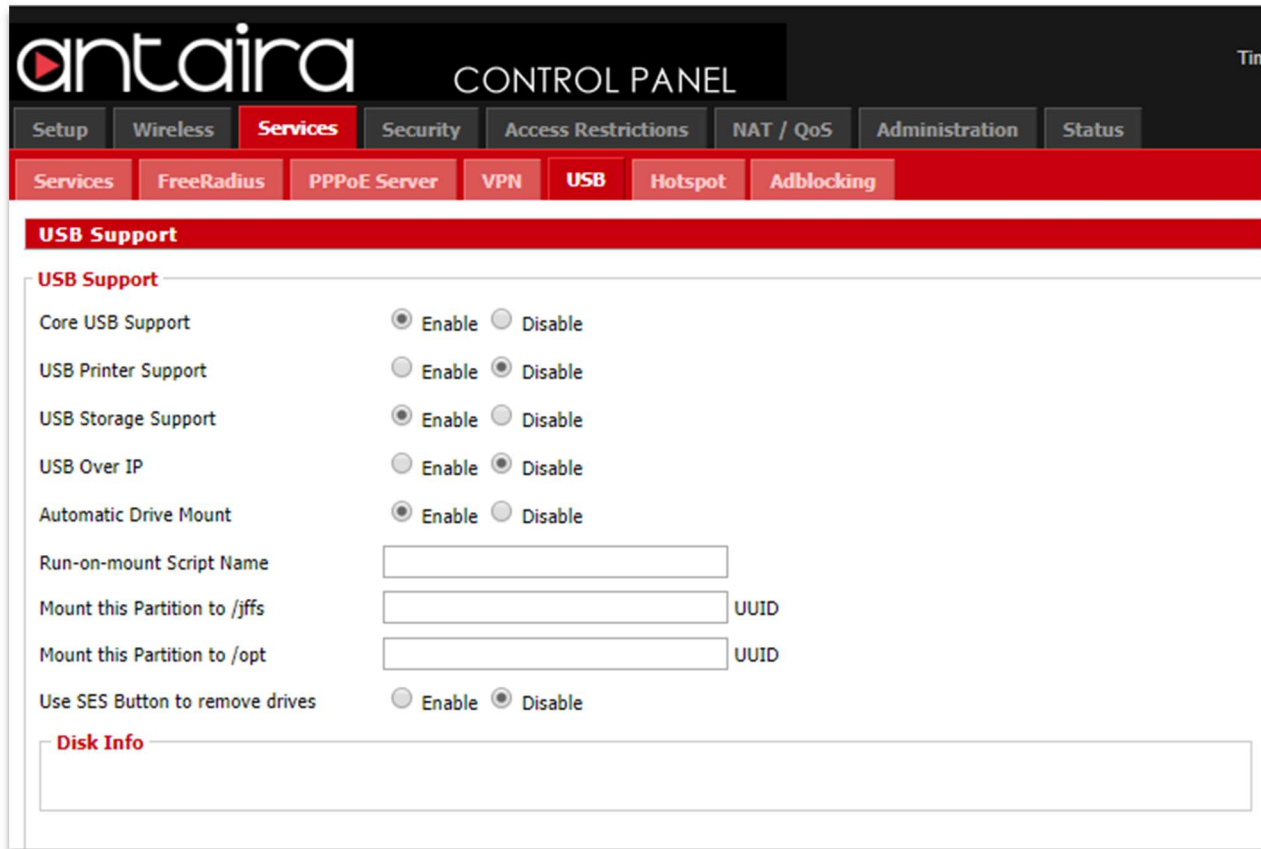
An alternative VPN service to OpenVPN.



The screenshot shows a web-based configuration page for SoftEther VPN. The page title is "SoftEther VPN". On the left side, there is a vertical menu with four items: "Server", "Bridge", "Client", and "Config". To the right of the menu, there are three rows of radio button controls. Each row has two radio buttons: "Enable" and "Disable". The "Disable" radio button is selected for all three rows: "Server", "Bridge", and "Client". Below these controls is a large, empty rectangular box with a thin border and a small diagonal line in the bottom right corner, likely intended for additional configuration or notes.

[Services > VPN > SoftEther VPN](#)

## 4.5 USB



### [Services > USB](#)

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

## 4.6 Hotspot


**antaira CONTROL PANEL** Tim

Setup | Wireless | **Services** | Security | Access Restrictions | NAT / QoS | Administration | Status

Services | FreeRadius | PPPoE Server | VPN | USB | **Hotspot** | Adblocking


### Hotspot Portal

**Hotspot System**



Hotspot System  Enable  Disable

**WiFiDog**



WiFiDog Gateway  Enable  Disable

**ChilliSpot**

ChilliSpot  Enable  Disable

**ChilliSpot Local User Management**

User List
Username   Password

**HTTP Redirect**

HTTP Redirect  Enable  Disable

**NoCatSplash**

NoCatSplash  Enable  Disable

**Zero IP Config**

Zero IP Config enabled  Enable  Disable

Range

**SMTP Redirect**

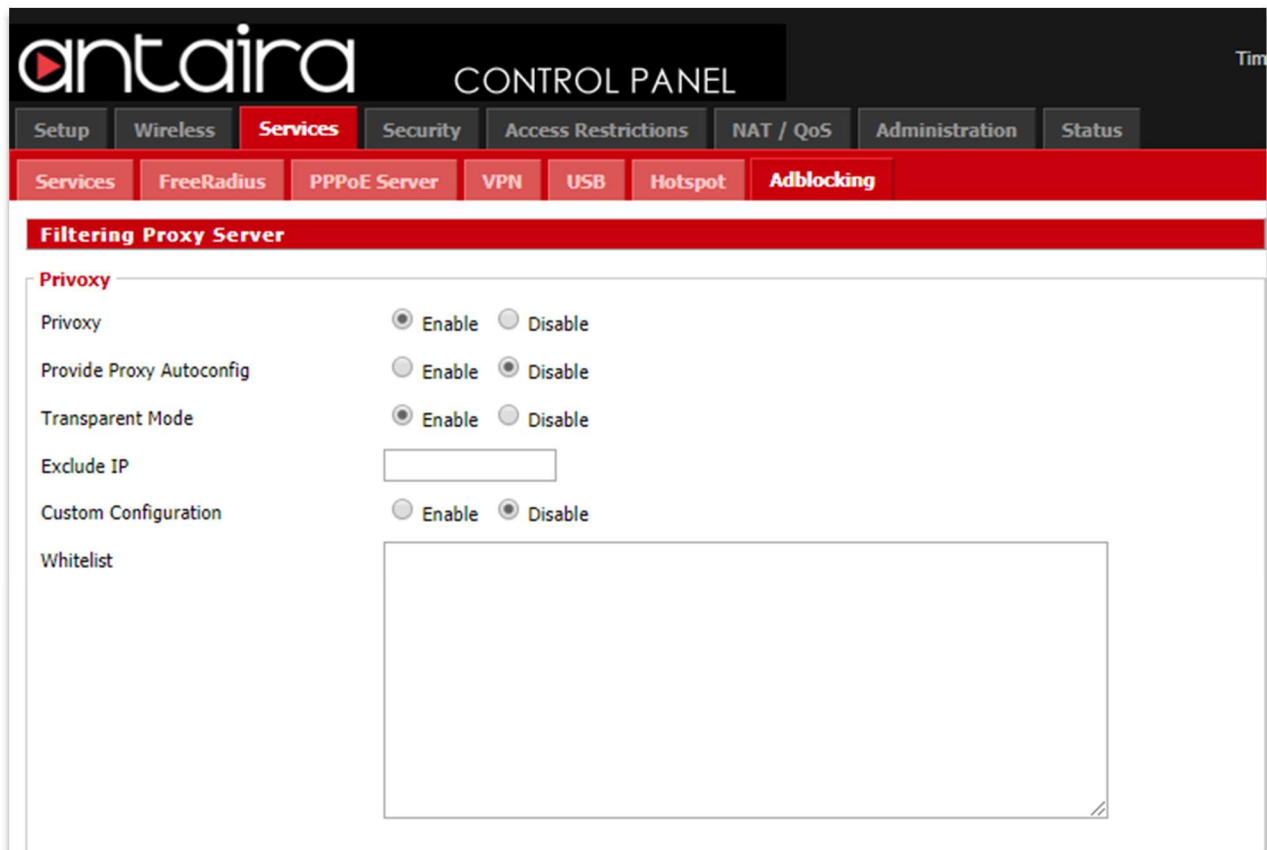
SMTP Redirect  Enable  Disable

[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.



### [Services > Adblocking](#)

Adblocking	Description
<b>Privoxy</b>	Enables you to filter common ads.
<b>Provide Proxy Autoconfig</b>	Publishes a WPAD/PAC file that clients use to automatically setup proxy details.
<b>Transparent Mode</b>	Traffic to port 80 is intercepted by Privoxy even if the client did not configure any proxy settings, thus allowing you to enforce filtering. Transparent mode cannot



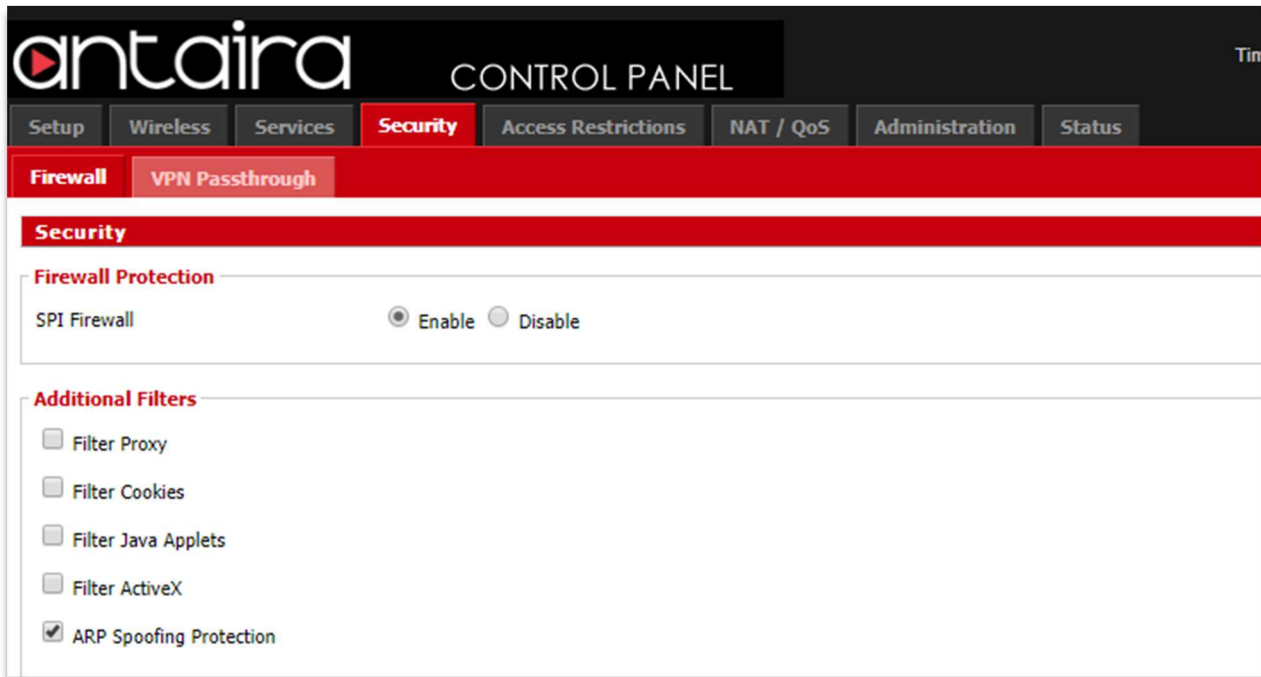
	intercept HTTPS connections. All HTTPS traffic will not be filtered by Privoxy unless added to the autconfig.
<b>Exclude IP</b>	Exclude an IP address.
<b>Custom Configuration</b>	Allows you to specify custom settings and paths to custom filters on external media. e.g. A USB.
<b>Whitelist</b>	Enter items to be whitelisted from the filter.

## 5. Security

### 5.1 Firewall

#### 5.1.1 Security

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



[Security > Firewall > Security](#)

Security	Description
<b>SPI Firewall</b>	Enable or disable the SPI Firewall.
<b>Filter Proxy</b>	Blocks HTTP requests containing the "Host:" string.
<b>Filter Cookies</b>	Identifies HTTP requests that contain the "Cookie:" string and mangle the cookie. Attempts to stop cookies from being used.
<b>Filter Java Applets</b>	Blocks HTTP requests containing a URL ending in ".js" or ".class".

<b>Filter ActiveX</b>	Blocks HTTP requests containing a URL ending in “.ocx” or “.cab”.
<b>ARP Spoofing Protection</b>	Enable protection against ARP spoofing.

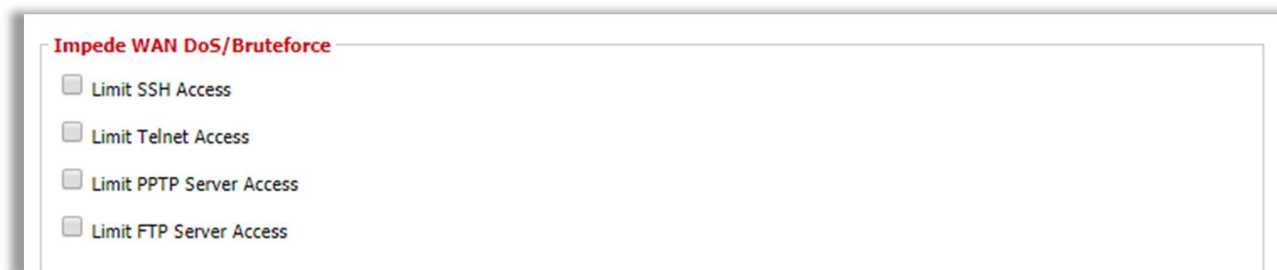
## 5.1.2 Block WAN Request



[Security > Firewall > Block WAN Request](#)

Block WAN Requests	Description
<b>Block Anonymous WAN Requests</b>	Stops the router from responding to pings from the WAN.
<b>Filter Multicast</b>	Prevents multicast packets from reaching the LAN.
<b>Filter WAN NAT Redirection</b>	Prevents hosts on the LAN from using WAN address of the router to contact servers on the LAN which may have been configured using port redirection.
<b>Filter IDENT (port 113)</b>	Prevents WAN access to port 113.
<b>Block WAN SNMP Access</b>	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
<b>Limit SSH Access</b>	Enable or disable this feature.
<b>Limit Telnet Access</b>	Enable or disable this feature.
<b>Limit PPTP Server Access</b>	Enable or disable this feature.
<b>Limit FTP Server Access</b>	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  (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
<b>Warning Notifier</b>	Enable or disable the Warning Notifier feature.
<b>Connection Limit</b>	Limit amount of connections. Default is 500.
<b>Email SMTP Server</b>	Email SMTP server.
<b>SMTP Auth Username</b>	The SMTP username.
<b>SMTP Auth Password</b>	The SMTP password.
<b>Senders Email Address</b>	The sender's email address.
<b>Senders Full Name</b>	The sender's name.
<b>Recipient Domain Name</b>	Enter recipient's domain name.
<b>Recipient Email Address</b>	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

**Options**

Dropped

Rejected

Accepted

[Security > Firewall > Log Management](#)

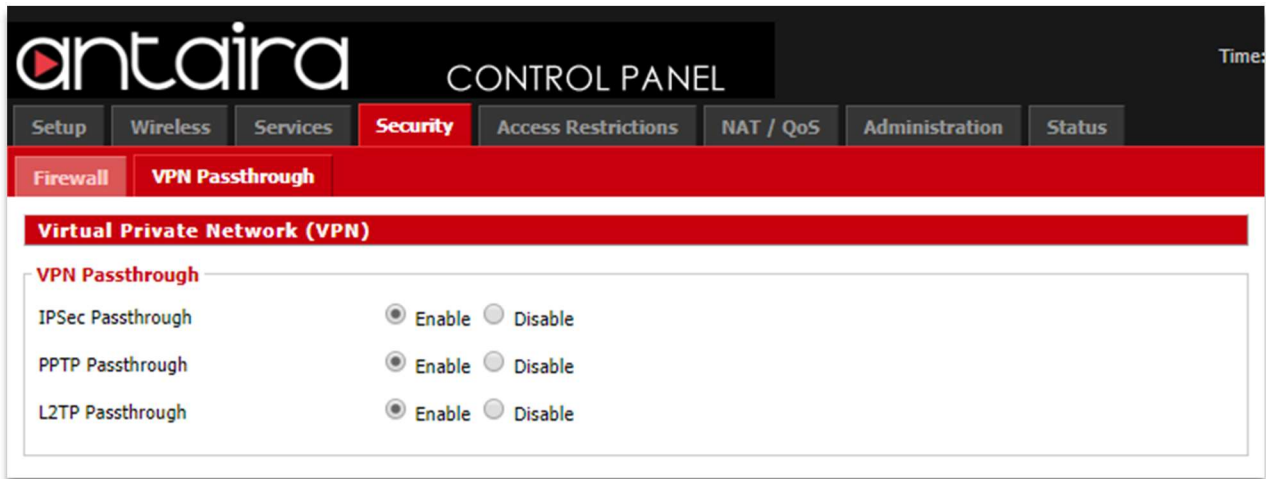
Log Management	Description
<b>Log</b>	To keep activity logs, select <b>Enable</b> .
<b>Log Level</b>	Set this to the required amount of information. Set Log Level higher to log more actions.
<b>Dropped</b>	Log Dropped items
<b>Rejected</b>	Log Rejected items
<b>Accepted</b>	Log Accepted items.

**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.



[Security > Firewall > VPN Passthrough](#)

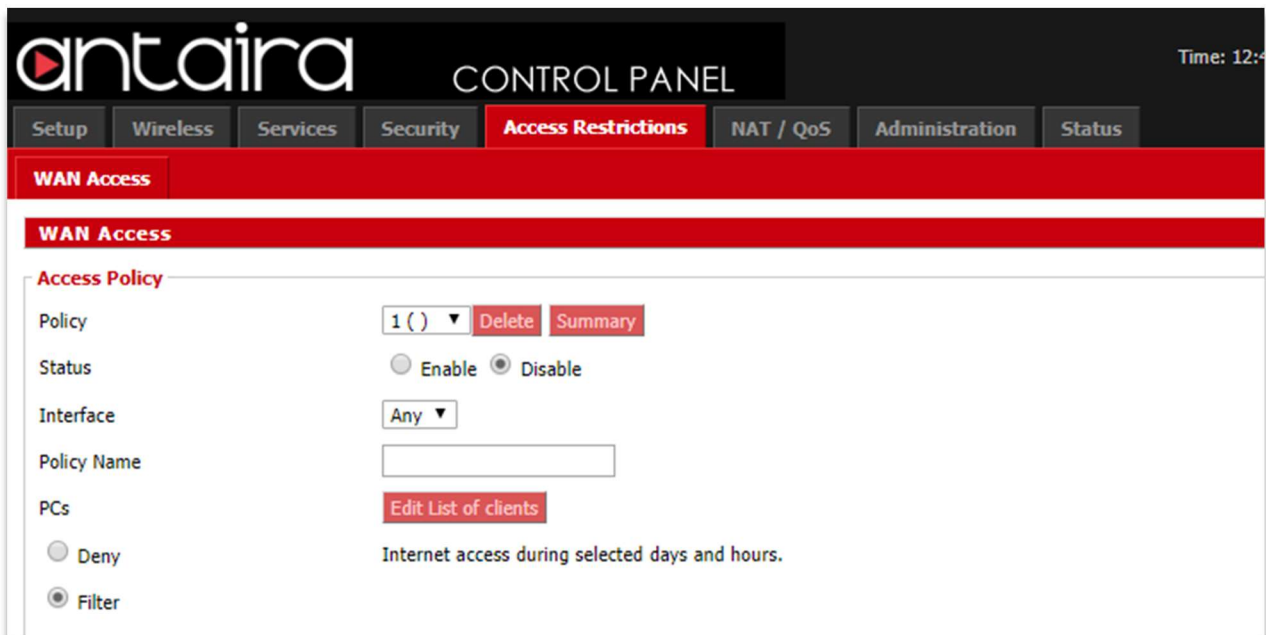
VPN Passthrough	Description
IPSec Passthrough	Allow IPSec.
PPTP Passthrough	Allow PPTP.
L2TP Passthrough	Allow P2TP.

# 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.



[Access Restriction > WAN Access > Access Policy](#)

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

### 6.1.2 Days and Times

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

[Access Restriction > WAN Access > Days and Times](#)

### 6.1.3 Blocked Services

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

[Access Restriction > WAN Access > Blocked Services](#)



## 6.1.4 Website Blocking

Block specific websites by URL or keyword.

The screenshot shows two sections for website blocking. The first section, 'Website Blocking by URL Address', contains five rows of three input fields each. The second section, 'Website Blocking by Keyword', contains five rows of four input fields each.

[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.

The screenshot shows the 'antaira CONTROL PANEL' interface. The 'NAT / QoS' menu is selected, and the 'Port Forwarding' sub-menu is active. Below the navigation tabs, there is a table for configuring port forwards.

Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
<input type="text"/>	Both ▼ TCP UDP Both	<input type="text"/>	0	0.0.0.0	0	<input type="checkbox"/>

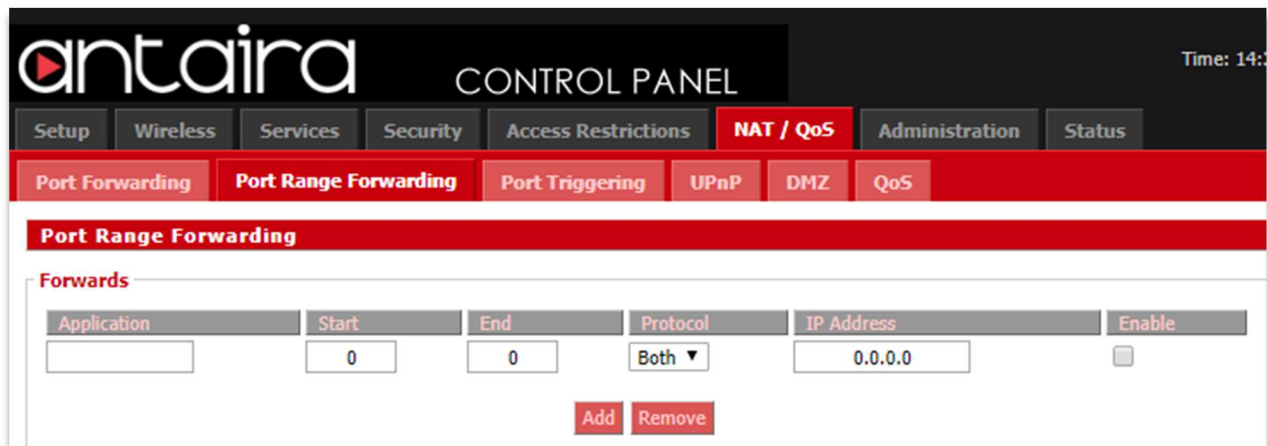
Buttons: Add, Remove

[NAT/QoS > Port Forwarding](#)

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

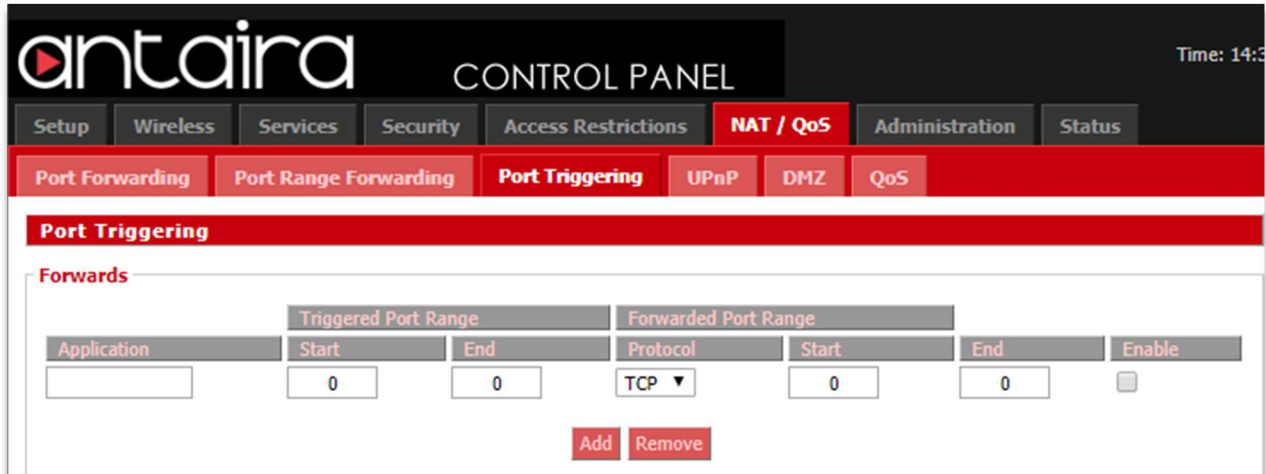


[NAT/QoS > Port Range Forwarding](#)

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

## 7.3 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.



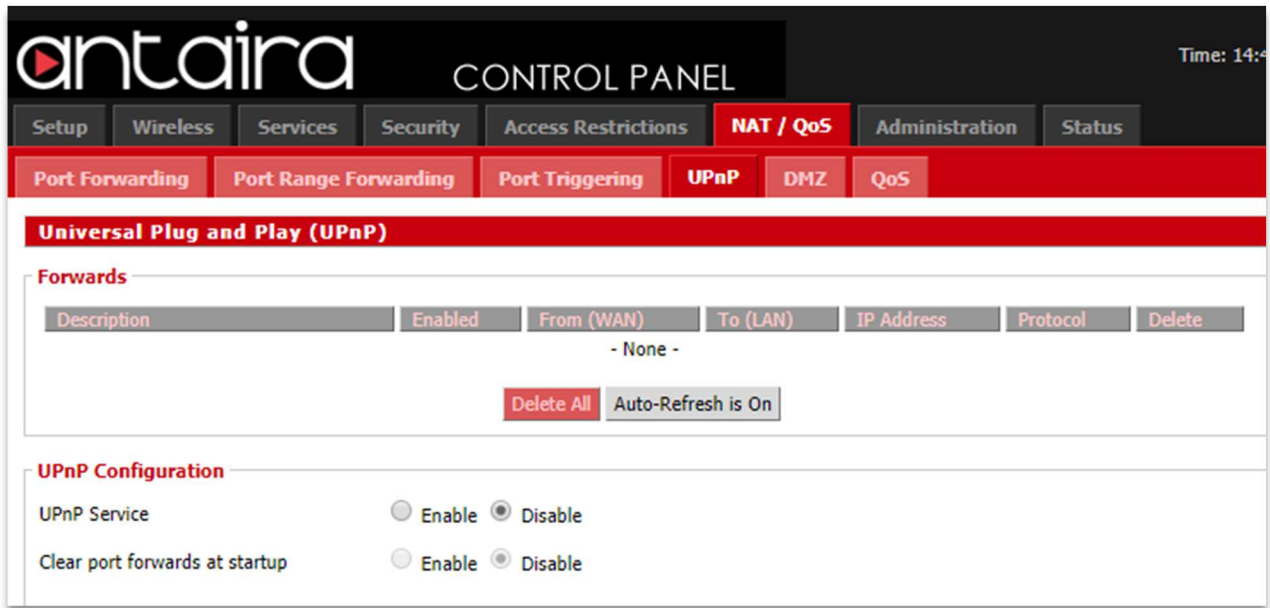
[NAT/QoS > Port Triggering](#)

Port Triggering	Description
<b>Application</b>	Enter the name of the application in the field provided.
<b>Triggered Port Range</b>	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 <i>Forwarded Port Range</i> will be forwarded to that PC.
<b>Protocol</b>	Choose the right protocol <i>TCP</i> , <i>UDP</i> , or <i>Both</i> . Set this to what the application requires.
<b>Forwarded Port Range</b>	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 <i>Triggered Port Range</i> .
<b>Enable</b>	Enable port triggering for the application.

## 7.4 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.

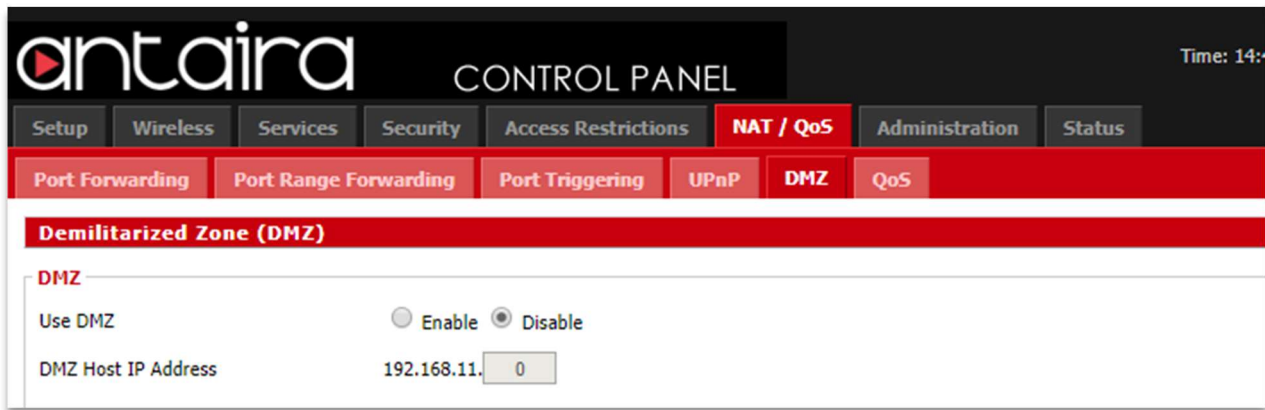


### [NAT/QoS > UPnP](#)

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

## 7.5 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.



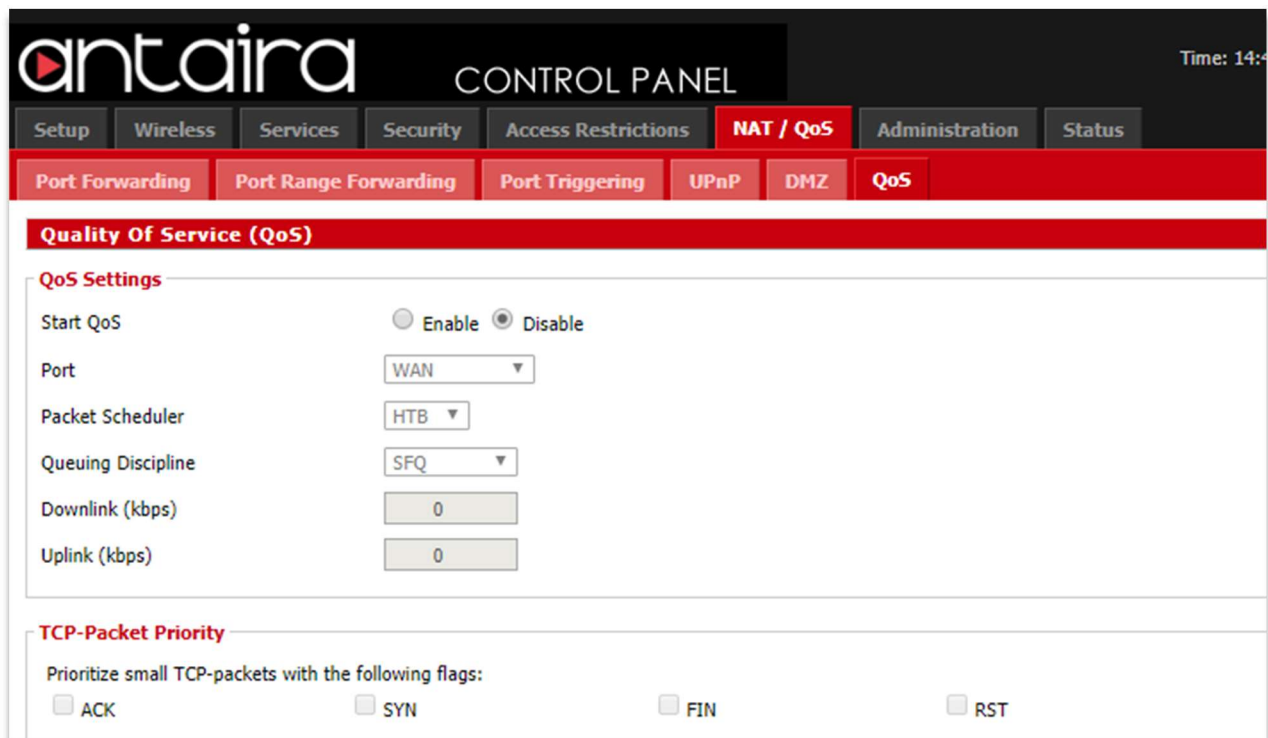
[NAT/QoS > DMZ](#)

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.

## 7.6 QoS

### 7.6.1 QoS Settings

Bandwidth management prioritizes the traffic on your router. Interactive traffic (telephony, browsing, telnet, etc) gets priority and bulk traffic (file transfers, 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.



[NAT/QoS > QoS > QoS Settings](#)

Quality of Service (QoS)	Description
<b>Start QoS</b>	Enable or disable QoS services.
<b>Port</b>	You must choose whether to apply QoS to the WAN or LAN & WLAN port ( <i>LAN and WLAN are bonded internally into a single virtual device</i> ).

<b>Packet Scheduler</b>	<p><b>HFSC:</b> 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.</p> <p><b>HTB:</b> 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.</p>
<b>Queuing Discipline</b>	Choose between <b>SFQ</b> or <b>FQ_CODEL</b> as the queuing discipline method.
<b>Downlink (kbps)</b>	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.
<b>Uplink (kbps)</b>	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.
<b>TCP Packet Priority</b>	Prioritize small TCP-packets with the following flags: <i>ACK, STN, FIN, RST.</i>

**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.

### 7.6.2 Services Priority

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

**Services Priority**

Delete	Service Name	Priority
<input type="button" value="Add"/>	100bao [ 0 ~ 0 ]	

**Port Services**

Service Name:

Protocol:

Port Range:  ~

[NAT/QoS > QoS > Services Priority](#)

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

### 7.6.3 Interface Priority

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

[NAT/QoS > QoS > Interface Priority](#)

### 7.6.4 Netmask Priority

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

[NAT/QoS > QoS > Netmask Priority](#)

### 7.6.5 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.

[NAT/QoS > QoS > MAC Priority](#)

### 7.6.6 Default Bandwidth Level

Enable per WAN or LAN default Bandwidth limits.

[NAT/QoS > 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 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 Router Password

The screenshot shows the Antaira Control Panel interface. The top navigation bar includes tabs for Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, Administration (selected), and Status. Below this is a secondary navigation bar with Management (selected), Keep Alive, Commands, WOL, Factory Defaults, Firmware Upgrade, and Backup. The main content area is titled "Router Management" and contains a section for "Router Password" with three input fields: Router Username, Router Password, and Re-enter to confirm.

[Administration > Management > Router Password](#)

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

## 8.1.2 Web Access

**Web Access**

Protocol  HTTP  HTTPS

Auto-Refresh (in seconds)

Enable Info Site  Enable  Disable

Info Site Password Protection  Enabled

Info Site MAC Masking  Enable  Disable

[Administration > Management > Web Access](#)

Web Access	Description
<b>Protocol</b>	Manage the router using either HTTP protocol or HTTPS protocol. If you choose to disable this feature, a manual reboot will be required.
<b>Auto-Refresh (seconds)</b>	Set the auto-refresh time of the web page.
<b>Enable Info Site</b>	Activate the router information web page.
<b>Info Site Password Protection</b>	Password protect the router information web page.
<b>Info site MAC Masking</b>	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  (Default: 8080, Range: 1 - 65535)

SSH Management  Enable  Disable

Telnet Management  Enable  Disable

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

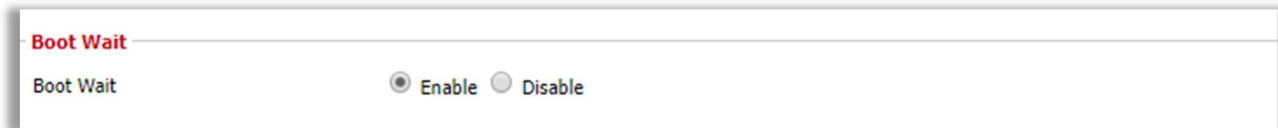
Allow Any Remote IP  Enable  Disable

[Administration > Management > Remote Access](#)

Remote Access	Description
<b>Web GUI Management</b>	Enable or disable remote access the web interface.
<b>Use HTTPS</b>	Use HTTPS, otherwise default is HTTP.
<b>Web GUI Port</b>	To remotely manage the router, enter <code>http://xxxx.xxxx.xxxx.xxxx:8080</code> (the 's represents the router's IP address, and 8080 represents the specified port) in your web browser's address field.
<b>SSH Management</b>	Enable SSH remote access. Note that the SSH daemon needs to be enabled in the <i>Services</i> page.
<b>Telnet Management</b>	Enable Telnet remote access.
<b>Telnet Remote Port</b>	Telnet port. Default is port 23.
<b>Allow Any Remote IP</b>	Allow any remote IP access or specify a range or IPs.

### 8.1.4 Boot Wait

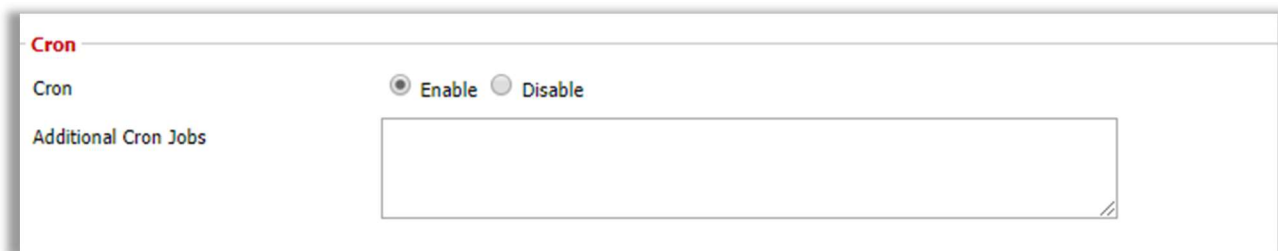
Boot Wait is a feature that introduces a short delay while booting (5 seconds). During this delay you can initiate the download of a new firmware if the one in flash rom is not broken. This is only necessary if you can no longer reflash using the web interface because the installed firmware will not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



[Administration > Management > Boot Wait](#)

### 8.1.5 Cron

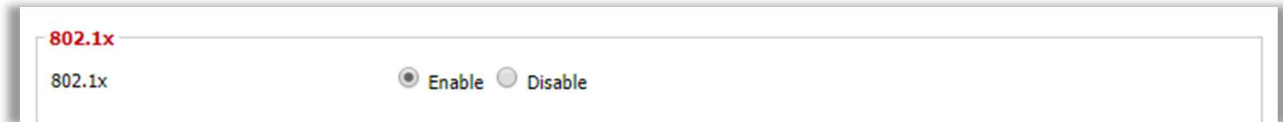
The cron subsystem schedules execution of Linux commands. You will need to use the command line or startup scripts to do this.



[Administration > Management > Cron](#)

### 8.1.6 802.1x

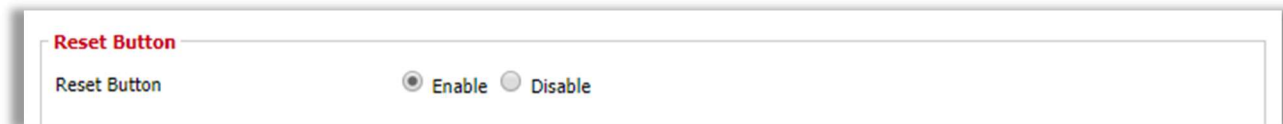
A limited 802.1x server needed to fulfil WPA handshake requirements to allow Windows XP clients to work with WPA.



[Administration > Management > 802.1x](#)

### 8.1.7 Reset Button

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

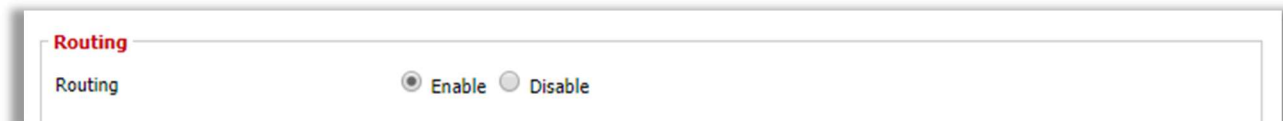


[Administration > Management > Reset Button](#)

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

### 8.1.8 Routing

Routing enables the OSPF and RIP routing daemons if you have set up OSPF or RIP in the *Advanced Routing* page.



[Administration > Management > Routing](#)

## 8.1.9 JFFS2 Support

**JFFS2 Support**

Internal Flash Storage	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Clean Internal Flash Storage	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Total / Free Size	(Not mounted)

[Administration > Management > JFFS2 Support](#)

## 8.1.10 Language Selection

Select the language presented on the router.

**Language Selection**

Language	English ▼
----------	-----------

[Administration > Management > Language Selection](#)

## 8.1.11 IP Filter Settings

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.

**IP Filter Settings (adjust these for P2P)**

TCP Congestion Control	westwood ▼	
Maximum Ports	4096	(Default: 32768, Range: 256 - 65535)
TCP Timeout (in seconds)	3600	(Default: 3600, Range: 1 - 86400)
UDP Timeout (in seconds)	120	(Default: 120, Range: 1 - 86400)

[Administration > Management > IP Filter Settings](#)



## 8.1.12 Router GUI Style

Select the graphical style of the router.

The screenshot shows the 'Router GUI Style' configuration page. It features a 'Style' dropdown menu currently set to 'red' and a 'Preview' button. Below this, there is a 'Use Dark Styles' section with two radio buttons: 'Enable' and 'Disable', with 'Disable' being the selected option.

[Administration > Management > Router GUI Style](#)

## 8.1.13 Router Reboot

You may reboot the router under this page as well.

The screenshot shows the bottom of the Router Reboot configuration page, which contains four red buttons: 'Save', 'Apply Settings', 'Cancel Changes', and 'Reboot Router'.

[Administration > Management > Router Reboot](#)

## 8.2 Keep Alive

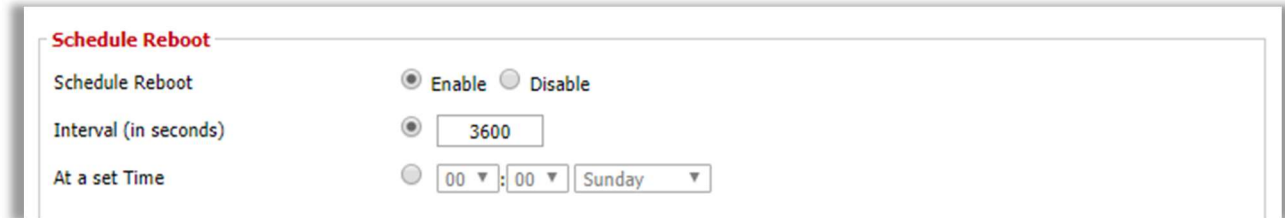
### 8.2.1 Proxy/Connection Watchdog

The screenshot shows the 'Proxy/Connection Watchdog' configuration page within the 'Keep Alive' section of the 'Administration' menu. The page has a dark header with the 'antaira' logo and 'CONTROL PANEL' text. The 'Administration' menu item is highlighted in red. Below the menu, there are sub-menus for 'Management', 'Keep Alive', 'Commands', 'WOL', 'Factory Defaults', 'Firmware Upgrade', and 'Backup'. The 'Keep Alive' sub-menu is selected. The 'Proxy/Connection Watchdog' section contains the following settings: 'Enable Proxy Watchdog' with 'Enable' selected, 'Interval (in seconds)' set to 120, 'Proxy IP Address' as an empty text box, and 'Proxy Port' set to 3128.

[Administration > Keep Alive > Proxy/Connection Watchdog](#)

## 8.2.2 Schedule Reboot

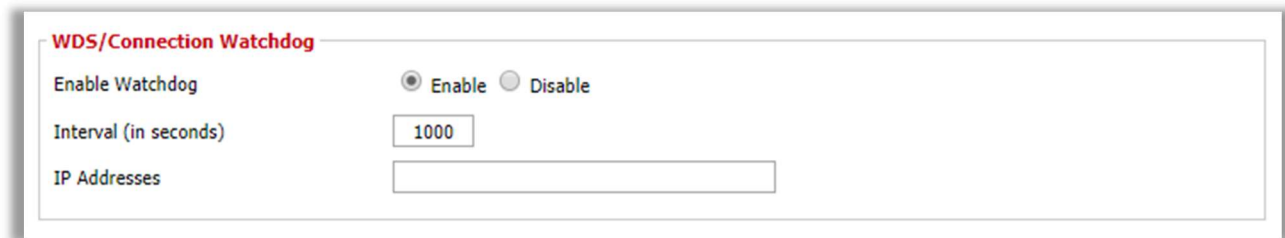
You can schedule regular reboots for the router after a certain amount of seconds or at a specific date and time each week or everyday.



The screenshot shows the 'Schedule Reboot' configuration page. It has a title 'Schedule Reboot' in red. Below the title, there are three rows of configuration options. The first row is 'Schedule Reboot' with radio buttons for 'Enable' (selected) and 'Disable'. The second row is 'Interval (in seconds)' with a radio button for 'Interval (in seconds)' (selected) and a text input field containing '3600'. The third row is 'At a set Time' with radio buttons for 'At a set Time' (selected), '00' (selected), ':00' (selected), and 'Sunday' (selected).

[Administration > Keep Alive > Schedule Reboot](#)

## 8.2.3 WDS/Connection Watchdog



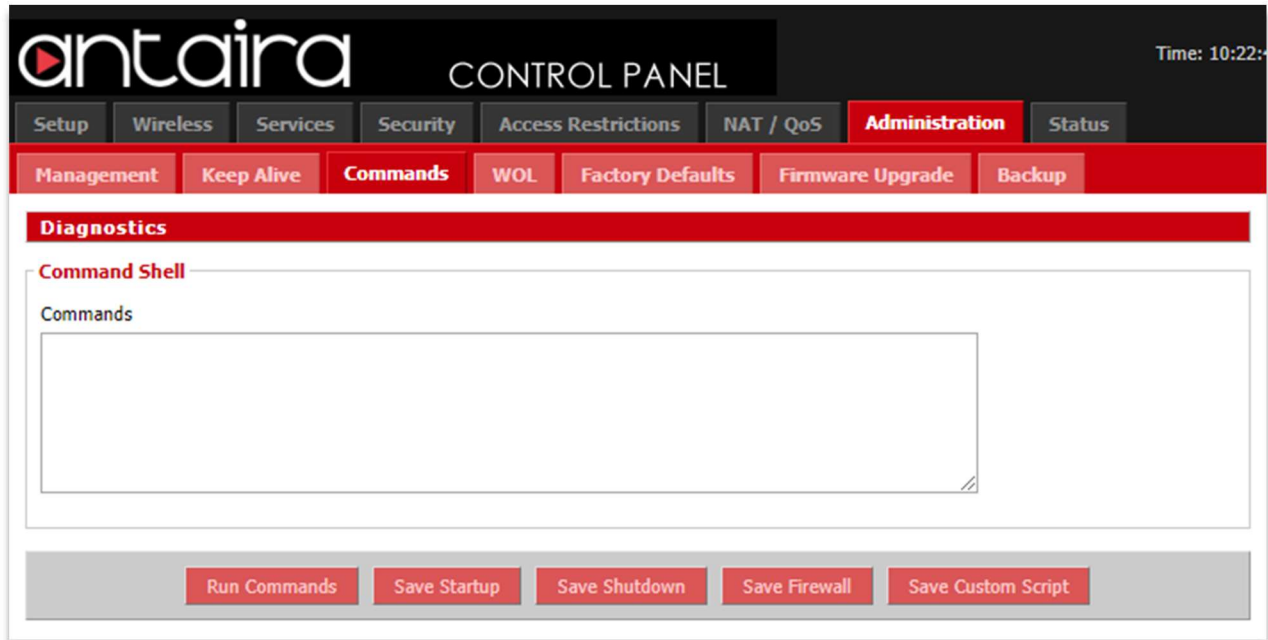
The screenshot shows the 'WDS/Connection Watchdog' configuration page. It has a title 'WDS/Connection Watchdog' in red. Below the title, there are three rows of configuration options. The first row is 'Enable Watchdog' with radio buttons for 'Enable' (selected) and 'Disable'. The second row is 'Interval (in seconds)' with a radio button for 'Interval (in seconds)' (selected) and a text input field containing '1000'. The third row is 'IP Addresses' with a text input field.

[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**.



[Administration > Commands](#)

## 8.4 Wake on LAN (WOL)

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

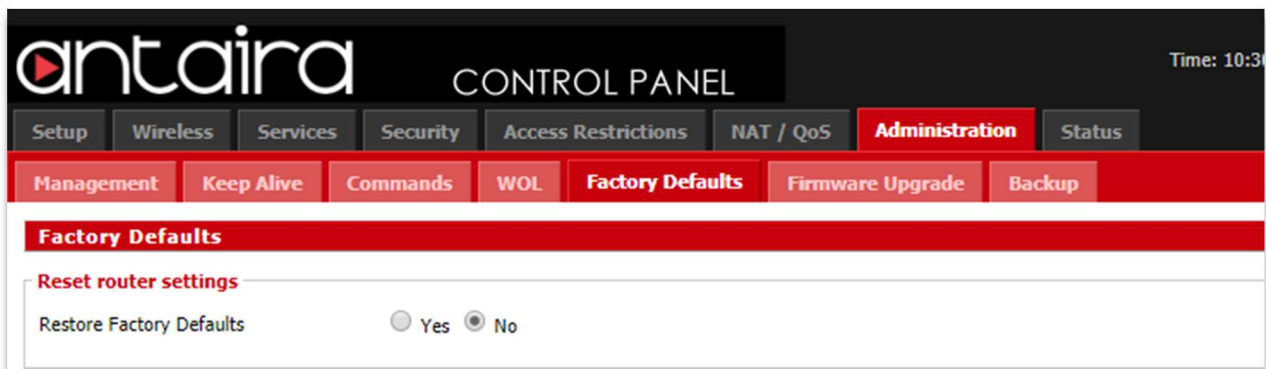
[Administration > WOL](#)

Wake on LAN	Description
<b>Available Hosts</b>	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.
<b>WOL Addresses</b>	The WOL addresses section allows individual hosts in the WOL list ( <i>stored in the wol_hosts NVRAM variable</i> ) to be Woken Up. The list is a combination of selected ( <i>enabled</i> ) available hosts and manually added WOL hosts.
<b>Manual WOL</b>	The manual WOL section allows individual or a list of hosts to be woken up by clicking Wake Up to send it the WOL magic packet.
<b>WOL daemon</b>	Besides attempting to Wake Up the manually specified hosts, clicking the <b>WOL daemon</b> 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.
<b>Hostname</b>	Enter a hostname for the WOL daemon.
<b>SecureOn Password</b>	Enter a password.
<b>MAC Addresses</b>	Fill the MAC address(es) ( <i>either separated by spaces or one per line</i> ) 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**.



[Administration > Factory Defaults](#)

## 8.6 Firmware Upgrade

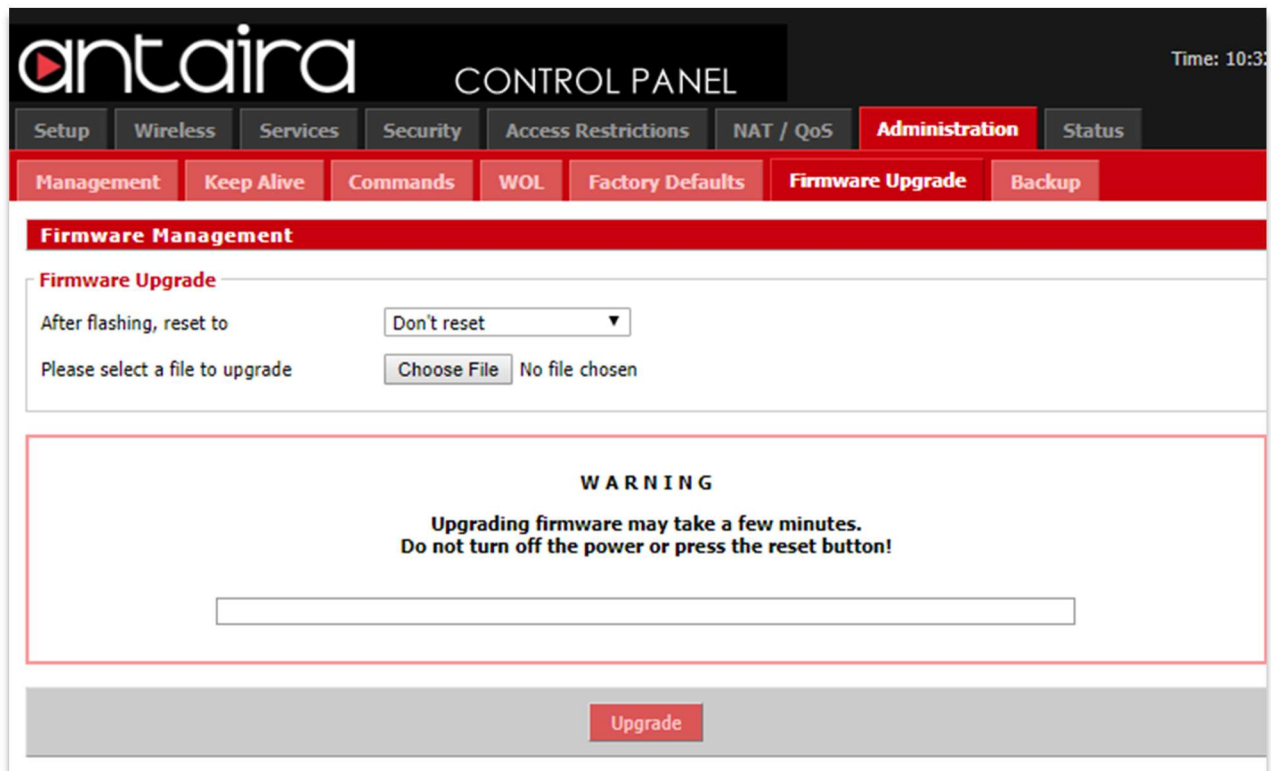
New firmware versions are available at [www.antaira.com](http://www.antaira.com). When you upgrade the router's firmware, you may lose its configuration settings, so make sure you write down the router settings before you upgrade its firmware.

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.



[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.

antaira CONTROL PANEL Time: 10:38

Setup Wireless Services Security Access Restrictions NAT / QoS Administration Status

Management Keep Alive Commands WOL Factory Defaults Firmware Upgrade Backup

**Backup Configuration**

**Backup Settings**

Click the "Backup" button to download the configuration backup file to your computer.

**Restore Configuration**

**Restore Settings**

Please select a file to restore  No file chosen

**WARNING**

Only upload files backed up using this firmware and from the same model of router.  
Do not upload any 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.

**antaira CONTROL PANEL** Time: 10:43

Setup | Wireless | Services | Security | Access Restrictions | NAT / QoS | Administration | **Status**

**Router** | WAN | LAN | Wireless | Bandwidth | Syslog | Sys-Info

### Router Information

**System**

Router Name	Antaira
Router Model	Industrial Router
Firmware Version	Antaira r38373 (01/22/19)
Kernel Version	Linux 3.18.132 #30962 Tue Jan 22 15:01:48 CET 2019 mips
MAC Address	<u>C4:93:00:0F:A9:3F</u>
Hostname	
WAN Domain Name	antaira.local
LAN Domain Name	
Current Time	Mon, 11 Feb 2019 10:43:01
Uptime	4 days, 1:31

**CPU**

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	0.11, 0.05, 0.01
Temperatures	Not available

**Memory**

Total Available	60928 kB / 65536 kB
Free	33224 kB / 60928 kB
Used	27704 kB / 60928 kB
Buffers	3484 kB / 27704 kB
Cached	8896 kB / 27704 kB
Active	8780 kB / 27704 kB
Inactive	5500 kB / 27704 kB



## 9.2 WAN

antaira
CONTROL PANEL Time: 10:56

Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status

Router
WAN
LAN
Wireless
Bandwidth
Syslog
Sys-Info

WAN

**Configuration Type**

Connection Type	Automatic Configuration - DHCP
Connection Uptime	0:00:25
IP Address	192.168.1.76
Subnet Mask	255.255.255.0
Gateway	192.168.1.10
DNS 1	192.168.1.2
DNS 2	
DNS 3	
Remaining Lease Time	7 days 23:59:34

DHCP Release
DHCP Renew

Traffic

**Total Traffic**

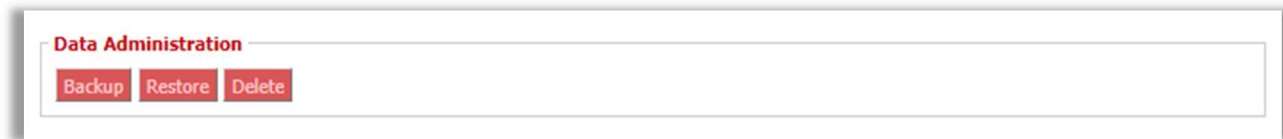
Incoming (MBytes)	159
Outgoing (MBytes)	21

Traffic by Month

Month	Incoming (MBytes)	Outgoing (MBytes)
1	0	0
2	0	0
3	0	0
4	140	10
5	220	15
6	0	0
7	40	5
8	50	10
9	20	5
10	25	5
11	20	5
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0
25	0	0
26	0	0
27	0	0
28	0	0

[Status > WAN](#)

## Data Administration



[Status](#) > [WAN](#) > [Data Administration](#)

## 9.3 LAN

The screenshot shows the Antaira Control Panel interface. At the top, the 'antaira' logo and 'CONTROL PANEL' are visible, along with the time 'Time: 11:02'. A navigation bar contains tabs for Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, Administration, and Status. Below this, a secondary navigation bar highlights 'Router', 'WAN', 'LAN', 'Wireless', 'Bandwidth', 'Syslog', and 'Sys-Info'. The main content area is titled 'Local Network' and contains several sections:

- LAN Status:** A table showing network parameters:

MAC Address	04:F0:21:41:AF:AE
IP Address	192.168.11.50
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0
- Active Clients:** A table with columns: Hostname, IP Address, MAC Address, Interface, Connections, Ratio [4096].

Hostname	IP Address	MAC Address	Interface	Connections	Ratio [4096]
*	192.168.1.84		eth0	4	0%
- Dynamic Host Configuration Protocol:**
  - DHCP Status:** A table showing DHCP configuration:

DHCP Server	Enabled
DHCP Daemon	DNSMasq
Start IP Address	192.168.11.100
End IP Address	192.168.11.149
Client Lease Time	1440 min
  - DHCP Clients:** A table with columns: Hostname, IP Address, MAC Address, Client Lease Time, Delete. It shows '- None -'.
  - Connected PPPoE Clients:** A table with columns: Interface, Username, Local IP, Delete. It shows '- None -'.

[Status > LAN](#)

## 9.4 Wireless

**antaira** CONTROL PANEL Time: 11:07

Setup Wireless Services Security Access Restrictions NAT / QoS Administration **Status**

Router WAN LAN **Wireless** Bandwidth Syslog Sys-Info

### Wireless

**Wireless Status**

Interface: ath0

MAC Address: 04:F0:21:41:AF:AE

Chipset: QCA988x 802.11ac

Radio: Radio is Off

Mode: Client

Network: Disabled

SSID:

Channel: Unknown

TX Power: Radio is Off

Rate: Disabled

ACK Timing: N/A

Encryption - Interface ath0: Enabled, WPA3-PSK

Connected Clients: 0

**Wireless Packet Info**

Received (RX)	0 OK, no error	100%
Transmitted (TX)	0 OK, no error	100%

**Wireless Nodes**

**Access Point & Clients**

MAC Address	Radioname	Interface	Uptime	TX Rate	RX Rate	Info	Signal	Noise	SNR	Signal Quality
- None -										

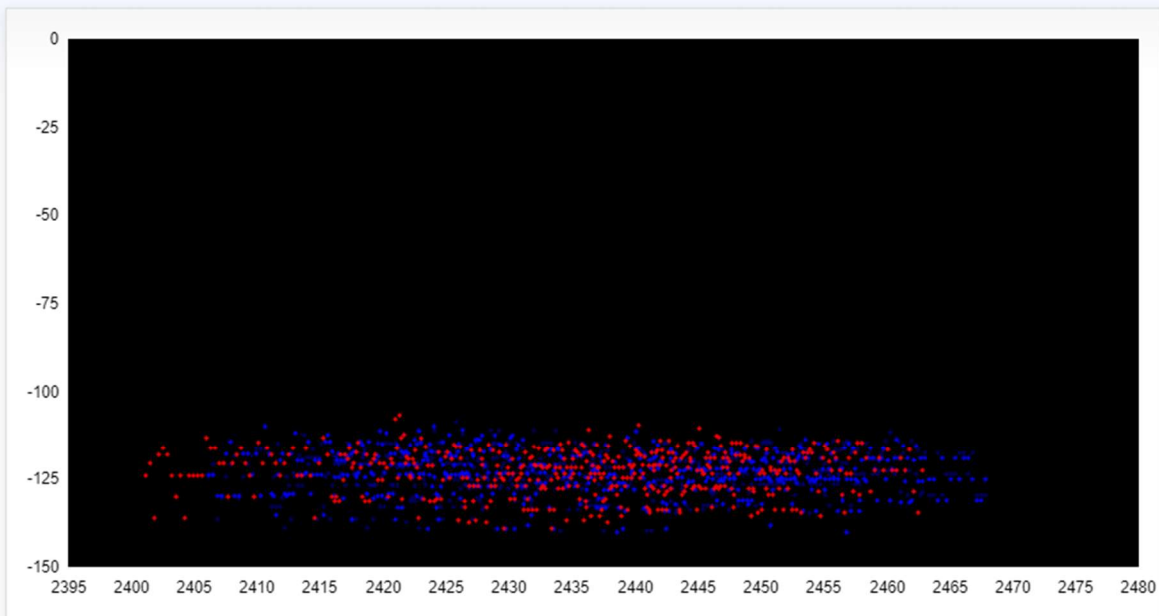
[Spectrum](#)
[Site Survey](#)
[Wiviz Survey](#)

[Status > Wireless](#)

## Spectrum

The spectral scan will show which frequencies have a lot of interference across either the 2.4GHz or 5GHz. No channel numbers are provided in the scan window. The x-axis represents frequencies in Hertz (Hz). The y-axis represents power drop in dB for noise. The higher numbers are better. Blue dots represent all of the samples taken while the red dots are averaged out over a certain time.

### Spectral Scan



Time between updates:  milliseconds

[Status > Wireless > Spectral Scan](#)

## Site Survey

Neighbor's Wireless Networks												
SSID	Mode	MAC Address	Channel	Frequency	RSSI	Noise	Quality	Beacon	Open	DTIM	Rate	Join Site
None												
<input type="button" value="Refresh"/> <input type="button" value="Close"/>												

[Status > Wireless > Site Survey](#)

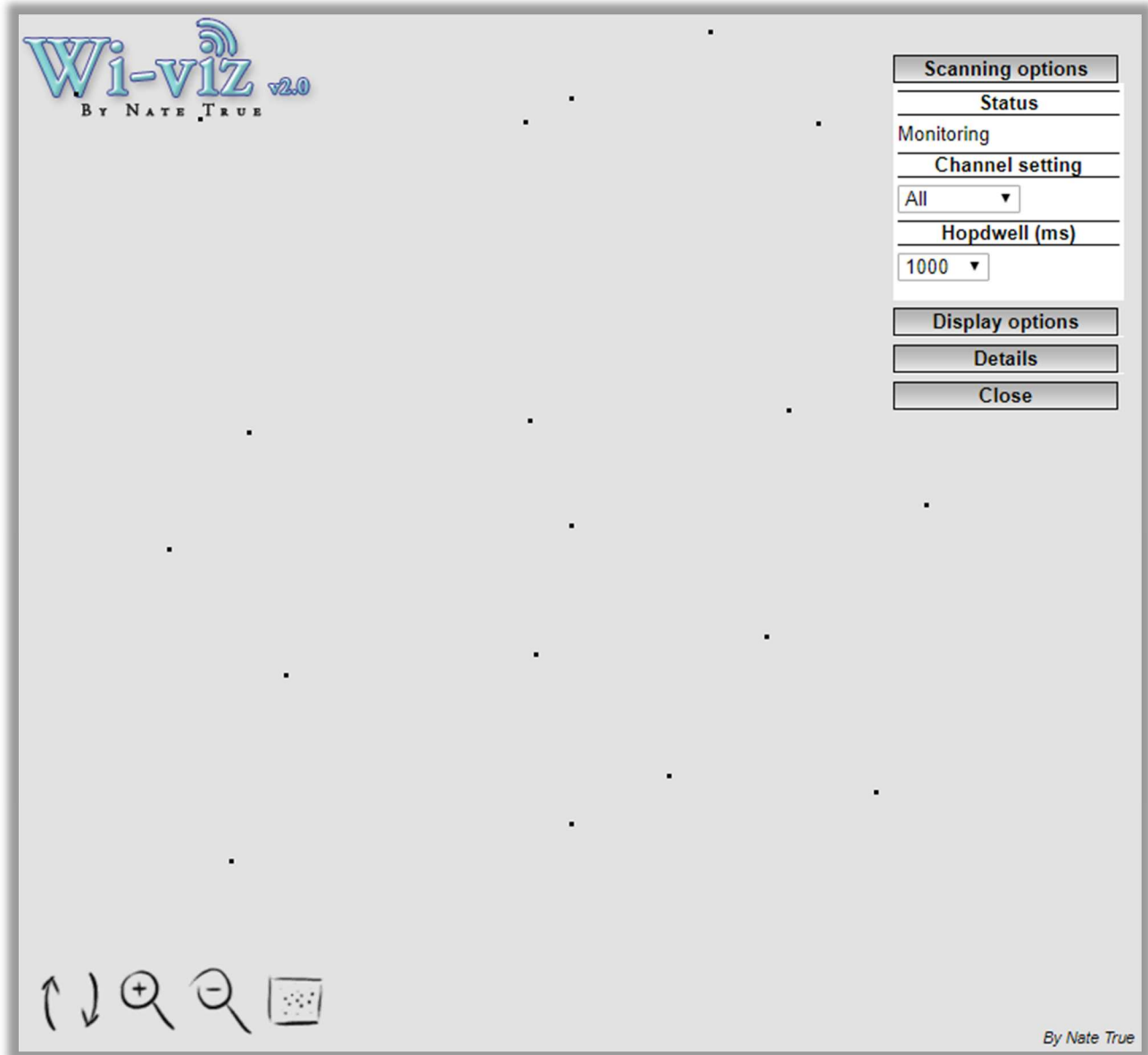
## Channel Survey

Channel Survey and Qualities								
Frequency	Channel	Noise	Quality	Active Time	Busy Time	Receive Time	Transmission Time	
2412	1	-105	99	99	284	3		
2417	2	-105	100	100	284	2		
2422	3	-105	100	100	284	1		
2427	4	-105	99	99	284	3		
2432	5	-105	99	99	284	5		
2437	6	-104	100	100	284	1		
2442	7	-104	100	100	284	0		
2447	8	-104	75	75	284	71		
2452	9	-105	93	93	284	20		
2457	10	-105	92	92	284	24		
2462	11	-104	95	95	284	17		
5180	36	-103	100	100	292	0		
5200	40	-102	91	91	292	29		
5220	44	-101	97	97	292	10		
[5240]	48	-104	97	813003	26141	422		817
5260	52	-100	100	100	292	0		
5280	56	-98	100	100	292	0		
5300	60	-95	71	71	292	85		
5320	64	-97	100	100	292	0		
5500	100	-85	100	100	292	0		
5520	104	-85	100	100	292	2		
5540	108	-85	100	100	292	1		
5560	112	-85	100	100	292	0		
5580	116	-88	100	100	292	0		
5600	120	-88	96	96	292	14		
5620	124	-90	100	100	292	0		
5640	128	-91	100	100	292	1		
5660	132	-92	100	100	292	0		
5680	136	-94	100	100	292	0		
5700	140	-94	100	100	292	0		
5720	144	-96	100	100	292	0		
5745	149	-98	99	99	292	4		
5765	153	-99	100	100	292	0		
5785	157	-101	100	100	292	1		
5805	161	-102	100	100	292	0		
5825	165	-100	100	100	292	0		
<input type="button" value="Refresh"/> <input type="button" value="Close"/>								

[Status > Wireless > Channel Survey](#)

## Wiviz Survey

Wiviz is an open source GPL project that allows you to use your router to see other networks. The interface scans for networks and shows signal strength and effects of antenna adjustment in real time.



[Status > Wireless > Wiviz Survey](#)

## 9.5 Bandwidth

The screenshot displays the antaira CONTROL PANEL interface. The top navigation bar includes tabs for Setup, Wireless, Services, Security, Access Restrictions, NAT / QoS, Administration, and Status. The Status tab is active, and the Bandwidth sub-tab is selected. The main content area is divided into two sections: "Bandwidth Monitoring - LAN" and "Bandwidth Monitoring - LAN (eth1)". Each section shows a graph with "In 0 Kbps" and "Out 0 Kbps" data points. The graph has a vertical axis with markers at 3 Kbps, 5 Kbps, and 8 Kbps. The interface also includes a "Switch to bytes/s" link and an "Autoscale (follow)" option.

[Status > Bandwidth](#)



## 9.6 Syslog

antaira CONTROL PANEL

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

Setup Wireless Services Security Access Restrictions NAT / QoS Administration **Status**

Router WAN LAN Wireless Bandwidth **Syslog** Sys-Info

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 : wlan : 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_contrack_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_contrack_pptp successfully loaded
Feb 11 19:20:01 Antaira user.info : vpn modules : nf_contrack_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_contrack_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
Feb 11 19:20:03 Antaira daemon.info pppoe-server[8116]: Terminating on signal 15 -- killing all PPPoE sessions
Feb 11 19:20:03 Antaira user.info : rp-pppoe : pppoe server successfully started
Feb 11 19:20:03 Antaira user.info : telnetd : daemon successfully stopped
Feb 11 19:20:03 Antaira user.info : dnsmasq : daemon successfully stopped
Feb 11 19:20:04 Antaira user.info : pppoe-server : daemon successfully stopped
Feb 11 19:20:04 Antaira user.info : ptpd : daemon successfully stopped
Feb 11 19:20:04 Antaira daemon.info pppoe-server[8351]: Terminating on signal 15 -- killing all PPPoE sessions
Feb 11 19:20:04 Antaira user.info : rp-pppoe : pppoe server successfully started
Feb 11 19:20:04 Antaira user.info : dnsmasq : daemon successfully started
Feb 11 19:20:04 Antaira user.info : telnetd : daemon successfully started
Feb 11 19:20:05 Antaira daemon.info pppoe-server[8483]: Could not lock PID file /var/run/pppoe-server.pid: Is another process running?
Feb 11 19:20:05 Antaira user.info : rp-pppoe : pppoe server successfully started
Feb 11 19:20:06 Antaira user.info : vpn modules : vpn modules successfully unloaded
Feb 11 19:20:06 Antaira user.info : vpn modules : nf_contrack_proto_gre successfully loaded
Feb 11 19:20:06 Antaira user.info : vpn modules : nf_nat_proto_gre successfully loaded
Feb 11 19:20:06 Antaira user.info : vpn modules : nf_contrack_pptp successfully loaded
Feb 11 19:20:06 Antaira user.info : vpn modules : nf_nat_pptp successfully loaded
Feb 11 19:20:09 Antaira user.info : pppoe-server : daemon successfully stopped
Feb 11 19:20:09 Antaira daemon.info pppoe-server[8377]: Terminating on signal 15 -- killing all PPPoE sessions
Feb 11 19:20:09 Antaira user.info : rp-pppoe : pppoe server successfully started
```

<< Prev Next >>

[Status > Syslog](#)

## 9.7 Sys-Info

**CONTROL PANEL**

Firmware: Antaira r38373 (01/22/19)  
 Time: 11:23:37 up 4 days, 2:11, load average: 0.10, 0.12, 0.04  
 WAN IP: 192.168.1.76

Setup
Wireless
Services
Security
Access Restrictions
NAT / QoS
Administration
Status

**System Information**

**Router**

Router Name	Antaira
Router Model	Industrial Router
LAN MAC	<a href="#">04:F0:21:41:AF:AE</a>
WAN MAC	<a href="#">C4:93:00:0F:A9:3F</a>
Wireless MAC	<a href="#">04:F0:21:41:AF:AE</a>
WAN IPv4	192.168.1.76
LAN IP	192.168.11.50

**Services**

DHCP Server	Enabled - Running
WRT-radauth	Disabled
WRT-rflow	Disabled
MAC-upd	Disabled
USB Support	Enabled

**Wireless**

Interface	ath0 ▼
Radio	Radio is Off
Mode	Client
Network	Disabled
SSID	
Channel	Unknown
TX Power	Radio is Off
Rate	Disabled

**Memory**

Total Available	59.5 MB / 64.0 MB
Free	32.1 MB / 59.5 MB
Used	27.4 MB / 59.5 MB
Buffers	3.6 MB / 27.4 MB
Cached	9.0 MB / 27.4 MB
Active	9.1 MB / 27.4 MB
Inactive	5.1 MB / 27.4 MB

**Wireless Packet Info**

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

**Wireless**

**Access Point & Clients**

MAC Address	Radioname	Interface	Uptime	Tx Rate	Rx Rate	Info	Signal	Noise	SNR	Signal Quality
- None -										

**DHCP**

**DHCP Clients**

Hostname	IP Address	MAC Address	Client Lease Time
- None -			

[Status > Sys-Info](#)

**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](http://www.antaira.com) / [support@antaira.com](mailto:support@antaira.com)

[www.antaira.eu](http://www.antaira.eu) / [info@antaira.eu](mailto:info@antaira.eu)

[www.antaira.com.tw](http://www.antaira.com.tw) / [info@antaira.com.tw](mailto:info@antaira.com.tw)

**Any changes to this material will be announced**