antaira®

making connectivity simple...

Wireless Software User's Manual

Version 2.1 (May 2019)

Trademark Information

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:

- AMS-7131-AC
- AMS7131-AC-T
- AMS-7131
- AMS-7131-T
- AMS-2111
- AMS-2111-T

This manual supports the following software version:

- Release: r39711 (5/2/19)

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

Table of Contents

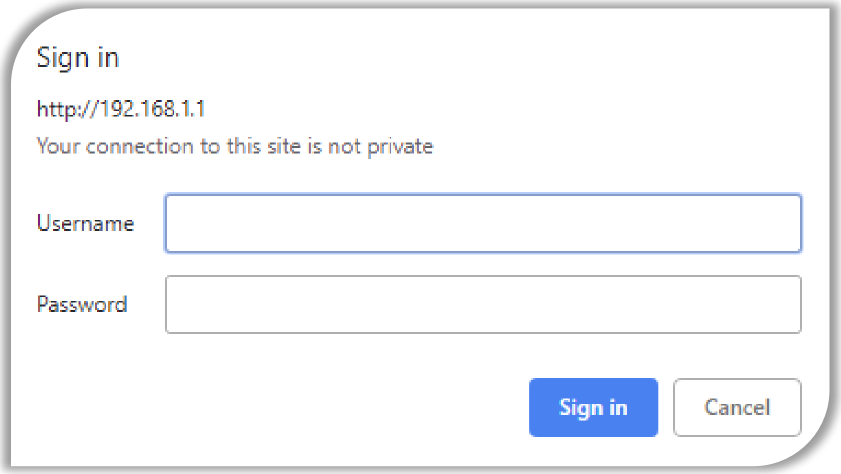
1. Access with Web Browser

1.1 Web GUI Login

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

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

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



Sign in

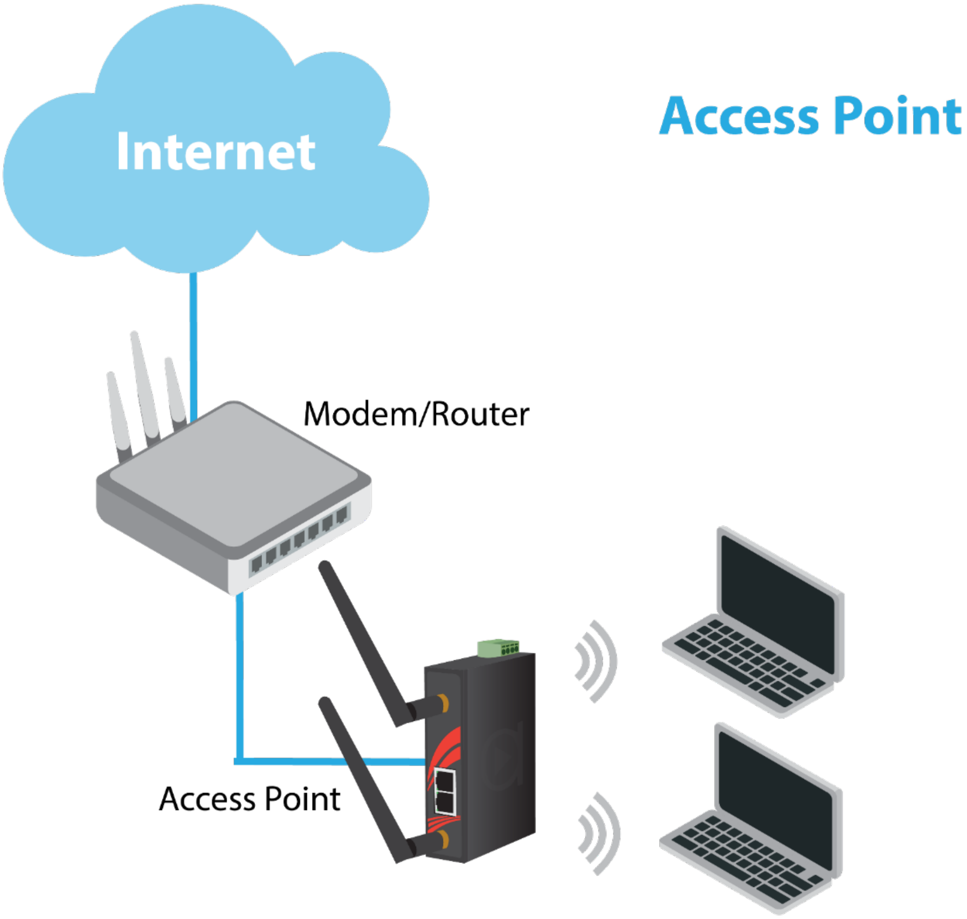
http://192.168.1.1

Your connection to this site is not private

1.2 Operation Modes

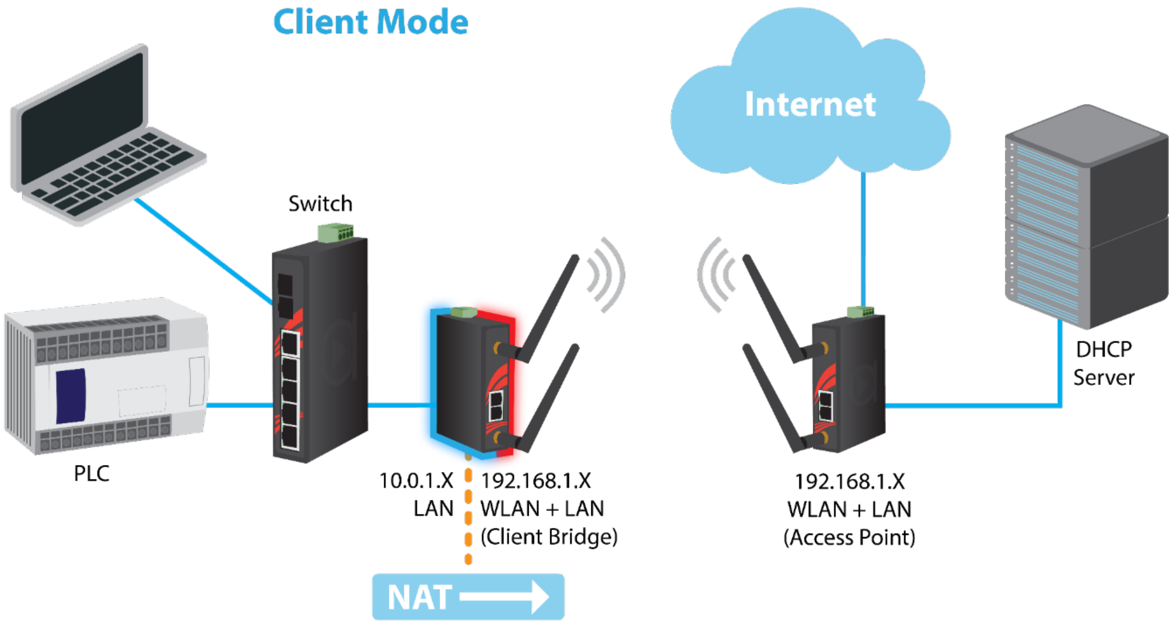
1.2.1 Access Point

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



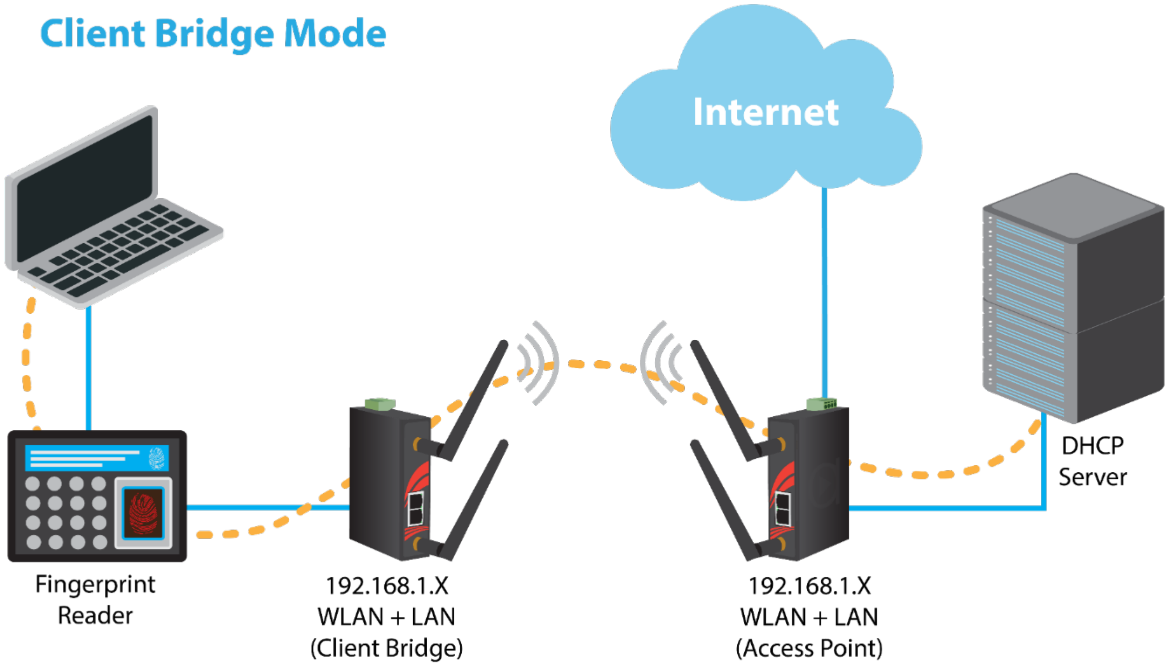
1.2.2 Client Mode

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.



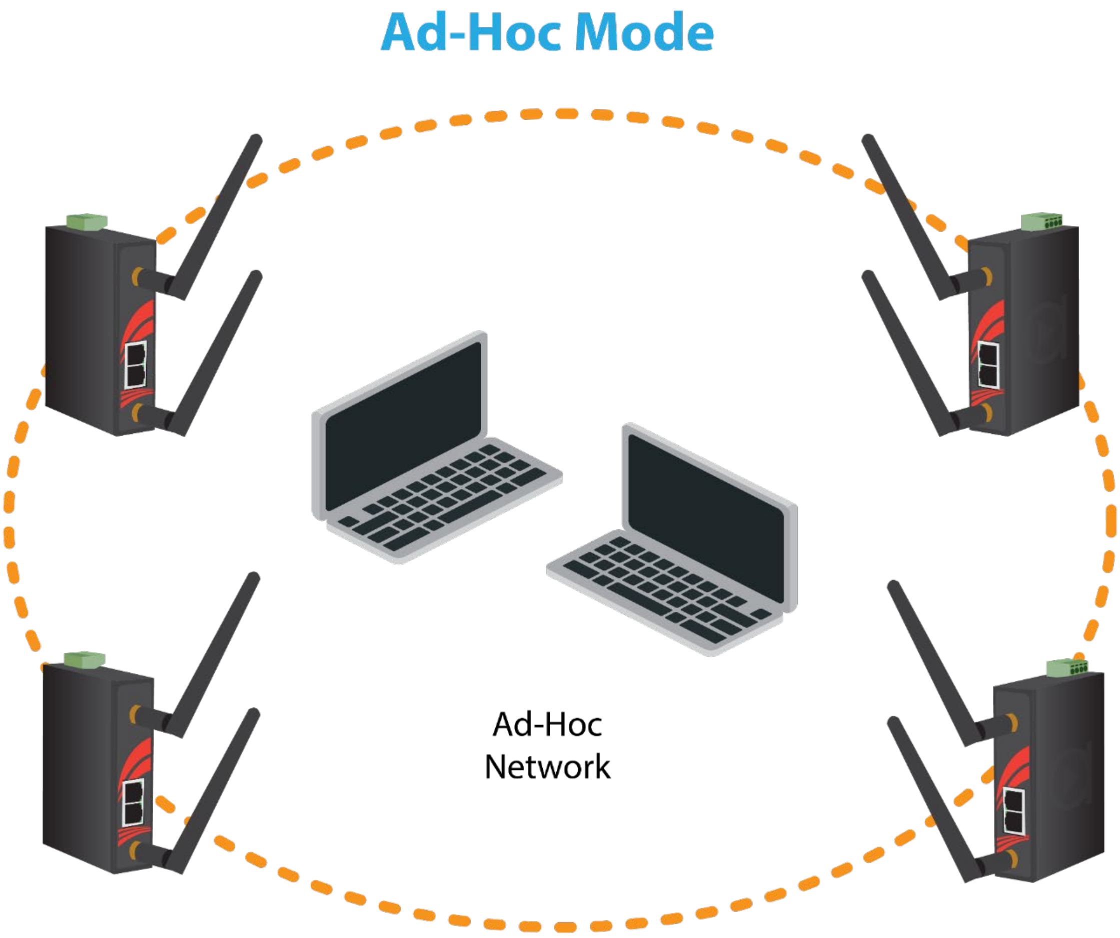
1.2.3 Client Bridge Mode

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.



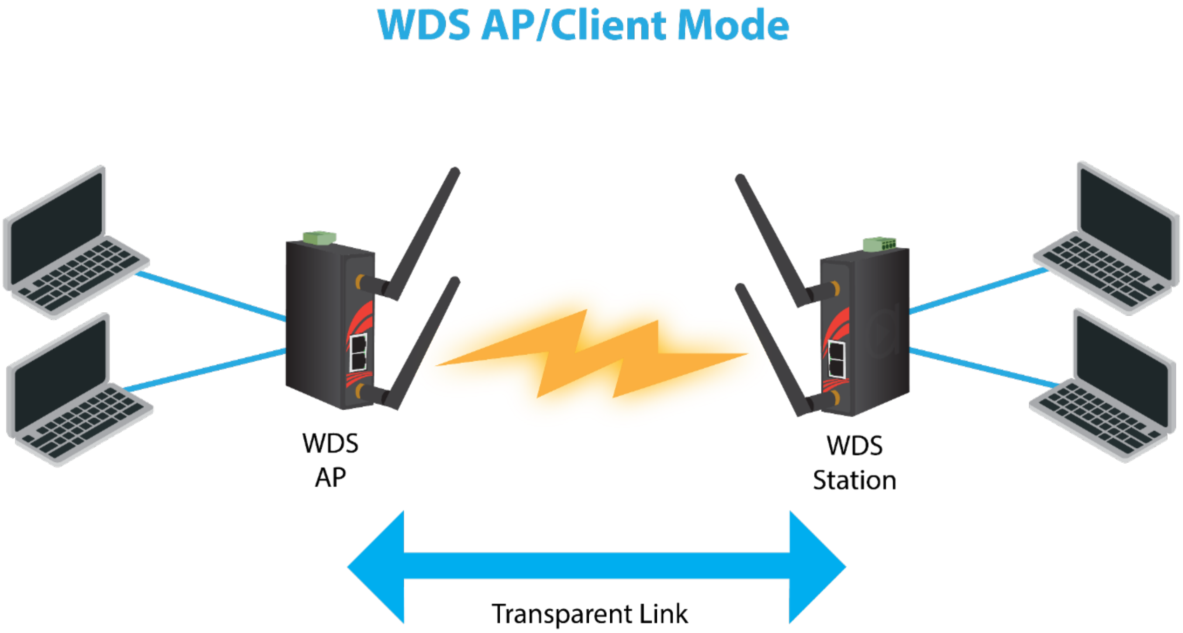
1.2.4 Ad Hoc Mode

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.



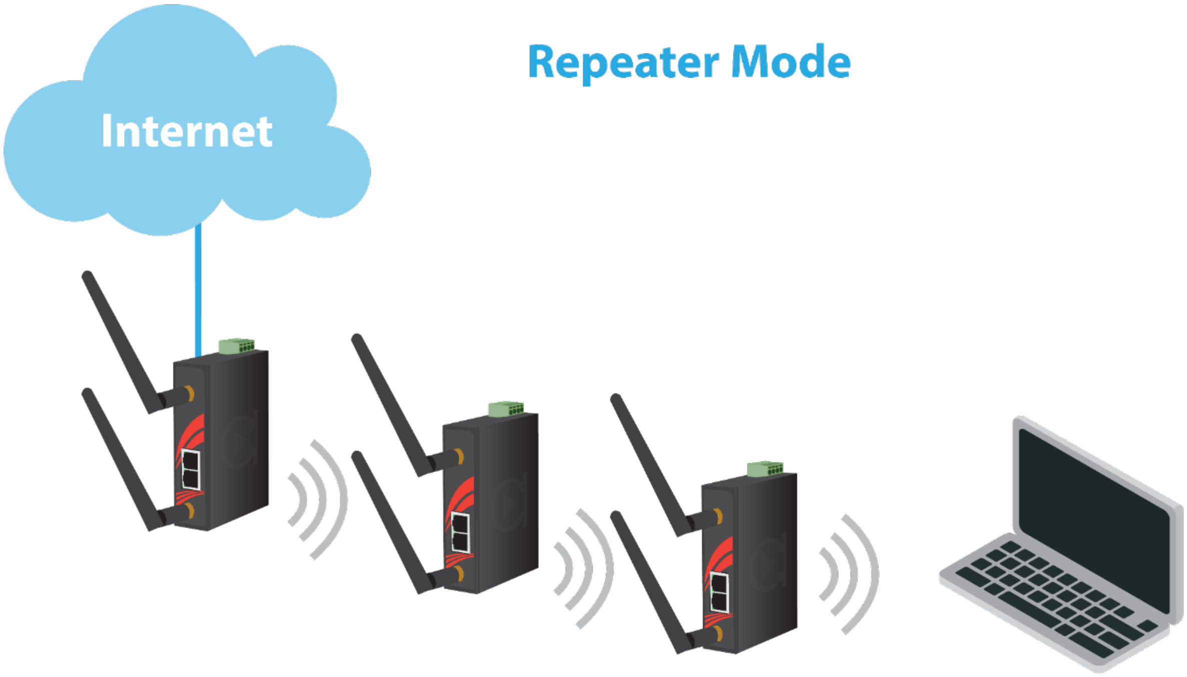
1.2.5 WDS Station/WDS Access Point

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.



1.2.6 Repeater Mode

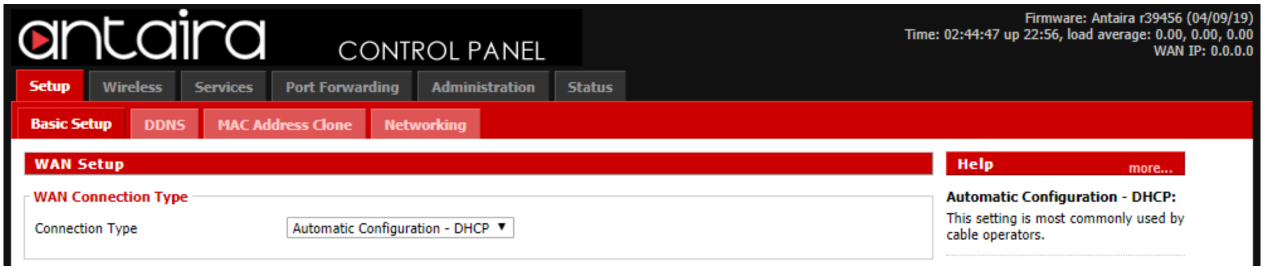
In Repeater Mode, the access point will act as a relay for another wireless signal. Repeater Mode takes an existing signal from a wireless AP or wireless router and rebroadcasts it. This mode is beneficial for extending the wireless range and coverage. The drawback is that the re-transmitted signal throughput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



Firmware: Antaira r39456 (04/09/19)
Time: 02:44:47 up 22:56, load average: 0.00, 0.00, 0.00
WAN IP: 0.0.0.0

WAN Setup

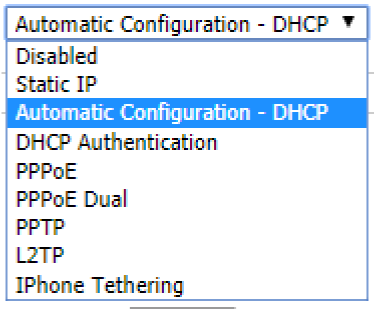
WAN Connection Type

Connection Type: Automatic Configuration - DHCP

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

Setup > Basic Setup

2.1.1 WAN Setup

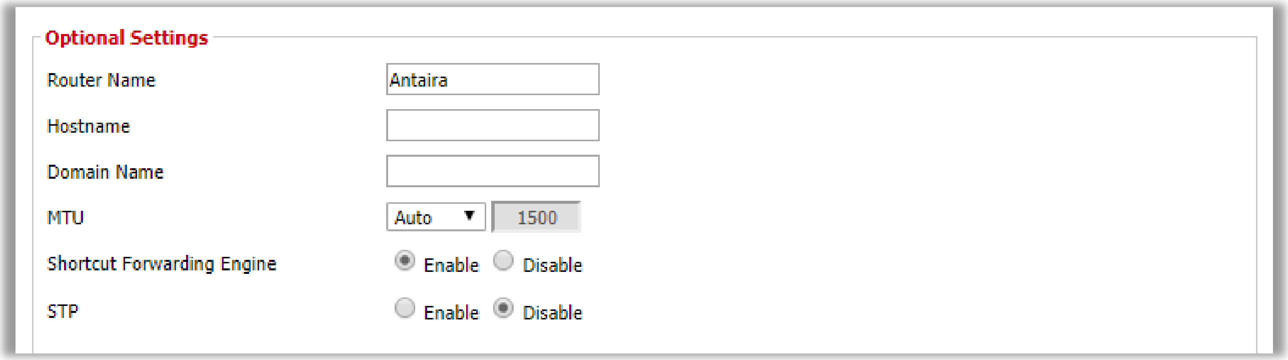


Automatic Configuration - DHCP ▼
Disabled
Static IP
Automatic Configuration - DHCP
DHCP Authentication
PPPoE
PPPoE Dual
PPTP
L2TP
IPhone Tethering

Setup > Basic Setup > WAN Setup

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

2.1.2 Optional Settings



Optional Settings

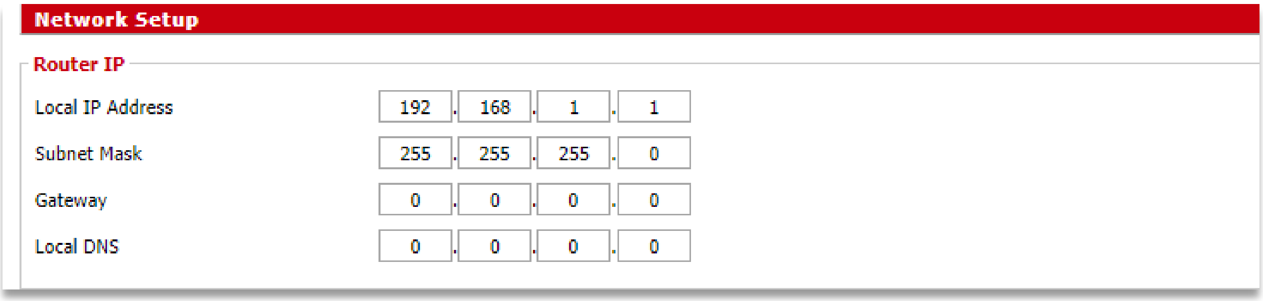
Router Name	Antaira
Hostname	
Domain Name	
MTU	Auto ▼ 1500
Shortcut Forwarding Engine	● Enable ○ Disable
STP	○ Enable ● Disable

Setup > Basic Setup > Optional Settings

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

2.1.3 Router IP

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



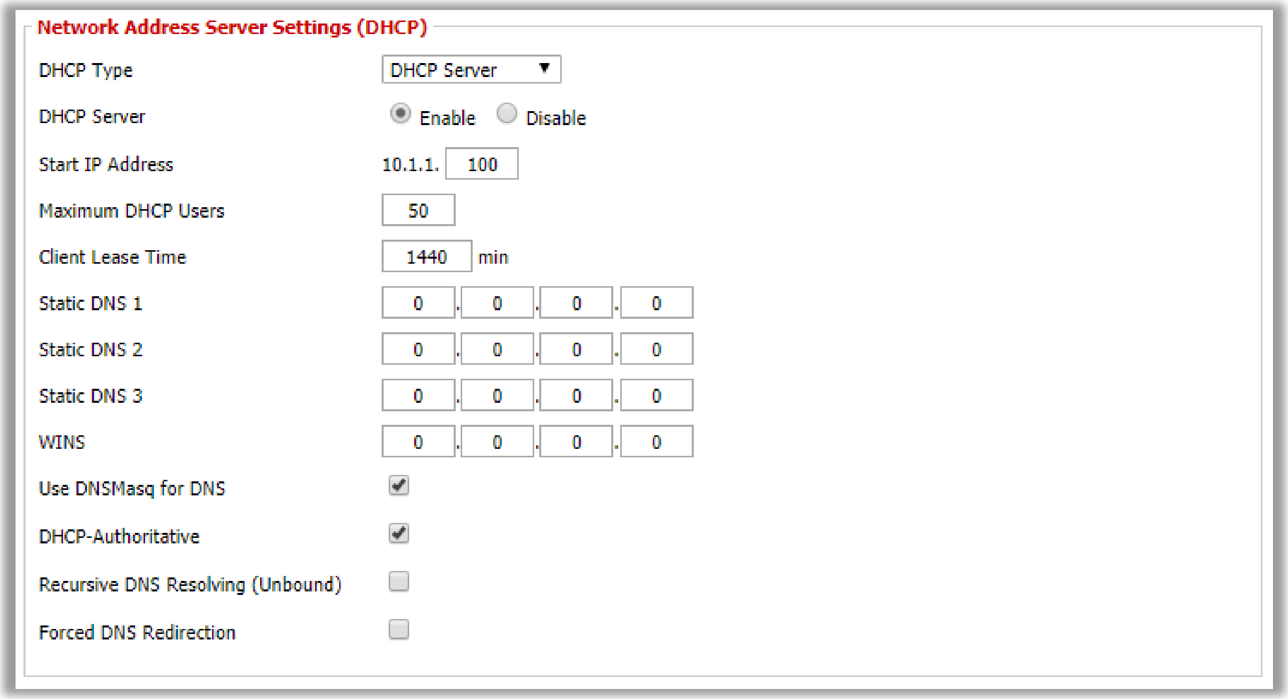
Network Setup

Router IP

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

Setup > Basic Setup > Network Setup

2.1.4 Network Address Server Settings (DHCP)



Network Address Server Settings (DHCP)

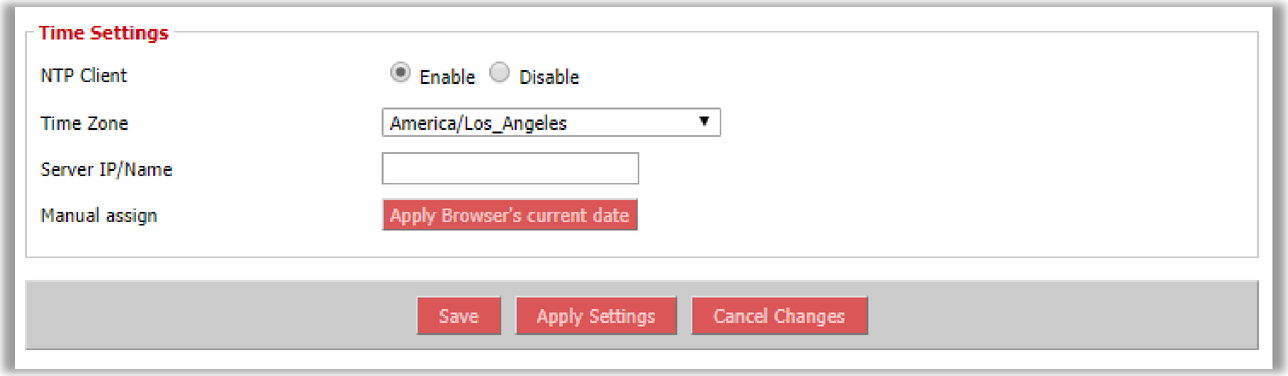
DHCP Type	DHCP Server ▼
DHCP Server	● Enable ○ Disable
Start IP Address	10.1.1. 100
Maximum DHCP Users	50
Client Lease Time	1440 min
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
WINS	0 . 0 . 0 . 0
Use DNSMasq for DNS	☑
DHCP-Authoritative	☑
Recursive DNS Resolving (Unbound)	□
Forced DNS Redirection	□

Setup > Basic Setup > Network Address Server Settings

Network Address Server Settings	Description
DHCP Type	**Server:** This device will function as the DHCP server. If there is already a DHCP server on the network, select **Disable**. **Forwarder:** Additional routers can be hardwired to the main router on the network. The additional routers will have the type set as Forwarder. Any devices connected to the additional routers will receive their DHCP information from the main router.
DHCP Server	**Enable** if you want this router to provide DHCP addressing. Disable if there is an existing DHCP server on the network.
Start IP Address	A numerical value for the DHCP server to start its addressing with when assigning IP addresses. ****Do not start with the routers IP address. ****
Maximum DHCP Users	The maximum number of devices the router will assign IP address through DHCP.

Client Lease Time	The lease time of an IP address given by the DHCP server before it expires.
Static DNS #	The Domain Name System is how domain names are translated to IP addresses. The ISP provider will typically provide at least one unique DNS IP address.
WINS	Windows Internet Naming Services: Manages the PC’s interaction with the Internet.

2.1.5 Time Settings



Time Settings

NTP Client ● Enable ○ Disable

Time Zone America/Los_Angeles

Server IP/Name

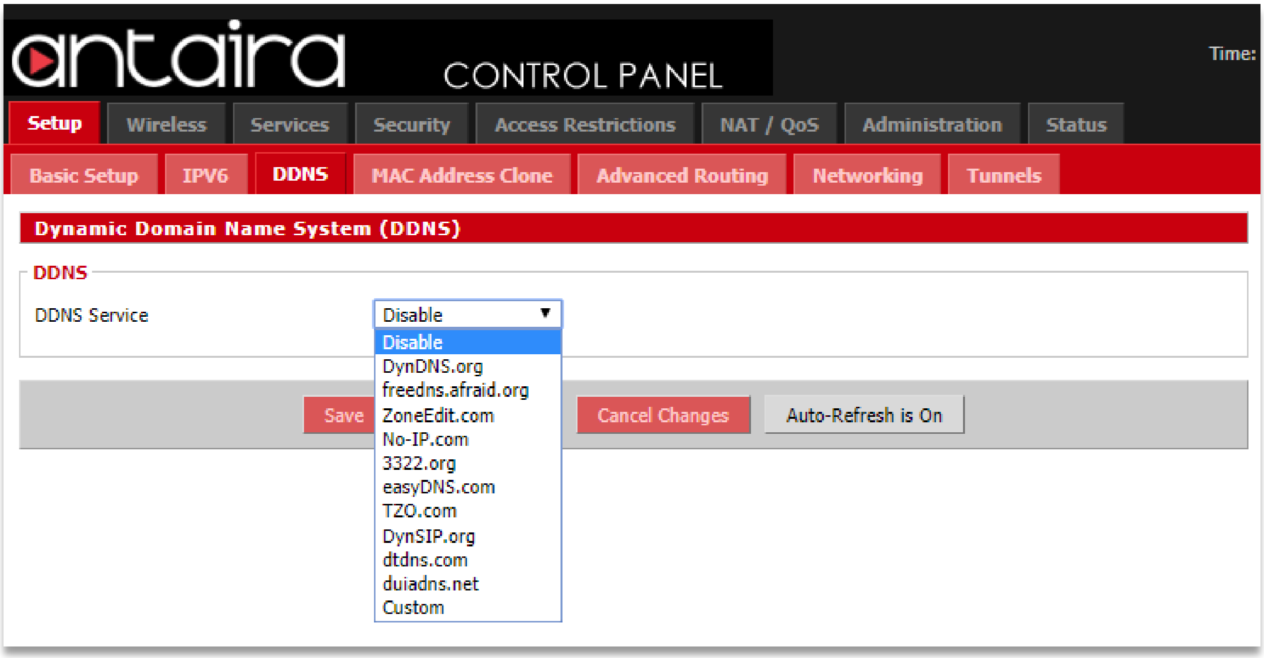
Manual assign

Setup > Basic Setup > Time Settings

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

2.2 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.



Dynamic Domain Name System (DDNS)

DDNS

DDNS Service: Disable

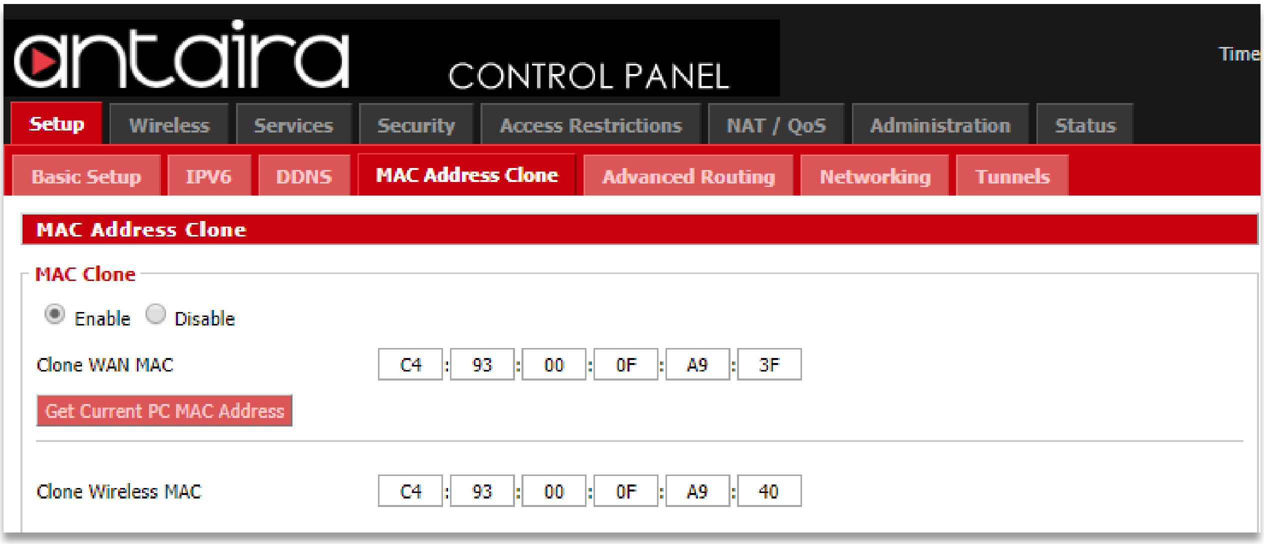
Disable
DynDNS.org
freedns.afraid.org
ZoneEdit.com
No-IP.com
3322.org
easyDNS.com
TZO.com
DynSIP.org
dtdns.com
duiadns.net
Custom

Setup > DDNS

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

2.3 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.



MAC Address Clone

MAC Clone

● Enable ○ Disable

Clone WAN MAC C4 : 93 : 00 : 0F : A9 : 3F

Clone Wireless MAC C4 : 93 : 00 : 0F : A9 : 40

Setup > MAC Address Clone

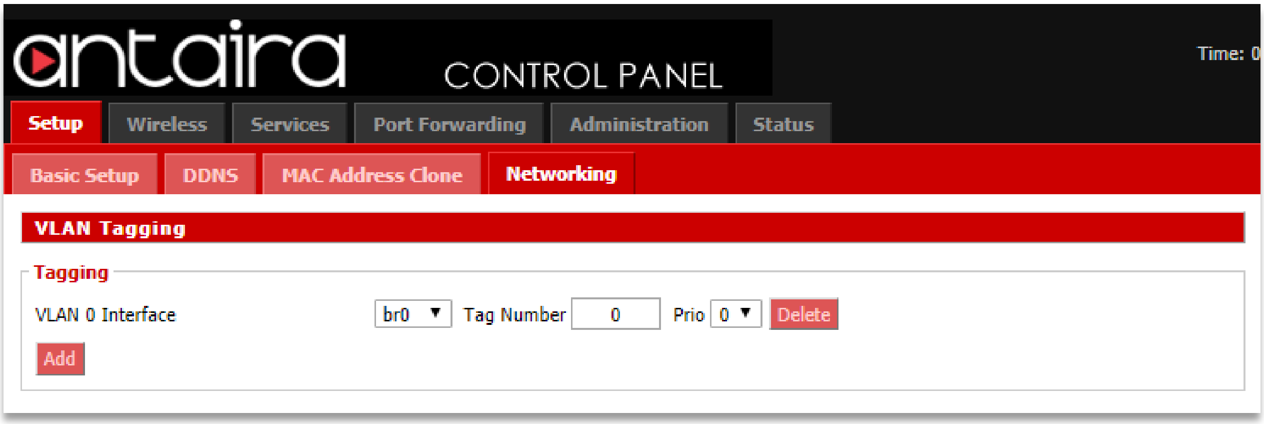
Enter the MAC address of the network adapter in the **Clone WAN MAC** section or click the **Get Current PC MAC Address** to fill in the MAC address of the PC currently connected. Get Current PC Mac is typically used when establishing a service with certain ISP providers.

2.4 Networking

2.4.1 VLAN Tagging

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

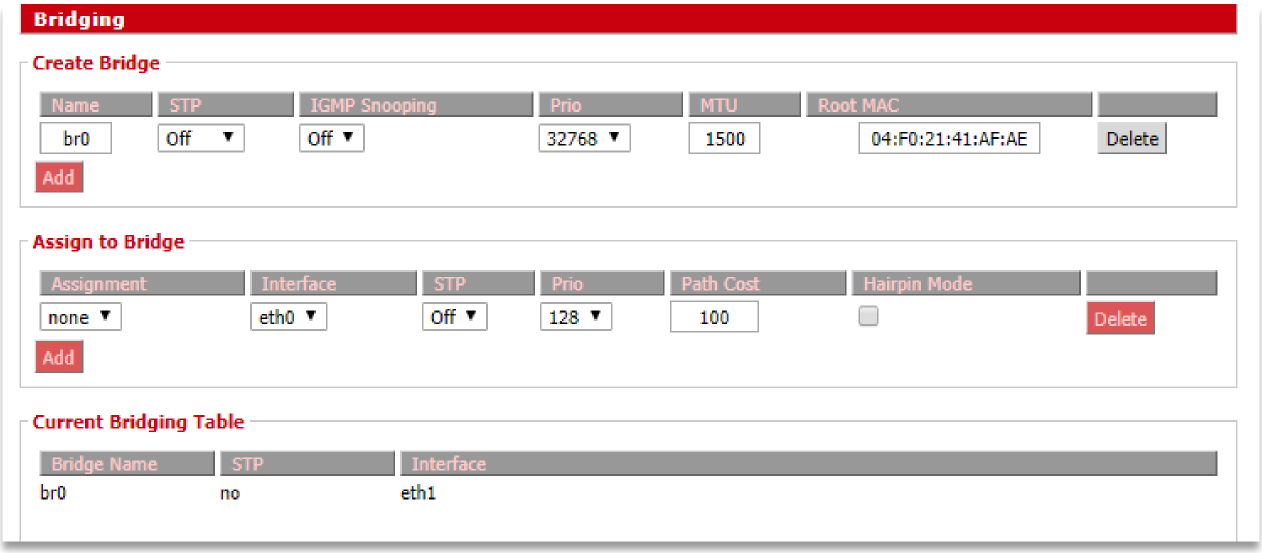
Tagging: Allows you to create a new VLAN interface out of a standard interface by filtering the interface using a defined TAG number.



VLAN 0 Interface br0 Tag Number 0 Prio 0

Setup > Networking > VLAN Tagging

2.4.2 Bridging



Bridging

Create Bridge

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

Assign to Bridge

Assignment	Interface	STP	Prio	Path Cost	Hairpin Mode	
none ▼	eth0 ▼	Off ▼	128 ▼	100	□	Delete

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 it the Bridging section of the networking tab.

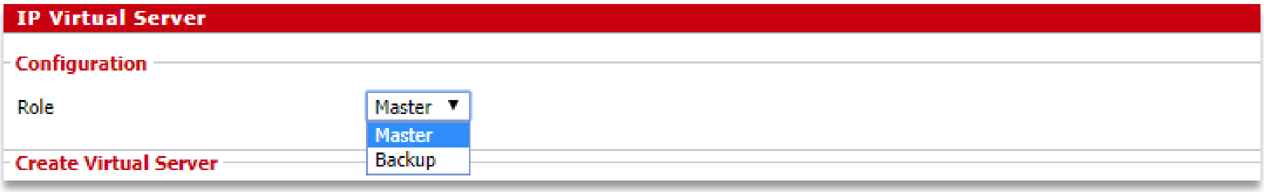
Create Bridge	Description
Add	Create a new network bridge.
STP	Spanning Tree Protocol. Turn on or off.
IGMP Snooping	Turn on or off IGMP Snooping.
Prio	Sets the bridge priority order. (Lower numbers are higher priority.)
MTU	Maximum Transmission Unit: Specifies the largest packet size permitted for Internet transmission. Auto will allow the device to select the best MTU for Internet connection. Manual values entered should be in the range 1200 – 1500.
Root MAC	The Root MAC address.

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

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

Path Cost	Set the path cost.
Hairpin Mode	Enables Hairpin routing.

2.4.3 IP Virtual Server



IP Virtual Server

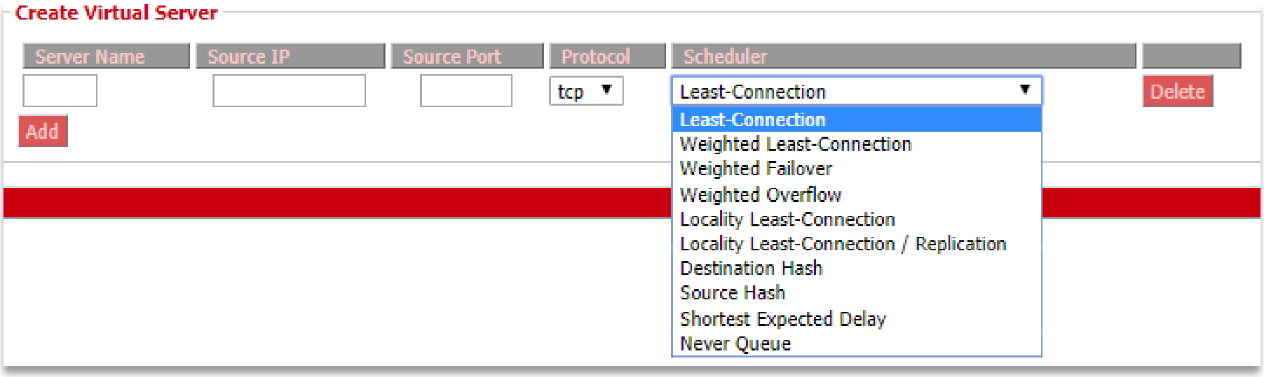
Configuration

Role: Master

Setup > Networking > IP Virtual Server

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

2.4.4 Create Virtual Server



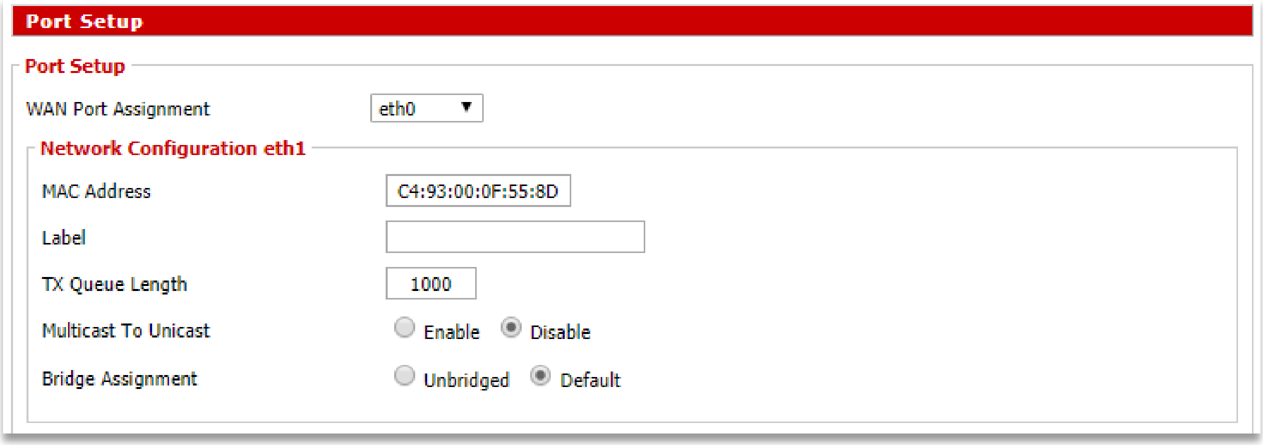
Create Virtual Server

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

Setup > Networking > Create Virtual Server

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

2.4.5 Port Setup



Port Setup

Port Setup

WAN Port Assignment: eth0

Network Configuration eth1

MAC Address: C4:93:00:0F:55:8D

Label:

TX Queue Length: 1000

Multicast To Unicast: ○ Enable ● Disable

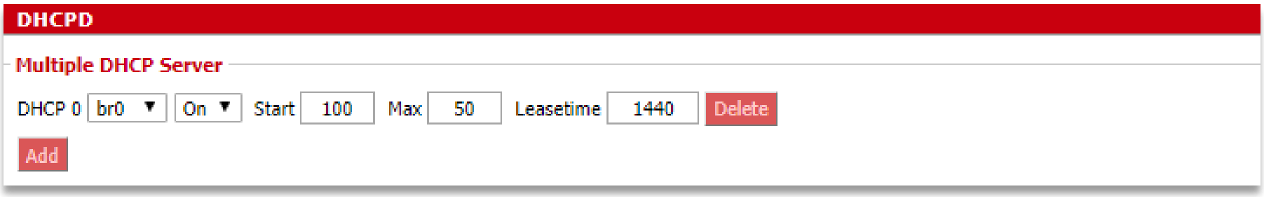
Bridge Assignment: ○ Unbridged ● Default

Setup > Networking > Port Setup

Port Setup	Description
WAN Port Assignment	Select a WAN Port.
MAC Address	MAC Address of the configured WAN port.
Label	Input a label if desired.
TX Queue Length	Set the TX-queue length.
Bridge Assignment	Select the bridge assignment: Unbridged or Default.

2.4.6 DHCPD

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



DHCPD

Multiple DHCP Server

DHCP 0 br0 On Start 100 Max 50 Leasetime 1440 Delete

Add

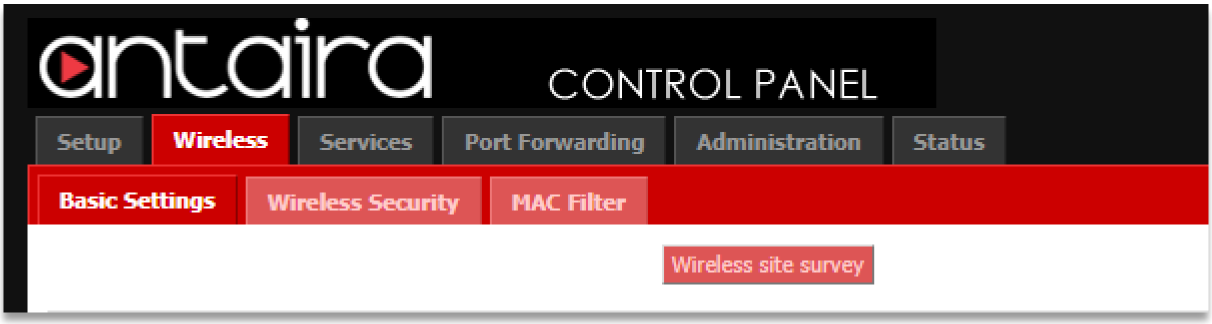
Setup > Networking > DHCPD

3. Wireless

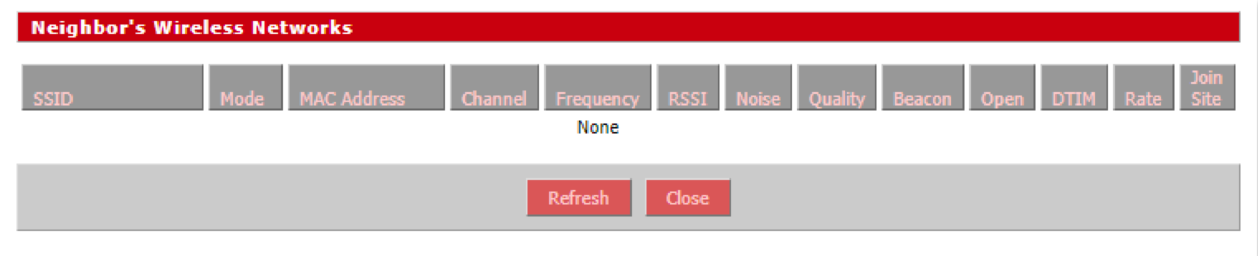
3.1 Basic Settings

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

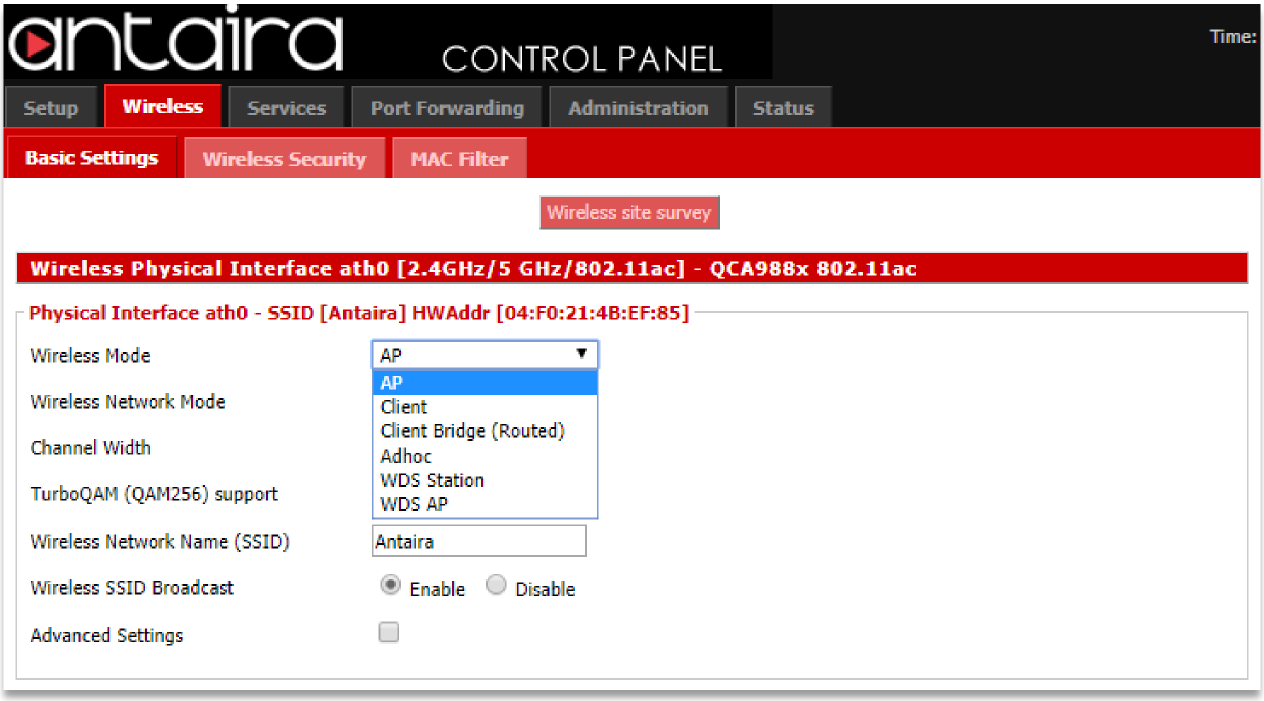


Neighbor's Wireless Networks

SSID	Mode	MAC Address	Channel	Frequency	RSSI	Noise	Quality	Beacon	Open	DTIM	Rate	Join Site
				None								

Wireless > Basic Settings > Wireless Site Survey

3.1.2 Wireless Mode



Wireless Physical Interface ath0 [2.4GHz/5 GHz/802.11ac] - QCA988x 802.11ac

Physical Interface ath0 - SSID [Antaira] HWAddr [04:F0:21:4B:EF:85]

Wireless Mode: AP

Wireless Network Mode

Channel Width

TurboQAM (QAM256) support

Wireless Network Name (SSID): Antaira

Wireless SSID Broadcast: ● Enable ○ Disable

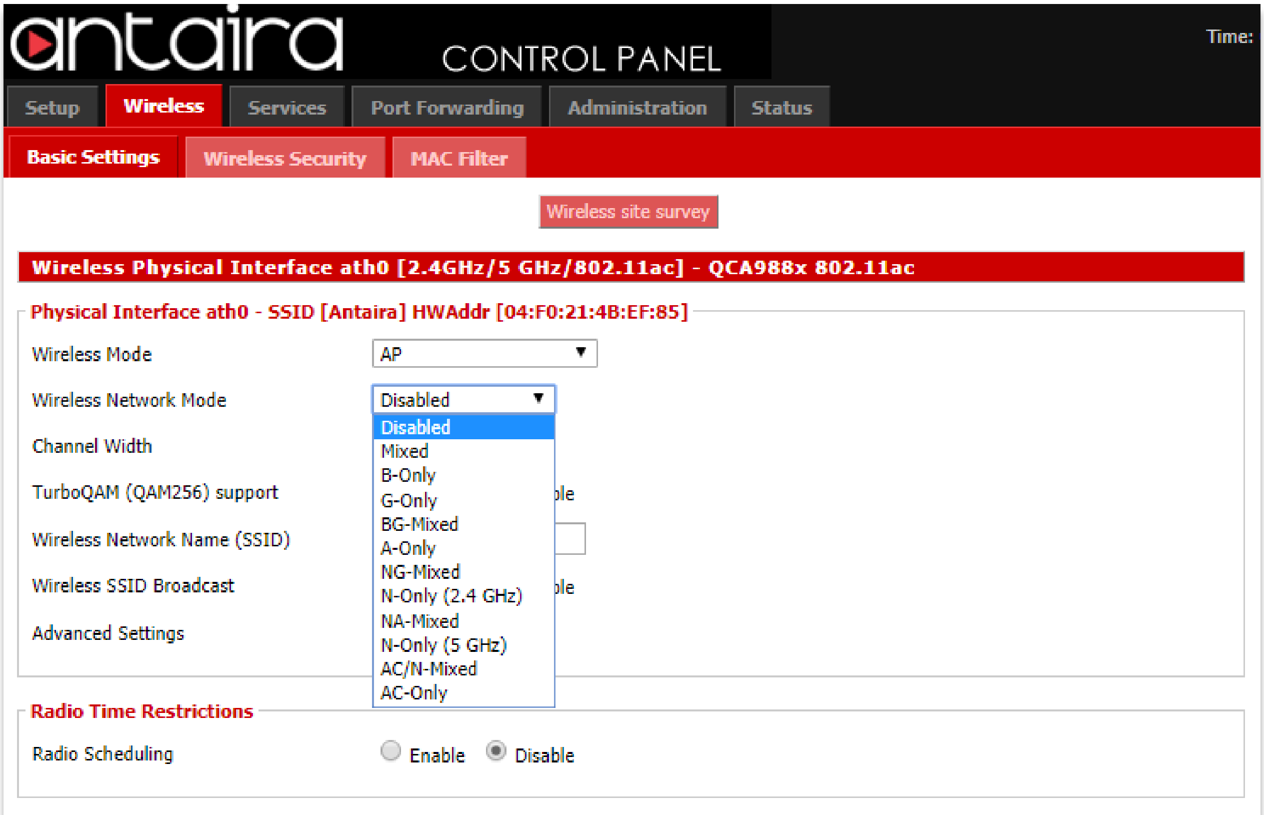
Advanced Settings: □

Wireless > Basic Settings > Wireless Mode

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

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

3.1.3 Wireless Network Mode



Wireless Physical Interface ath0 [2.4GHz/5 GHz/802.11ac] - QCA988x 802.11ac

Physical Interface ath0 - SSID [Antaira] HWAddr [04:F0:21:4B:EF:85]

Wireless Mode: AP

Wireless Network Mode: Disabled

Radio Time Restrictions

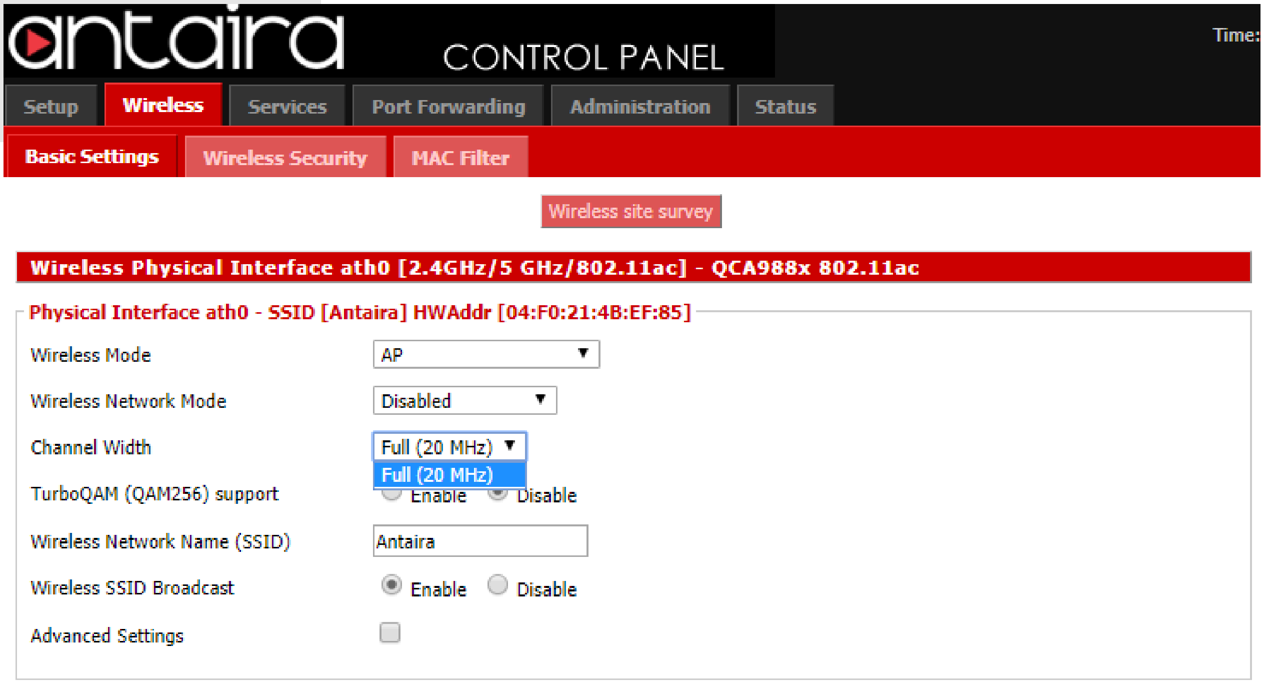
Radio Scheduling: ○ Enable ● Disable

Wireless > Basic Settings > Wireless Network Mode

Basic Settings	Description
Wireless Network Mode	**Disabled:** Disables the wireless network mode.
	Mixed: If you have mixed b/g/n devices on your network.
	B-Only: IEEE 802.11b allows a maximum data rate of 11Mbits/s through 2.4GHz wireless connections. If only B-type wireless devices are on the network, use this mode.
	G-Only: IEEE 802.11g allows a maximum data rate of 54Mbits/s through 2.4GHz wireless connections. If only G-type wireless devices are on the network, use this mode.
	BG-Mixed: If B and G-type wireless devices are on the network, use this mode.
	A-Only: IEEE 802.11a allows a maximum data rate of 54Mbits/s through 5GHz wireless connections. If only A-

	type devices are on the network, use this mode**.**
	NG-Mixed: Mix band of 802.11b/g/b modes.
	N-Only (2.4GHz): N-Only wireless network mode.
	NA-Mixed: Mix band of 802.11n/a modes.
	N-Only (5GHz): Improved throughput for 5GHz devices.
	AC/N-Mixed: Mix band of 802.11ac/n modes.
	AC-Only: AC-Only wireless network mode.

3.1.4 Channel Width



Wireless Physical Interface ath0 [2.4GHz/5 GHz/802.11ac] - QCA988x 802.11ac

Physical Interface ath0 - SSID [Antaira] HWAddr [04:F0:21:4B:EF:85]

Wireless Mode	AP
Wireless Network Mode	Disabled
Channel Width	Full (20 MHz)
TurboQAM (QAM256) support	○ Enable ● Disable
Wireless Network Name (SSID)	Antaira
Wireless SSID Broadcast	● Enable ○ Disable
Advanced Settings	□

Wireless > Basic Settings > Channel Width

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

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

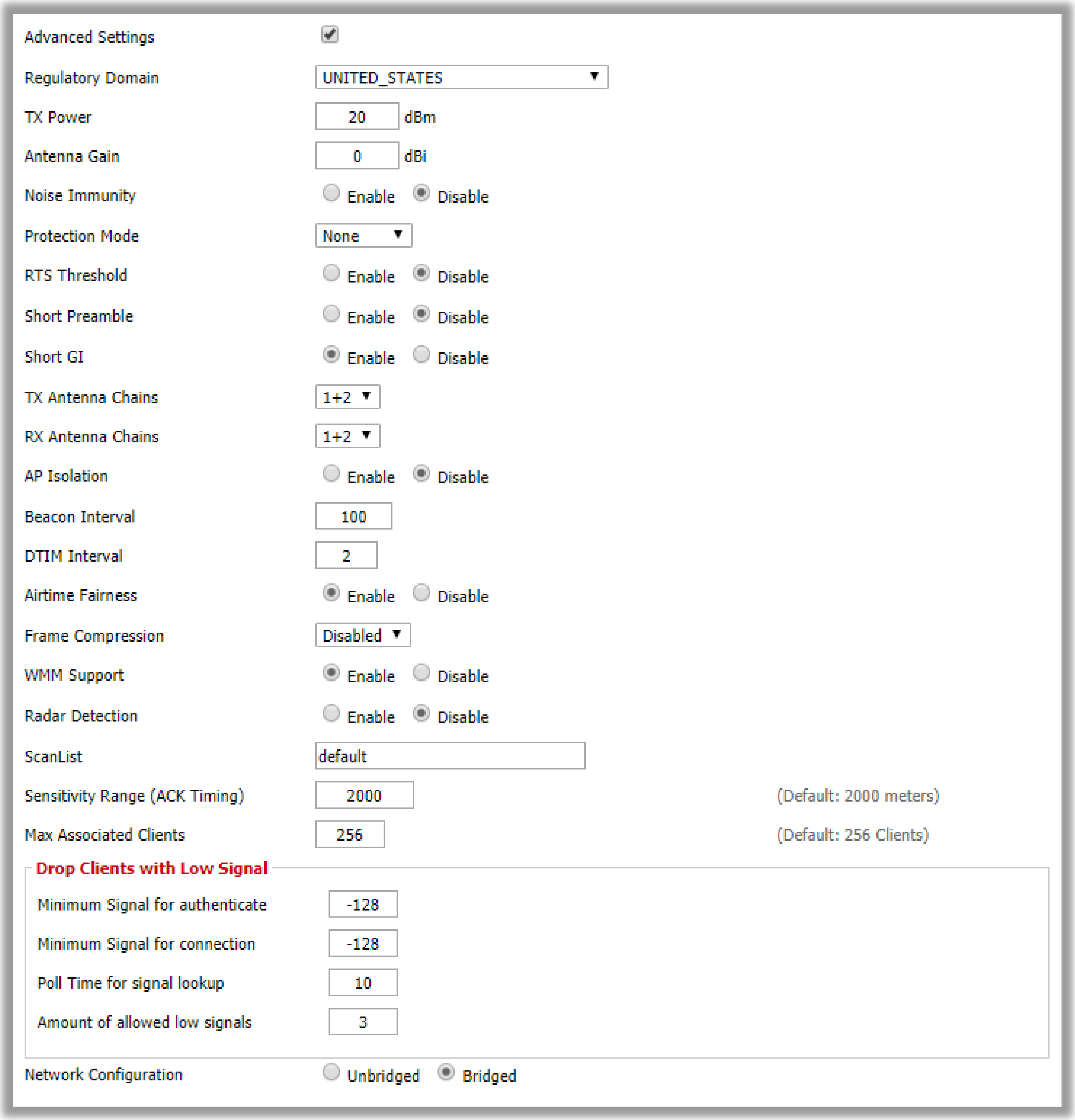
3.1.5 Wireless Network Name (SSID)

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

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

3.1.6 Advanced Settings

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



Advanced Settings	☑	
Regulatory Domain	UNITED_STATES ▼	
TX Power	20 dBm	
Antenna Gain	0 dBi	
Noise Immunity	○ Enable ● Disable	
Protection Mode	None ▼	
RTS Threshold	○ Enable ● Disable	
Short Preamble	○ Enable ● Disable	
Short GI	● Enable ○ Disable	
TX Antenna Chains	1+2 ▼	
RX Antenna Chains	1+2 ▼	
AP Isolation	○ Enable ● Disable	
Beacon Interval	100	
DTIM Interval	2	
Airtime Fairness	● Enable ○ Disable	
Frame Compression	Disabled ▼	
WMM Support	● Enable ○ Disable	
Radar Detection	○ Enable ● Disable	
ScanList	default	
Sensitivity Range (ACK Timing)	2000	(Default: 2000 meters)
Max Associated Clients	256	(Default: 256 Clients)

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

Network Configuration	○ Unbridged ● Bridged

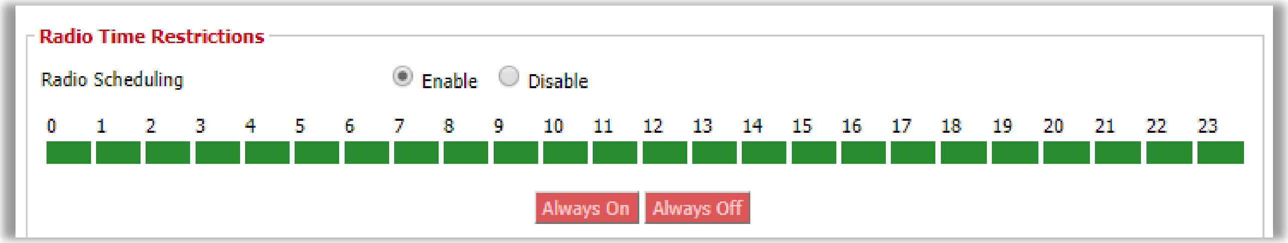
Wireless > Basic Settings > Advanced Settings

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

Noise Immunity	Enable or disable this feature.
Protection Mode	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.
RTS Threshold	Specifies the maximum size for a packet before data is fragmented into multiple packets.
Short Preamble	Default is Long Preamble. A short preamble can be used but communication issues might occur when communicating with IEEE 802.11b devices.
Short GI	Enable or disable this feature.
TX Antenna Chains	Used based on external antennas to provide optimum performance.
RX Antenna Chains	Used based on external antennas to provide optimum performance.
AP Isolation	Disabled by default. If enabled, wireless clients are isolated and access to and from other wireless clients is stopped.
Beacon Interval	Set the beacon interval.
DTIM Interval	Set the STIM interval.
Airtime Fairness	Enable or disable this feature.
Frame Compression	Enable or disable this feature.
WMM Support	Enable or disable this feature.
Radar Detection	Looks for airport or military pulses from radars to prevent unintended interference between equipment.
ScanList	
Sensitivity Range (ACK Timing)	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.
Max Associated Clients	Number of clients that can be connected to the access point.
Minimum Signal for Authenticate	Set the minimum signal for authentication.
Minimum Signal for	Set the minimum signal for connection.

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

3.1.7 Radio Time Restrictions



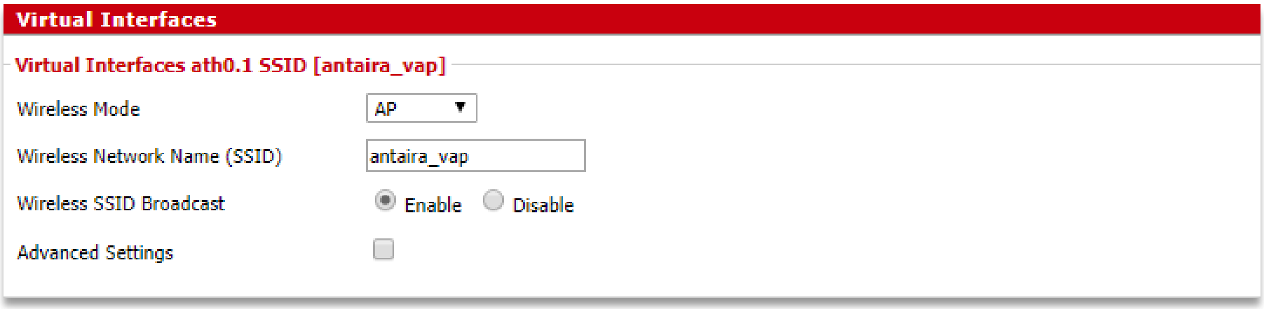
Radio Time Restrictions

Radio Scheduling ● Enable ○ Disable

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Wireless > Basic Settings > Radio Time Restrictions

3.1.8 Virtual Interfaces



Virtual Interfaces

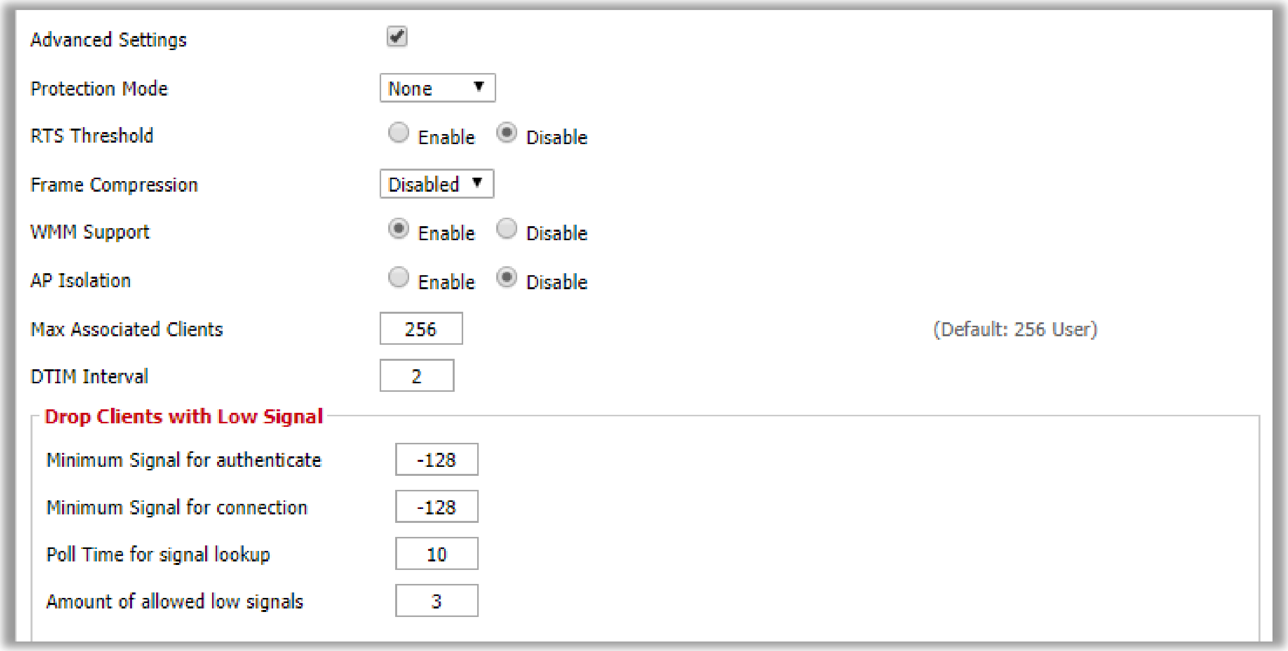
Virtual Interfaces ath0.1 SSID [antaira_vap]

Wireless Mode	AP ▼
Wireless Network Name (SSID)	antaira_vap
Wireless SSID Broadcast	● Enable ○ Disable
Advanced Settings	□

Wireless > Basic Settings > Virtual Interfaces

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

3.1.9 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	

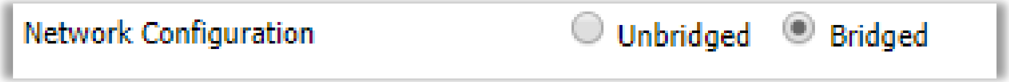
Drop Clients with Low Signal

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



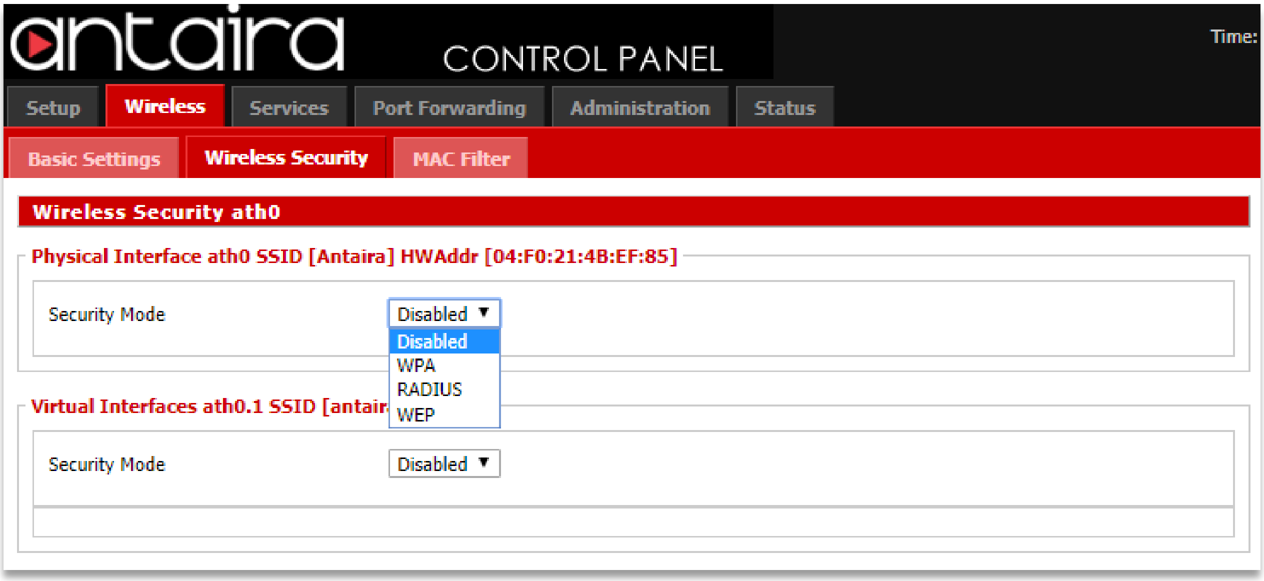
Network Configuration ○ Unbridged ● Bridged

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

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

3.2 Wireless Security

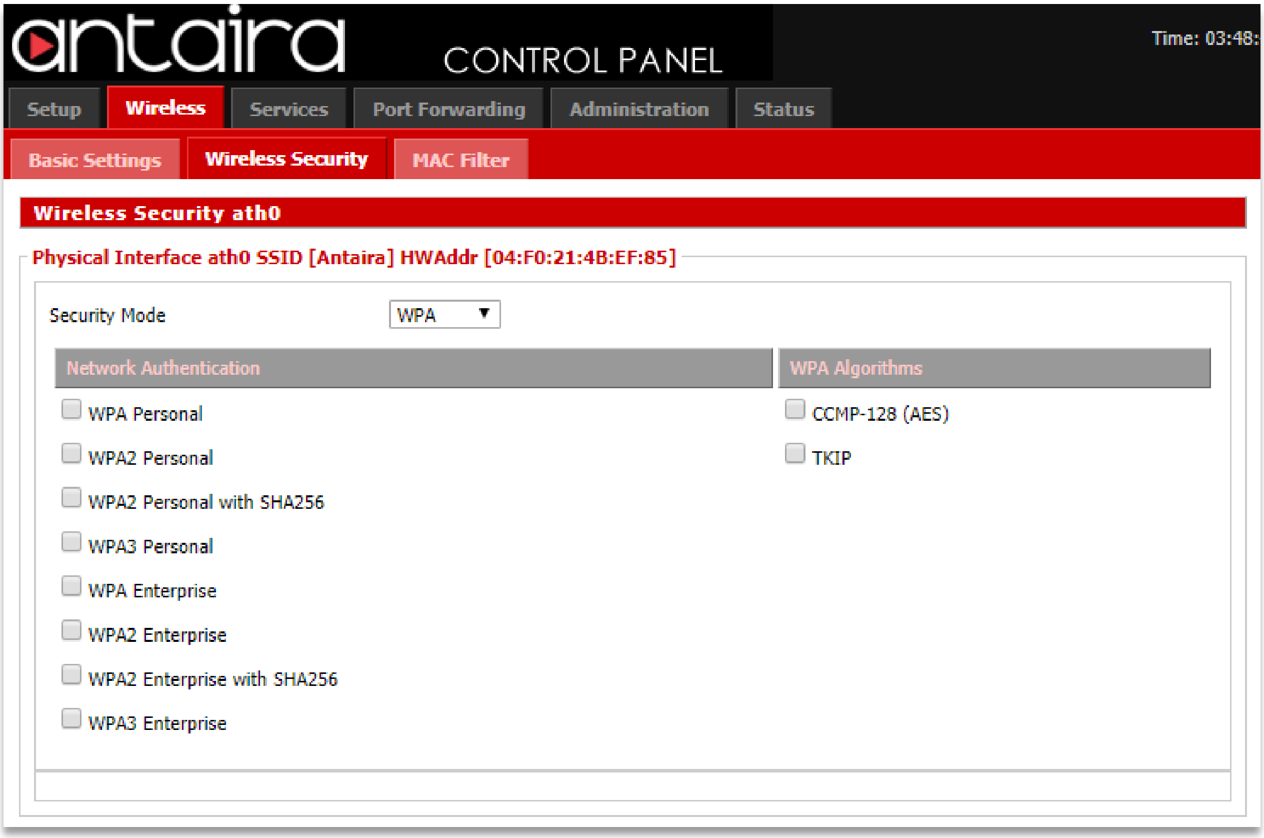
The Antaira router supports different types of security settings for your network: WiFi Protected Access (WPA), WPA2, WPA3, Remote Access Dial In User Service (RADIUS), and Wires Equivalent Privacy (WEP), which can be selected from the list next to Security Mode. To disable security settings, select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



Wireless > Wireless Security > Security Mode

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

3.2.1 WPA



Wireless Security ath0

Physical Interface ath0 SSID [Antaira] HWAddr [04:F0:21:4B:EF:85]

Security Mode: WPA

Network Authentication	WPA Algorithms
□ WPA Personal	□ CCMP-128 (AES)
□ WPA2 Personal	□ TKIP
□ WPA2 Personal with SHA256	
□ WPA3 Personal	
□ WPA Enterprise	
□ WPA2 Enterprise	
□ WPA2 Enterprise with SHA256	
□ WPA3 Enterprise	

Wireless > Wireless Security > Security Mode > WPA

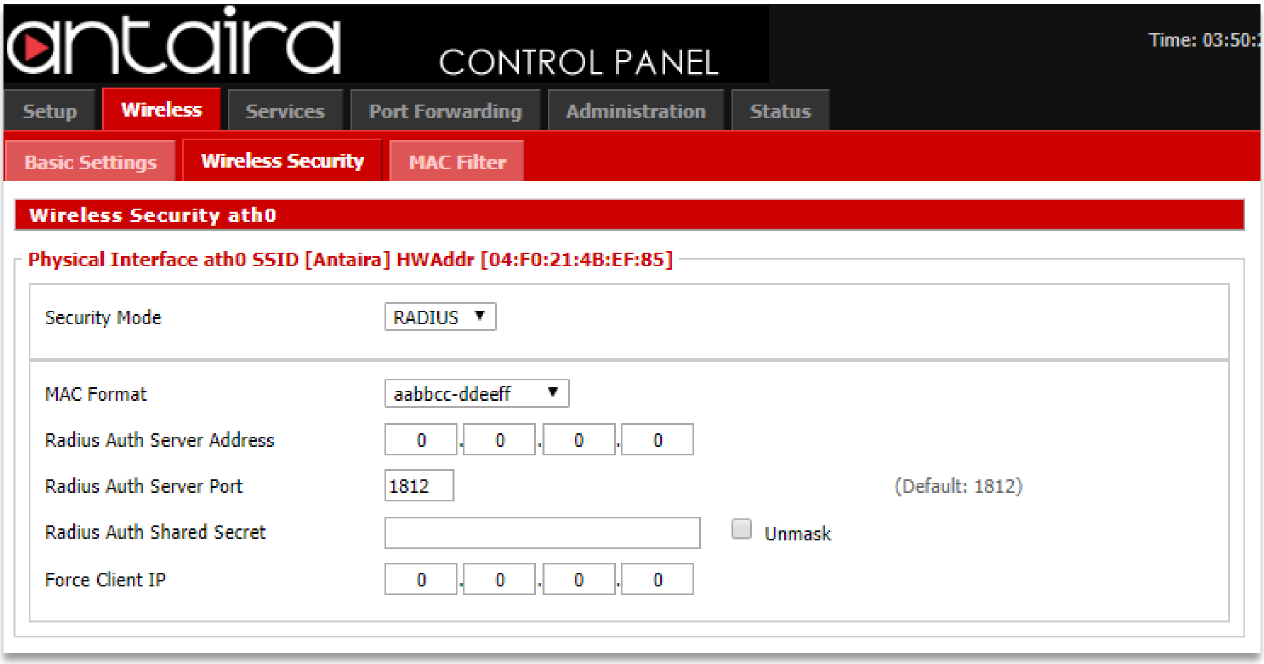
Wireless Security	Description
Network Authentication	Choose the network authentication method.

WPA Algorithms

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

3.2.2 RADIUS

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



Wireless Security ath0

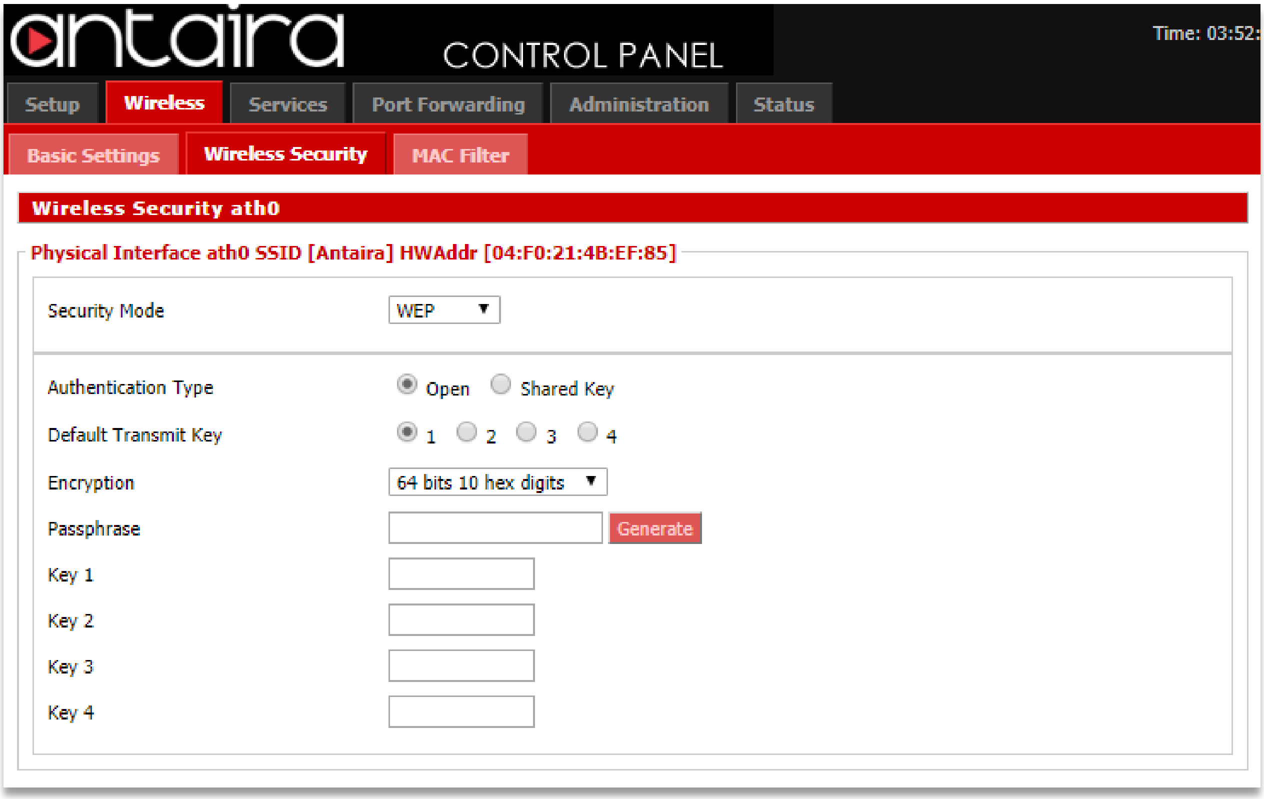
Physical Interface ath0 SSID [Antaira] HWAddr [04:F0:21:4B:EF:85]

Security Mode	RADIUS
MAC Format	aabbcc-ddeeff
Radius Auth Server Address	0 . 0 . 0 . 0
Radius Auth Server Port	1812 (Default: 1812)
Radius Auth Shared Secret	□ Unmask
Force Client IP	0 . 0 . 0 . 0

Wireless > Wireless Security > Security Mode > RADIUS

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

3.2.3 WEP



Wireless Security ath0

Physical Interface ath0 SSID [Antaira] HWAddr [04:F0:21:4B:EF:85]

Security Mode: WEP

Authentication Type: ● Open ○ Shared Key

Default Transmit Key: ● 1 ○ 2 ○ 3 ○ 4

Encryption: 64 bits 10 hex digits

Passphrase:

Key 1:

Key 2:

Key 3:

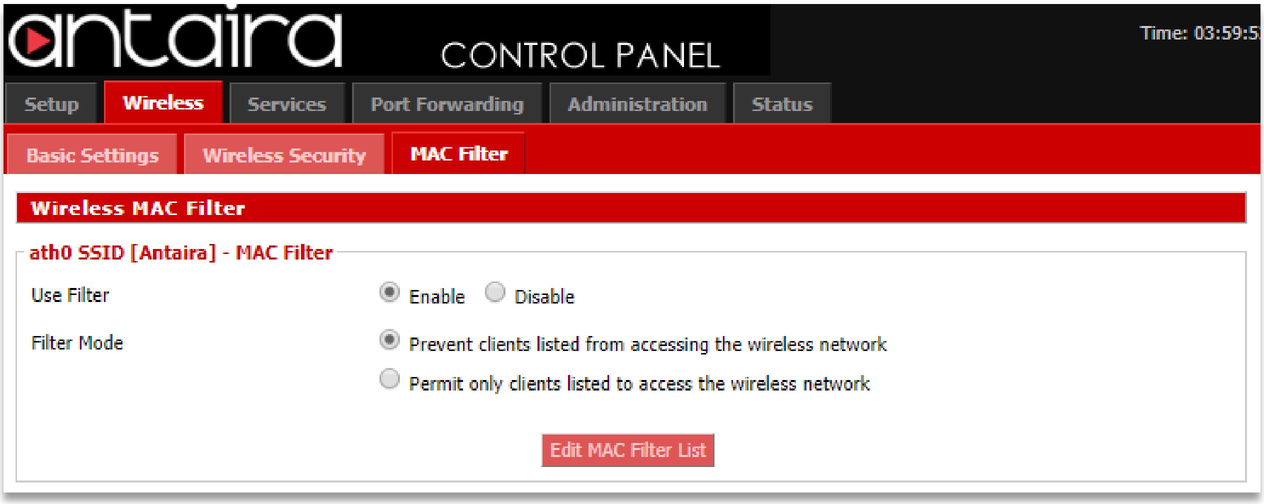
Key 4:

Wireless > Wireless Security > Security Mode > WEP

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

3.3 MAC Filter

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



Wireless MAC Filter

ath0 SSID [Antaira] - MAC Filter

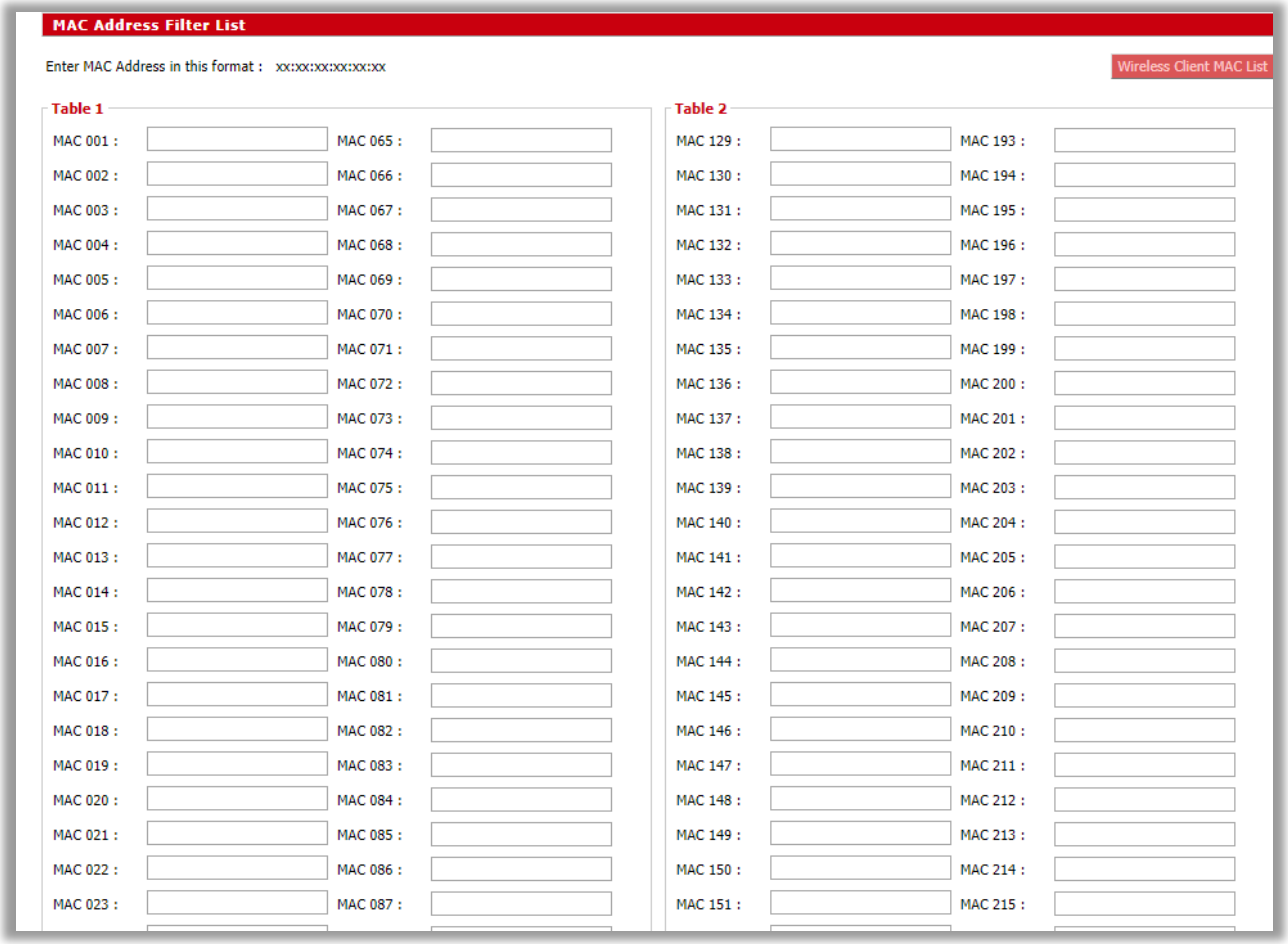
Use Filter ● Enable ○ Disable

Filter Mode ● Prevent clients listed from accessing the wireless network
○ Permit only clients listed to access the wireless network

Wireless > MAC Filter

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

3.3.1 Edit MAC Filter List



MAC Address Filter List

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

Table 1

MAC 001 :		MAC 065 :	
MAC 002 :		MAC 066 :	
MAC 003 :		MAC 067 :	
MAC 004 :		MAC 068 :	
MAC 005 :		MAC 069 :	
MAC 006 :		MAC 070 :	
MAC 007 :		MAC 071 :	
MAC 008 :		MAC 072 :	
MAC 009 :		MAC 073 :	
MAC 010 :		MAC 074 :	
MAC 011 :		MAC 075 :	
MAC 012 :		MAC 076 :	
MAC 013 :		MAC 077 :	
MAC 014 :		MAC 078 :	
MAC 015 :		MAC 079 :	
MAC 016 :		MAC 080 :	
MAC 017 :		MAC 081 :	
MAC 018 :		MAC 082 :	
MAC 019 :		MAC 083 :	
MAC 020 :		MAC 084 :	
MAC 021 :		MAC 085 :	
MAC 022 :		MAC 086 :	
MAC 023 :		MAC 087 :	

Table 2

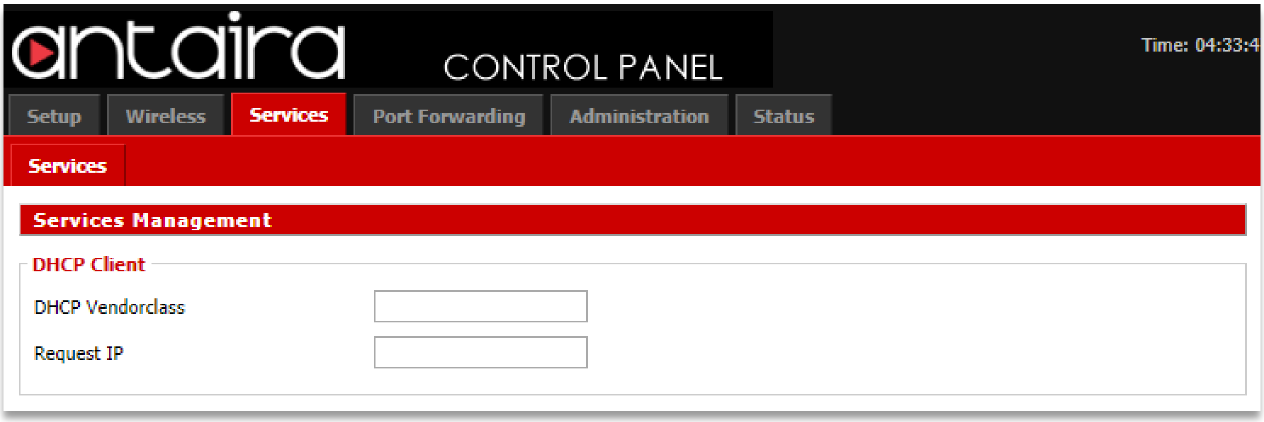
MAC 129 :		MAC 193 :	
MAC 130 :		MAC 194 :	
MAC 131 :		MAC 195 :	
MAC 132 :		MAC 196 :	
MAC 133 :		MAC 197 :	
MAC 134 :		MAC 198 :	
MAC 135 :		MAC 199 :	
MAC 136 :		MAC 200 :	
MAC 137 :		MAC 201 :	
MAC 138 :		MAC 202 :	
MAC 139 :		MAC 203 :	
MAC 140 :		MAC 204 :	
MAC 141 :		MAC 205 :	
MAC 142 :		MAC 206 :	
MAC 143 :		MAC 207 :	
MAC 144 :		MAC 208 :	
MAC 145 :		MAC 209 :	
MAC 146 :		MAC 210 :	
MAC 147 :		MAC 211 :	
MAC 148 :		MAC 212 :	
MAC 149 :		MAC 213 :	
MAC 150 :		MAC 214 :	
MAC 151 :		MAC 215 :	

Wireless > MAC Filter > Edit MAC Filter List

4. Services

4.1 Services

4.1.1 DHCP Client



Services Management

DHCP Client

DHCP Vendorclass

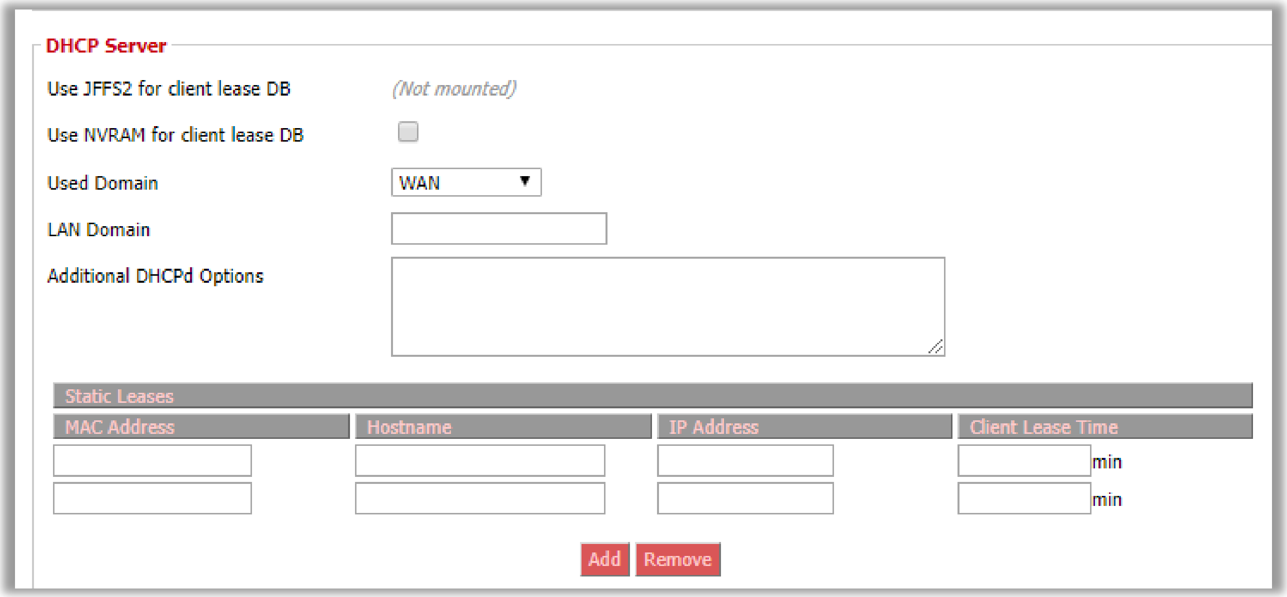
Request IP

Services > Services > DHCP Client

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

4.1.2 DHCP Server

A DHCP server assigns IP addresses to your local devices.



DHCP Server

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

Use NVRAM for client lease DB □

Used Domain WAN

LAN Domain

Additional DHCPd Options

Static Leases

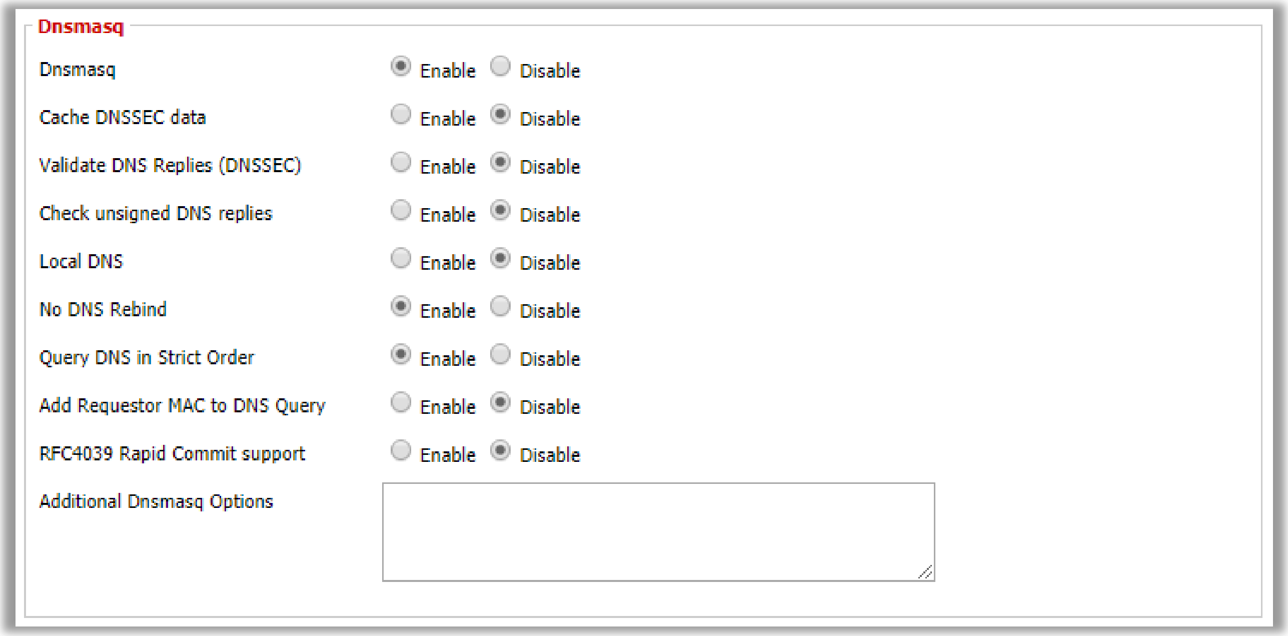
MAC Address	Hostname	IP Address	Client Lease Time
			min
			min

Services > Services > DHCP Server

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

4.1.3 Dnsmasq

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



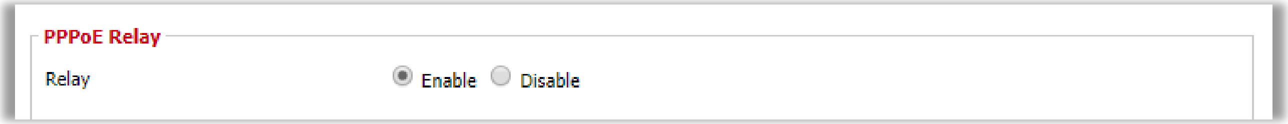
Dnsmasq

Dnsmasq	● Enable ○ Disable
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
RFC4039 Rapid Commit support	○ Enable ● Disable
Additional Dnsmasq Options	

Services > Services > Dnsmasq

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

4.1.4 PPPoE Relay

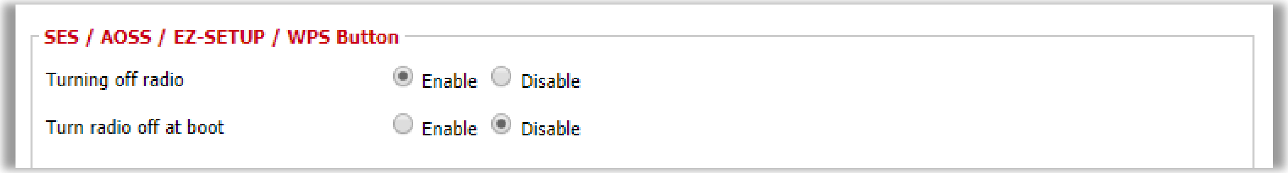


PPPoE Relay

Relay ● Enable ○ Disable

Services > Services > PPPoE Relay

4.1.5 SES/AOSS/EZ-SETUP/WPS Button



SES / AOSS / EZ-SETUP / WPS Button

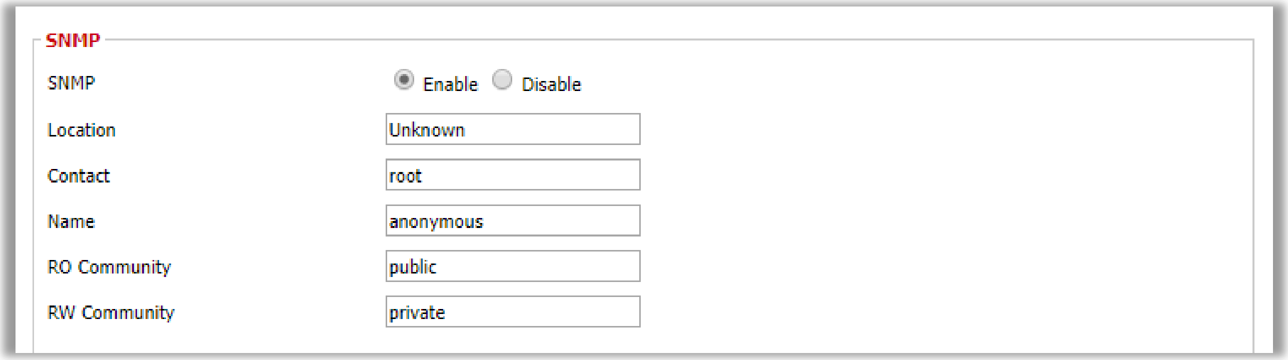
Turning off radio ● Enable ○ Disable

Turn radio off at boot ○ Enable ● Disable

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

4.1.6 SNMP

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



SNMP

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

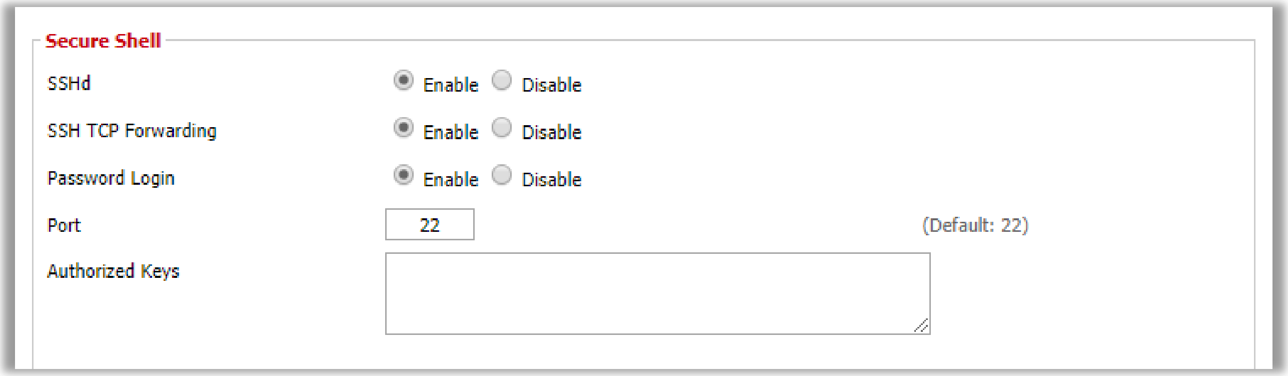
Services > Services > SNMP

SNMP	Description
SNMP	Enable or disable SNMP.
Location	Enter location information.

Contact	Enter contact information.
Name	Enter a name.
RO Community	Enter a Read-Only Community string.
RW Community	Enter a Read/Write Community string.

4.1.7 Secure Shell

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



Secure Shell

SSHd ● Enable ○ Disable

SSH TCP Forwarding ● Enable ○ Disable

Password Login ● Enable ○ Disable

Port 22 (Default: 22)

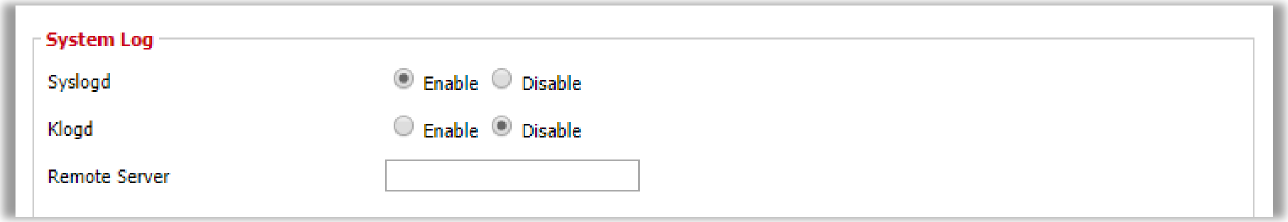
Authorized Keys

Services > Services > Secure Shell

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

4.1.8 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



System Log

Syslogd ● Enable ○ Disable

Klogd ○ Enable ● Disable

Remote Server

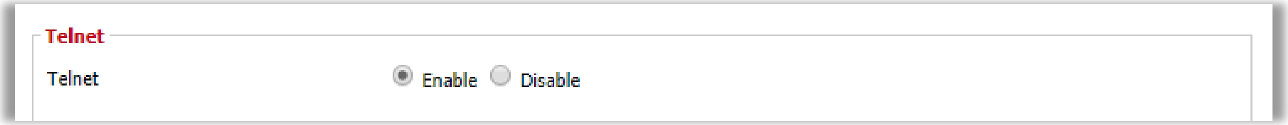
detection, and intrusion forensics.

Services > Services > System Log

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

4.1.9 Telnet

Enable or disable Telnet.

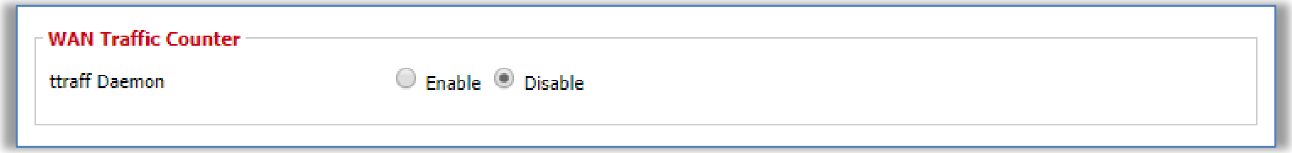


Telnet

Telnet ● Enable ○ Disable

Services > Services > Telnet

4.1.10 WAN Traffic Counter



WAN Traffic Counter

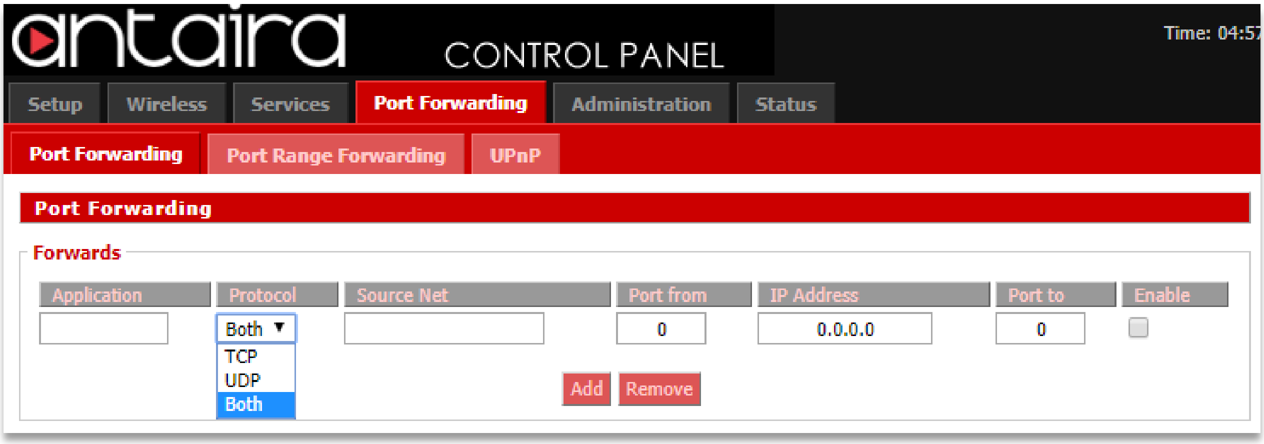
ttraff Daemon ○ Enable ● Disable

Services > Services > WAN Traffic Counter

5. Port Forwarding

5.1 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.

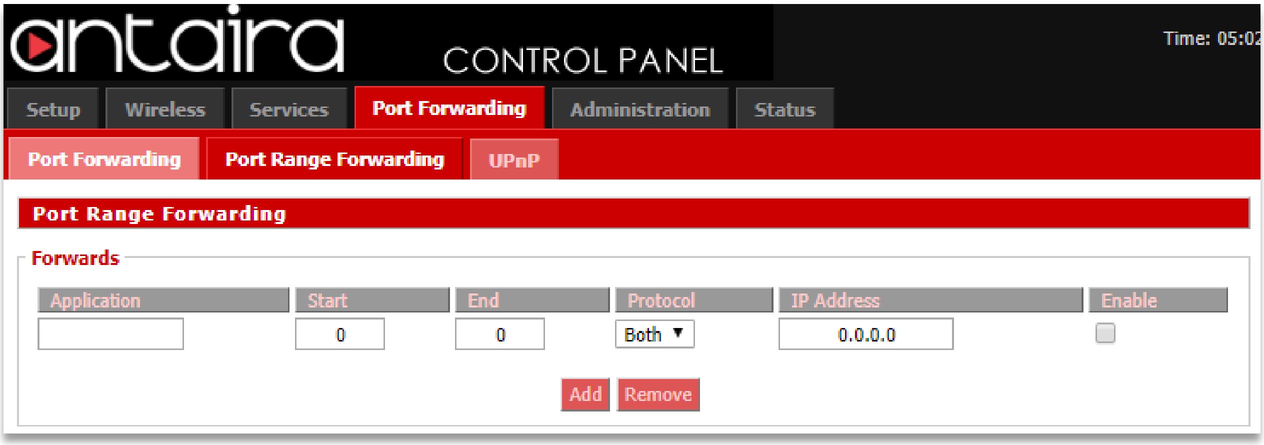


NAT/QoS > Port Forwarding

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

5.2 Port Range Forwarding

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



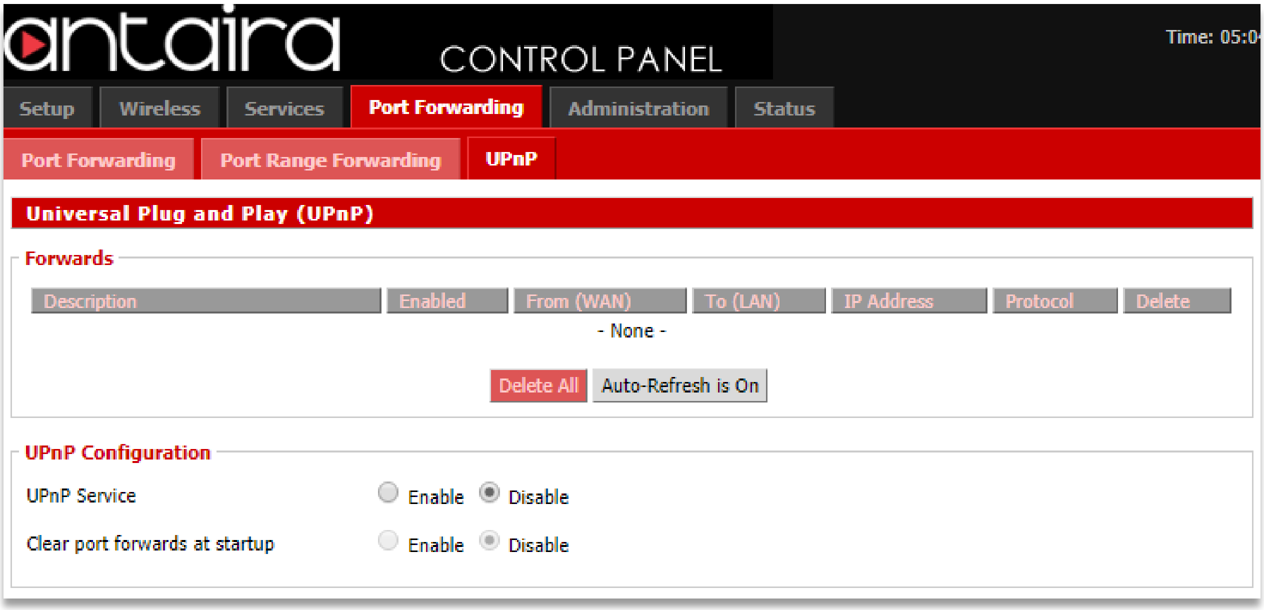
Application	Start	End	Protocol	IP Address	Enable
	0	0	Both ▾	0.0.0.0	□

NAT/QoS > Port Range Forwarding

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

5.3 UPnP

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



Universal Plug and Play (UPnP)

Forwards

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

UPnP Configuration

UPnP Service ○ Enable ● Disable

Clear port forwards at startup ○ Enable ● Disable

NAT/QoS > UPnP

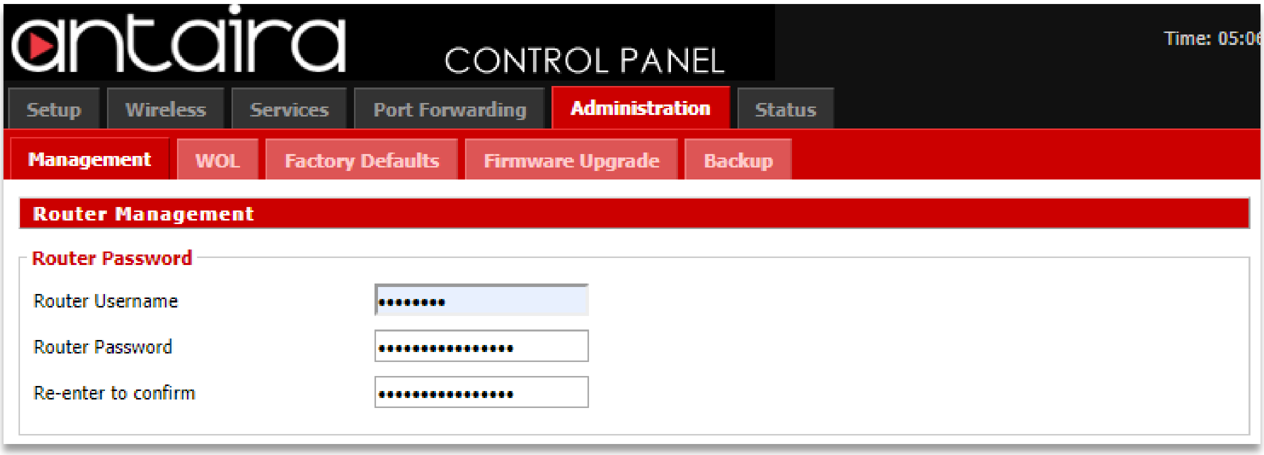
Universal Plug and Play (UPnP)	Description
Forwards	The UPnP forwards table shows all open ports forwarded automatically by the UPnP process.
UPnP Service	Enables UPnP service.
Clear Port Forwards at Startup	If enabled, a presentation URL tag is sent with the device description. This allows the router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

6. 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.

6.1 Management

6.1.1 Router Password



Router Username ••••••••

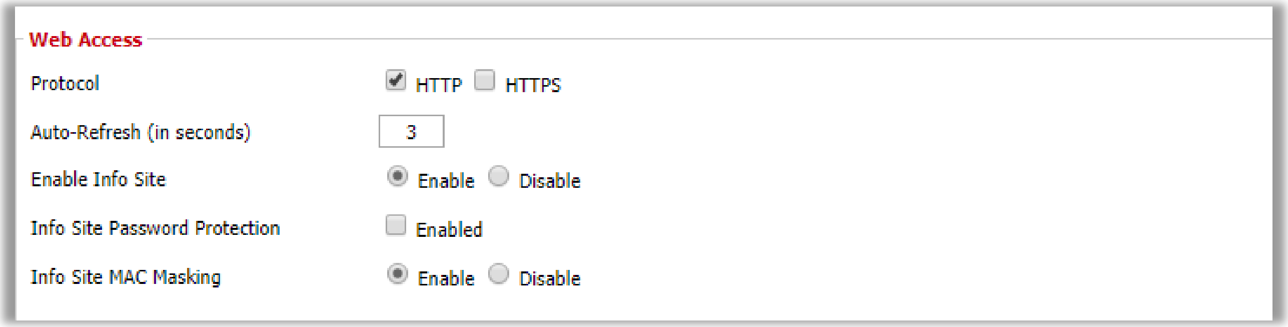
Router Password ••••••••••••••••

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.

6.1.2 Web Access



Web Access

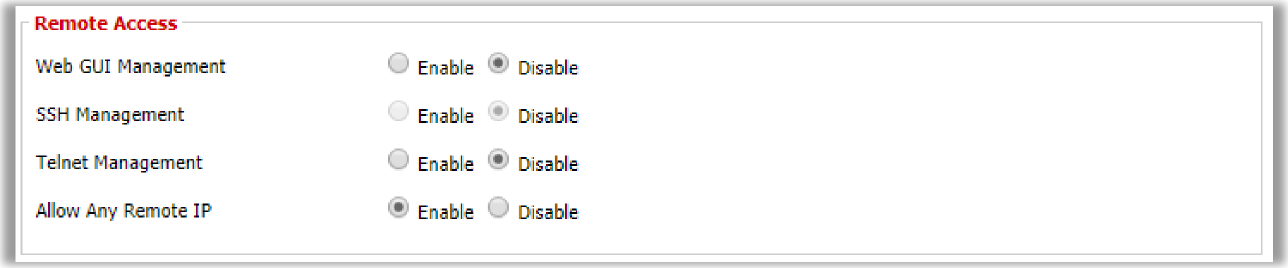
Protocol	☑ HTTP □ HTTPS
Auto-Refresh (in seconds)	3
Enable Info Site	● Enable ○ Disable
Info Site Password Protection	□ Enabled
Info Site MAC Masking	● Enable ○ Disable

Administration > Management > Web Access

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

6.1.3 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
SSH Management	○ Enable ● Disable
Telnet Management	○ Enable ● Disable
Allow Any Remote IP	● Enable ○ Disable

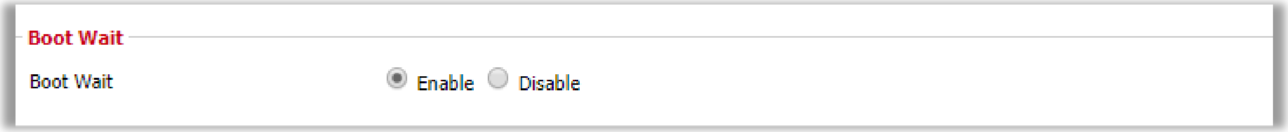
Administration > Management > Remote Access

Remote Access	Description
Web GUI	Enable or disable remote access the web interface.

Management	
SSH Management	Enable SSH remote access. Note that the SSH daemon needs to be enabled in the *Services* page.
Telnet Management	Enable Telent remote access.
Allow Any Remote IP	Allow any remote IP access or specify a range or IPs.

6.1.4 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.



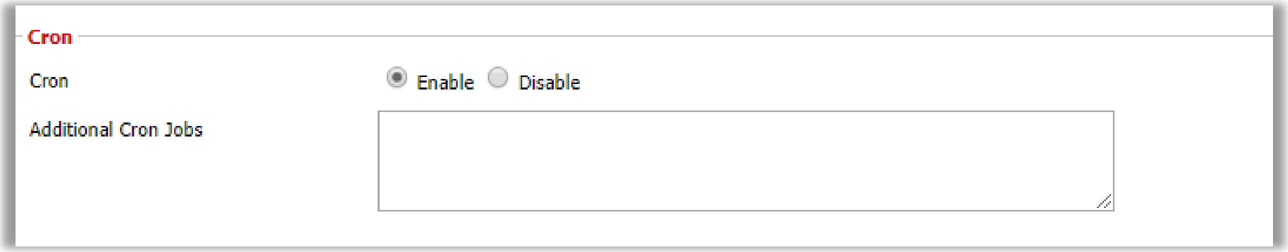
Boot Wait

Boot Wait ● Enable ○ Disable

Administration > Management > Boot Wait

6.1.5 Cron

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



Cron

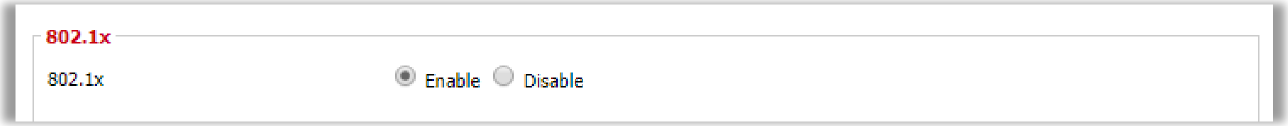
Cron ● Enable ○ Disable

Additional Cron Jobs

Administration > Management > Cron

6.1.6 802.1x

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



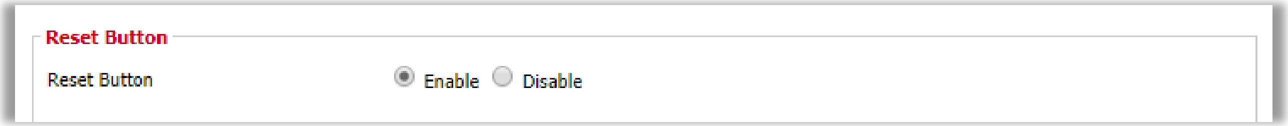
802.1x

802.1x ● Enable ○ Disable

Administration > Management > 802.1x

6.1.7 Reset Button

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



Reset Button

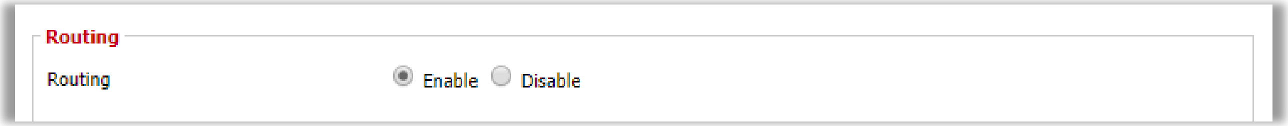
Reset Button ● Enable ○ Disable

Administration > Management > Reset Button

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

6.1.8 Routing

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

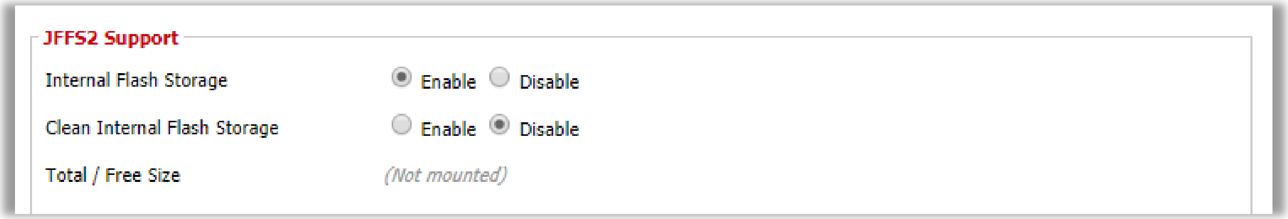


Routing

Routing ● Enable ○ Disable

Administration > Management > Routing

6.1.9 JFFS2 Support



JFFS2 Support

Internal Flash Storage ● Enable ○ Disable

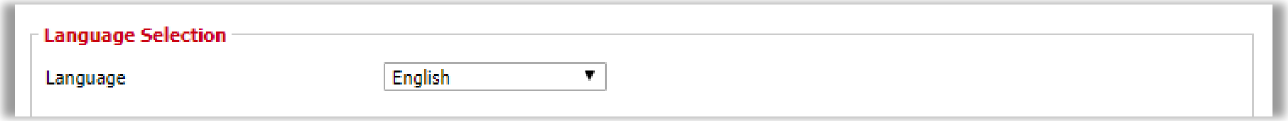
Clean Internal Flash Storage ○ Enable ● Disable

Total / Free Size *(Not mounted)*

Administration > Management > JFFS2 Support

6.1.10 Language Selection

Select the language presented on the router.



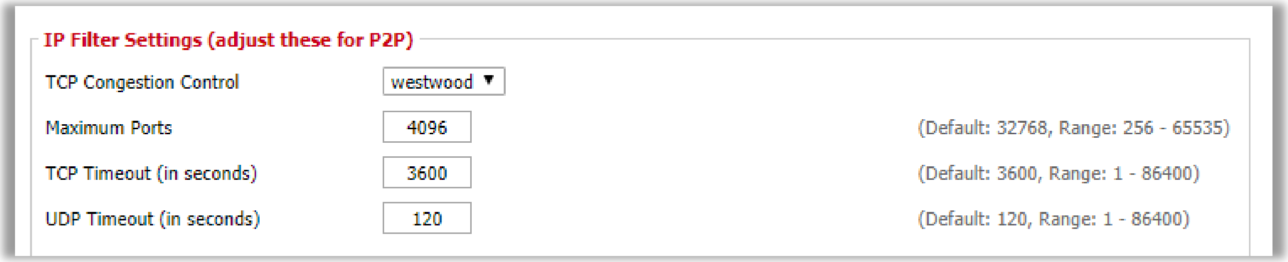
Language Selection

Language: English ▾

Administration > Management > Language Selection

6.1.11 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.



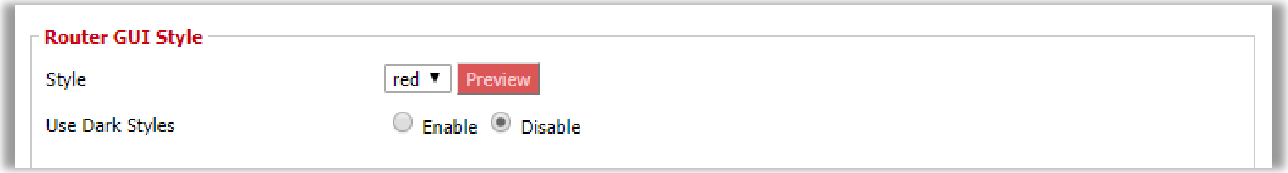
IP Filter Settings (adjust these for P2P)

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

6.1.12 Router GUI Style

Select the graphical style of the router.



Router GUI Style

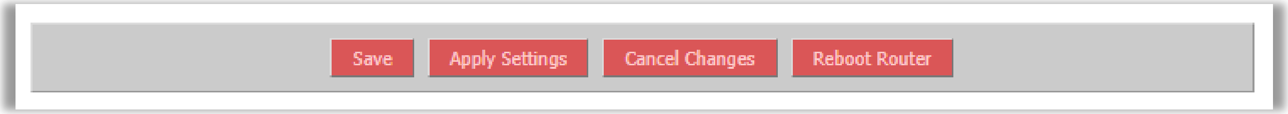
Style: red ▾

Use Dark Styles: ○ Enable ● Disable

Administration > Management > Router GUI Style

6.1.13 Router Reboot

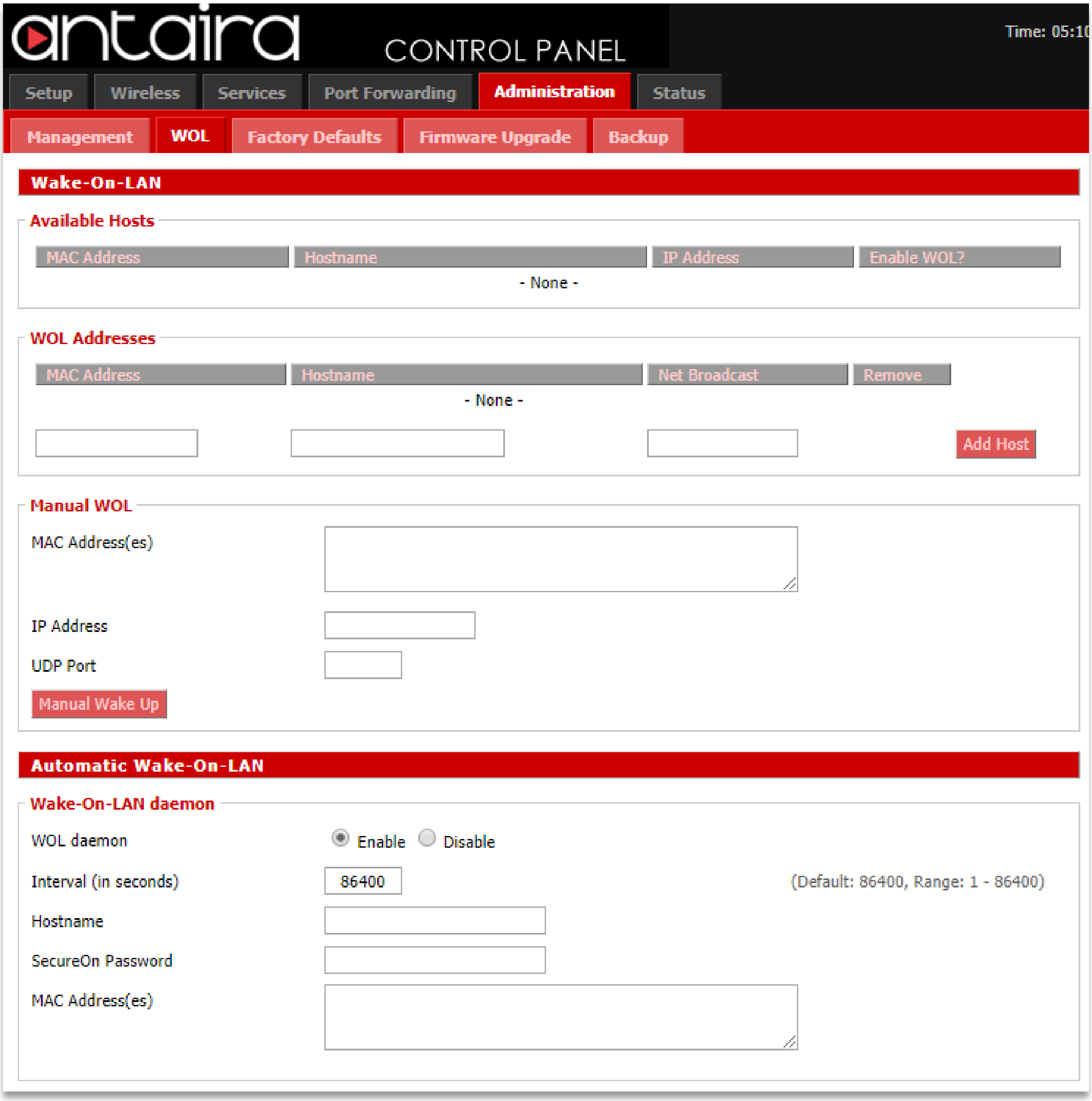
You may reboot the router under this page as well.



Administration > Management > Router Reboot

6.2 Wake on LAN (WOL)

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



Wake-On-LAN

Available Hosts

MAC Address	Hostname	IP Address	Enable WOL?
- None -			

WOL Addresses

MAC Address	Hostname	Net Broadcast	Remove
- None -			

Manual WOL

MAC Address(es)

IP Address

UDP Port

Automatic Wake-On-LAN

Wake-On-LAN daemon

WOL daemon ● Enable ○ Disable

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

Hostname

SecureOn Password

MAC Address(es)

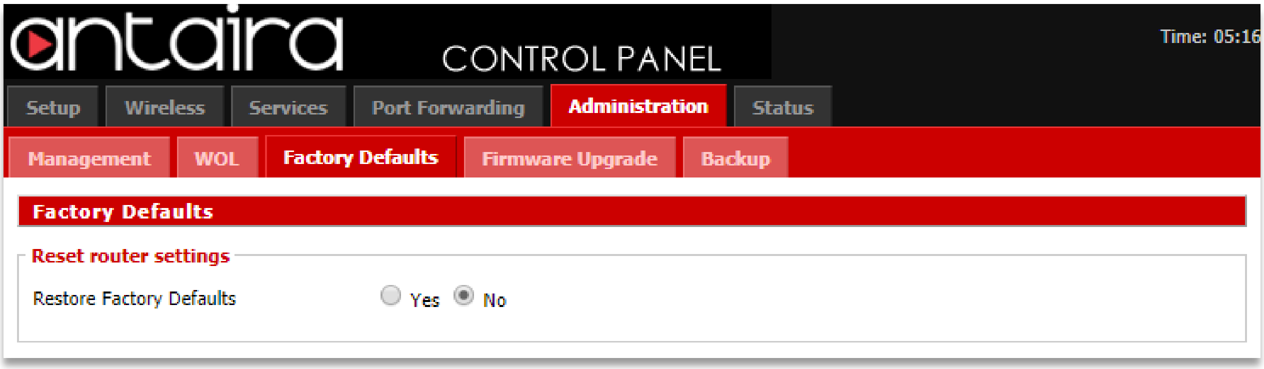
Administration > WOL

Wake on LAN	Description
Available Hosts	The available hosts section provides a list of hosts to add/remove from the WOL address list. This list is a

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

6.3 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**.



Factory Defaults

Reset router settings

Restore Factory Defaults ○ Yes ● No

Administration > Factory Defaults

6.4 Firmware Upgrade

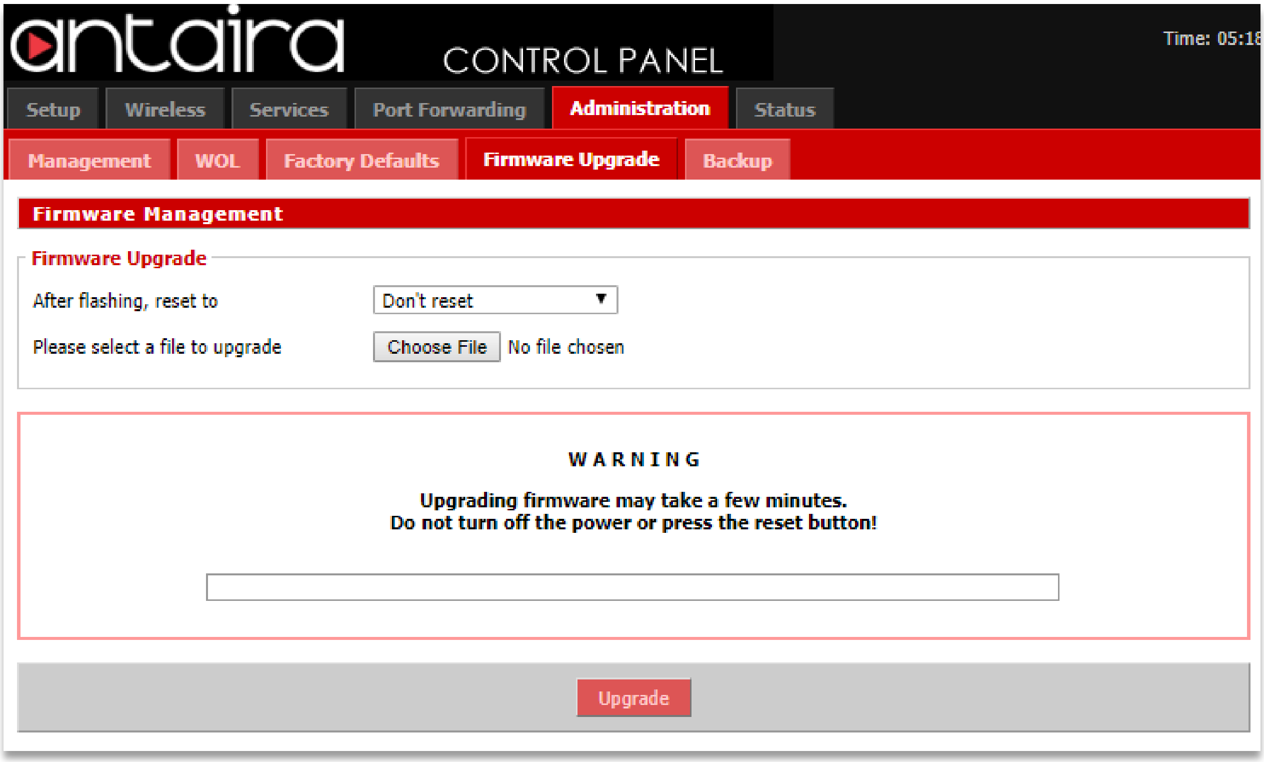
New firmware versions are available at www.antaira.com. When you upgrade the router's firmware, you may lose its configuration settings, so make sure you write down the router settings before you upgrade its firmware.

To upgrade the router's firmware:

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

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

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



After flashing, reset to: Don't reset

Please select a file to upgrade: No file chosen

WARNING

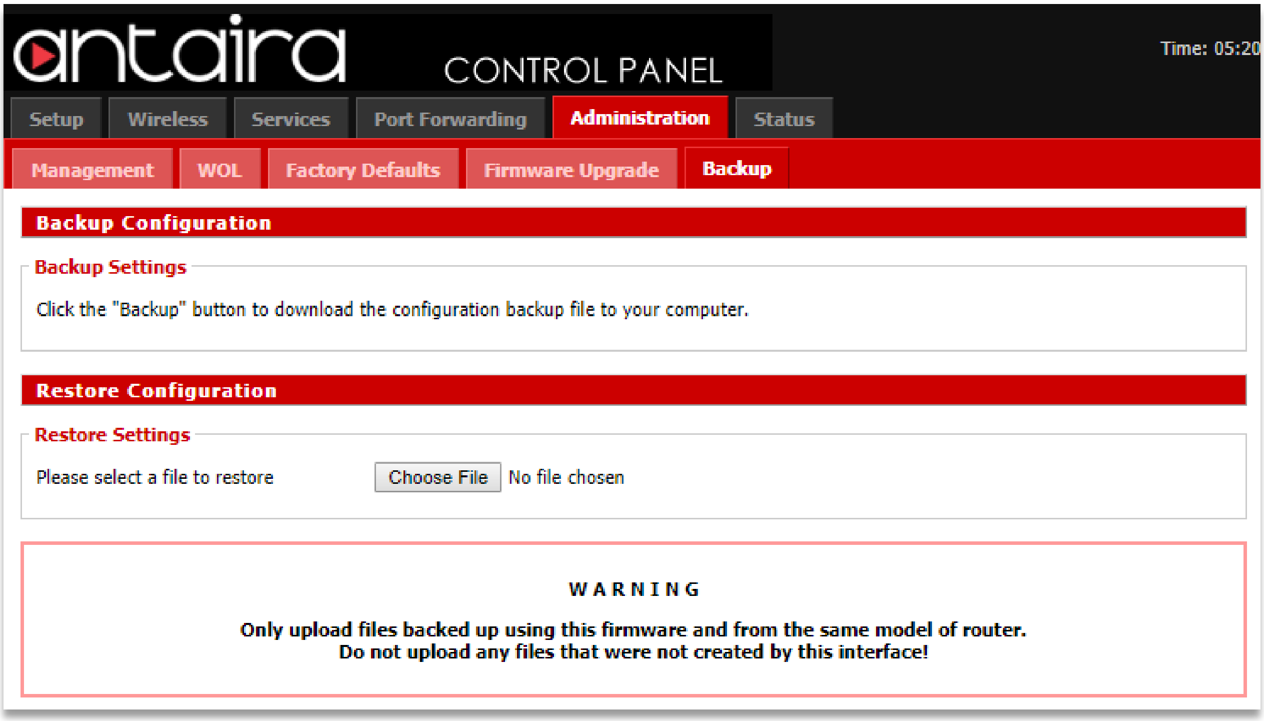
Upgrading firmware may take a few minutes.
Do not turn off the power or press the reset button!

Administration > Firmware Upgrade

6.5 Backup

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

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



Backup Configuration

Backup Settings

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

Restore Configuration

Restore Settings

Please select a file to restore No file chosen

WARNING

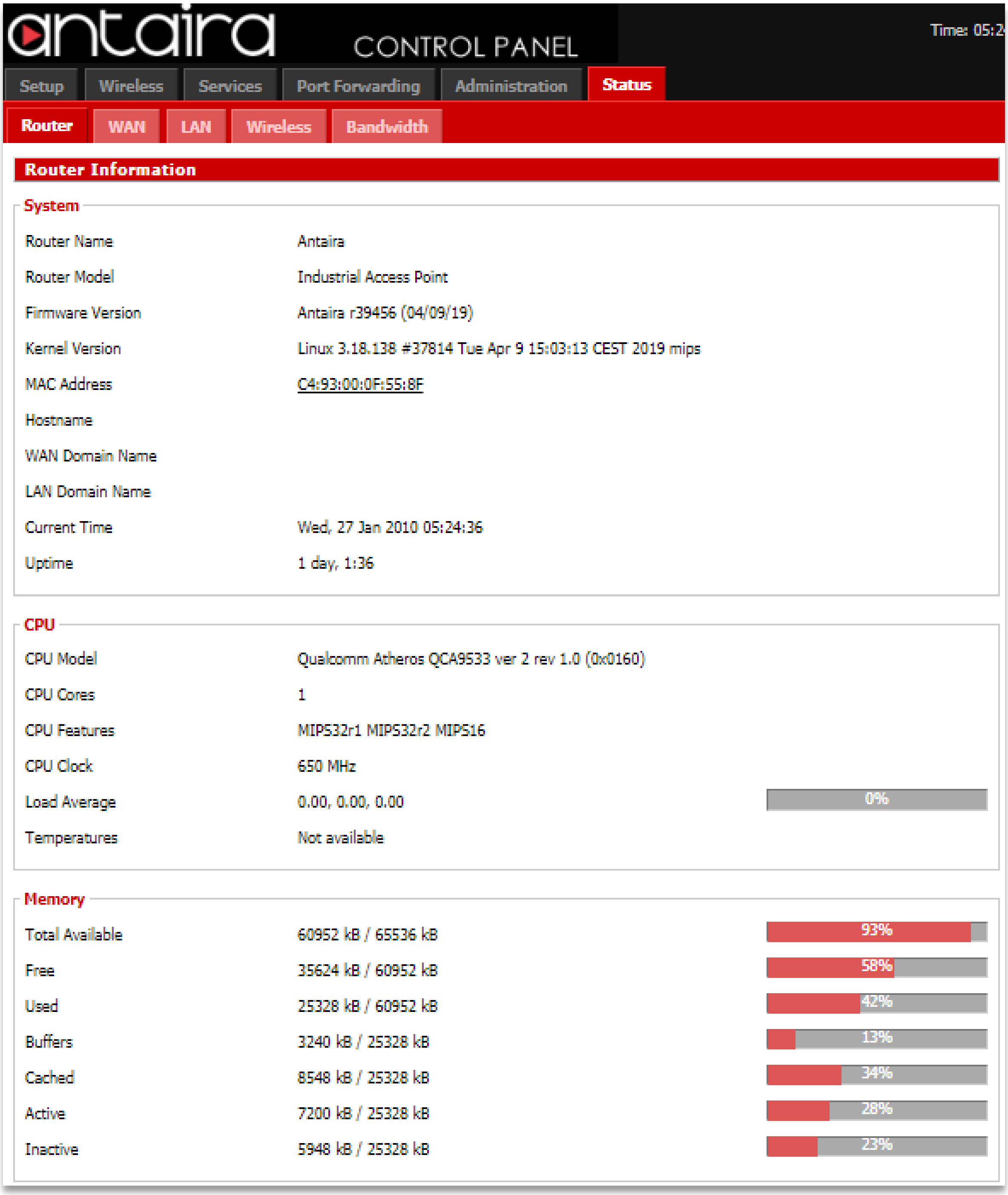
Only upload files backed up using this firmware and from the same model of router.
Do not upload any files that were not created by this interface!

Administration > Backup

7. Status

7.1 Router

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



Router Information

System

Router Name	Antaira
Router Model	Industrial Access Point
Firmware Version	Antaira r39456 (04/09/19)
Kernel Version	Linux 3.18.138 #37814 Tue Apr 9 15:03:13 CEST 2019 mips
MAC Address	C4:93:00:0F:55:8F
Hostname	
WAN Domain Name	
LAN Domain Name	
Current Time	Wed, 27 Jan 2010 05:24:36
Uptime	1 day, 1:36

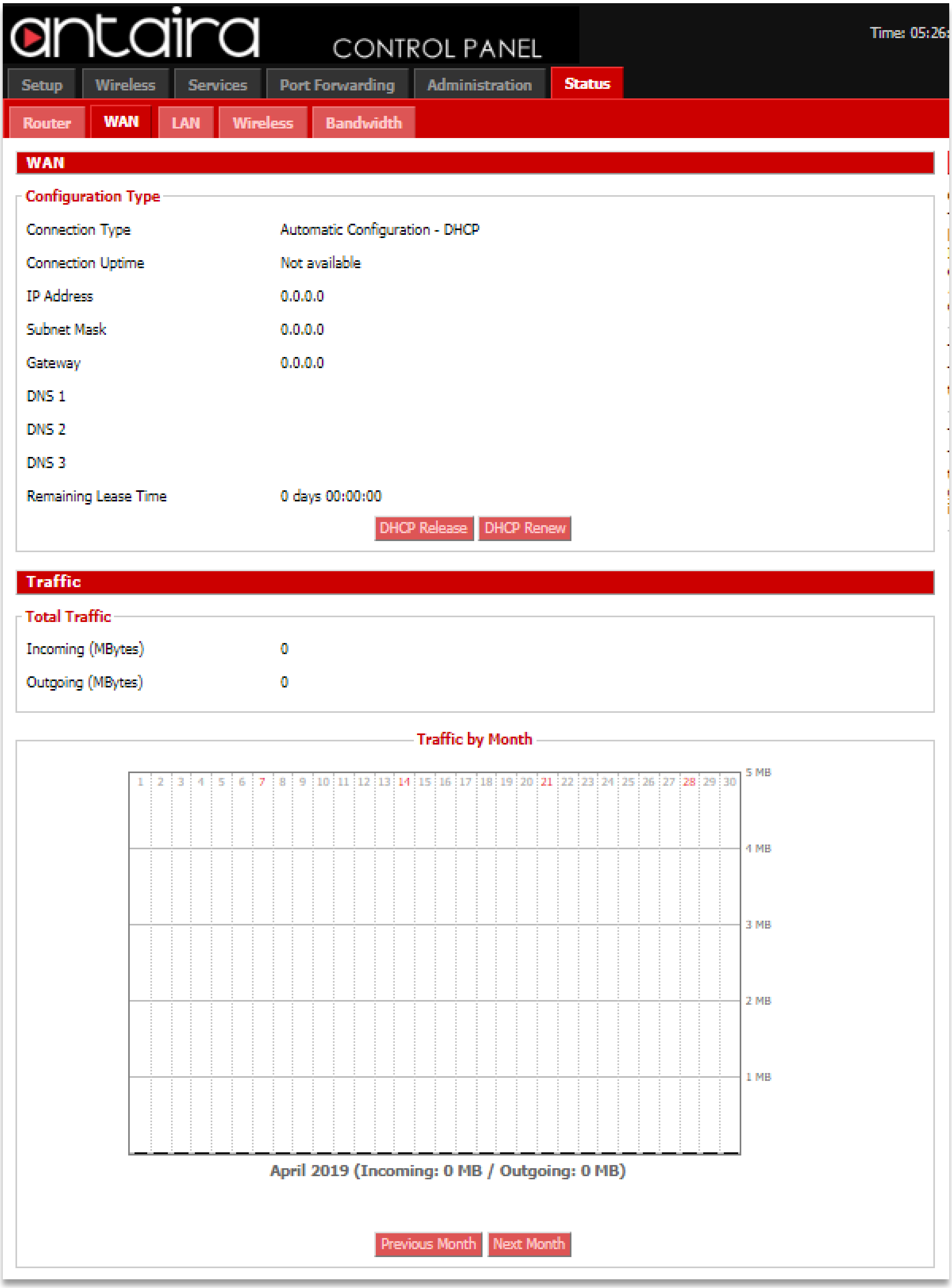
CPU

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	0.00, 0.00, 0.00	0%
Temperatures	Not available	

Memory

Total Available	60952 kB / 65536 kB	93%
Free	35624 kB / 60952 kB	58%
Used	25328 kB / 60952 kB	42%
Buffers	3240 kB / 25328 kB	13%
Cached	8548 kB / 25328 kB	34%
Active	7200 kB / 25328 kB	28%
Inactive	5948 kB / 25328 kB	23%

7.2 WAN



WAN

Configuration Type

Connection Type	Automatic Configuration - DHCP
Connection Uptime	Not available
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	
Remaining Lease Time	0 days 00:00:00

Traffic

Total Traffic

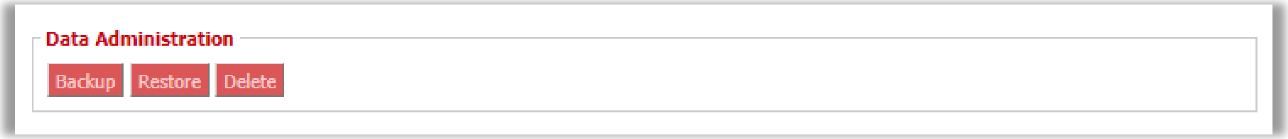
Incoming (MBytes)	0
Outgoing (MBytes)	0

Traffic by Month

April 2019 (Incoming: 0 MB / Outgoing: 0 MB)

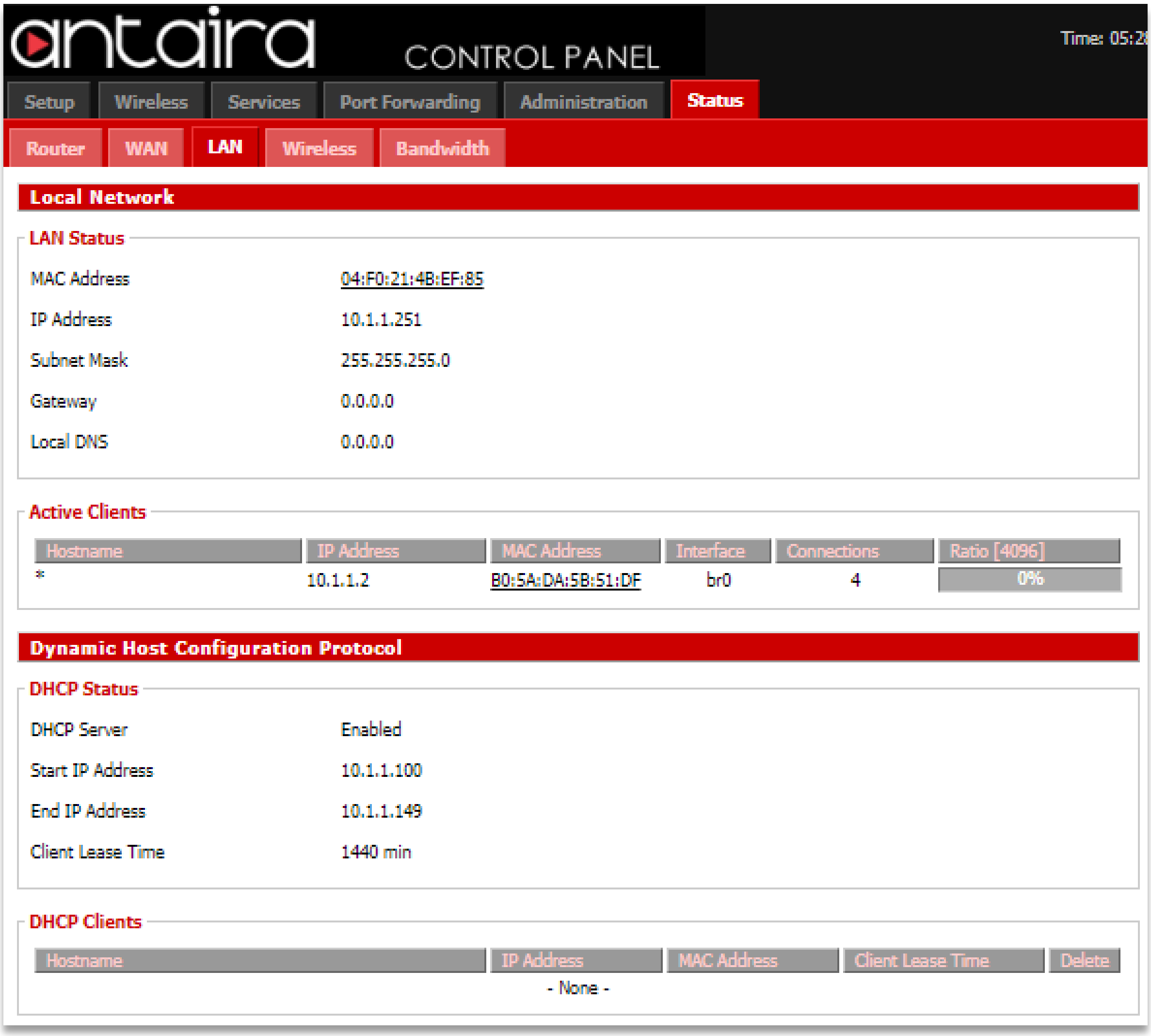
Status > WAN

Data Administration



Status > WAN > Data Administration

7.3 LAN



Local Network

LAN Status

MAC Address	04:F0:21:4B:EF:85
IP Address	10.1.1.251
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

Active Clients

Hostname	IP Address	MAC Address	Interface	Connections	Ratio [4096]
*	10.1.1.2	B0:5A:DA:5B:51:DF	br0	4	0%

Dynamic Host Configuration Protocol

DHCP Status

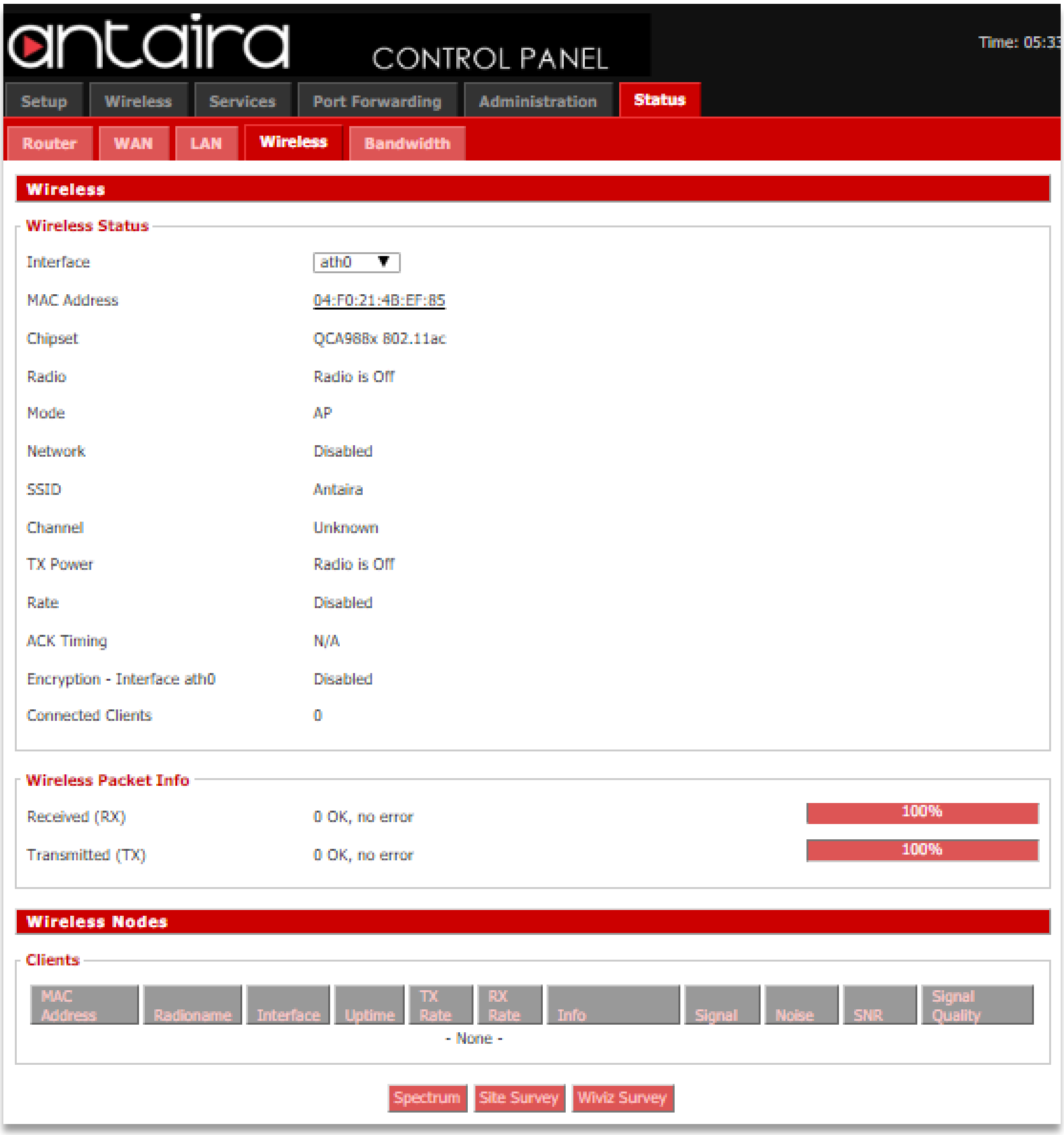
DHCP Server	Enabled
Start IP Address	10.1.1.100
End IP Address	10.1.1.149
Client Lease Time	1440 min

DHCP Clients

Hostname	IP Address	MAC Address	Client Lease Time	Delete
- None -				

Status > LAN

7.4 Wireless



Wireless

Wireless Status

Interface	ath0 ▼
MAC Address	04:F0:21:4B:EF:85
Chipset	QCA988x 802.11ac
Radio	Radio is Off
Mode	AP
Network	Disabled
SSID	Antaira
Channel	Unknown
TX Power	Radio is Off
Rate	Disabled
ACK Timing	N/A
Encryption - Interface ath0	Disabled
Connected Clients	0

Wireless Packet Info

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

Wireless Nodes

Clients

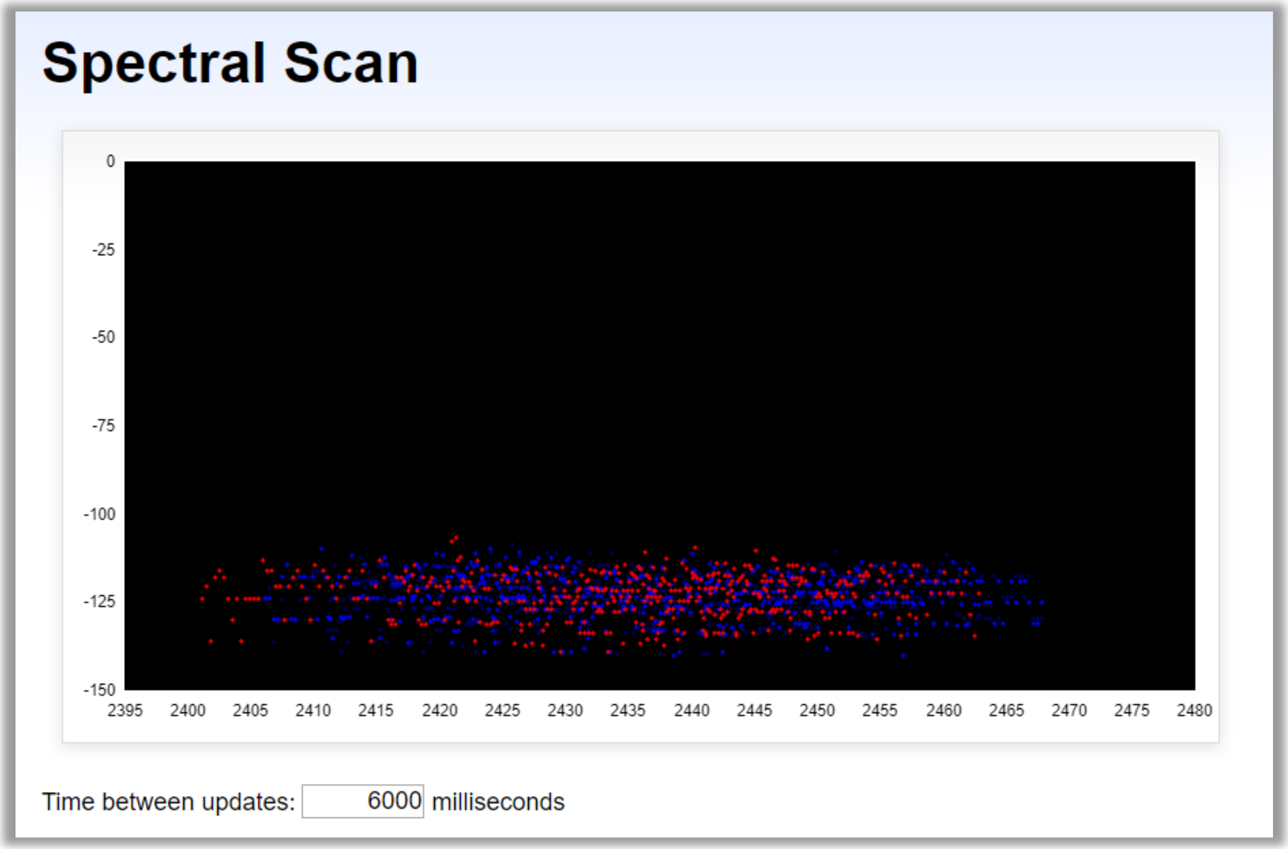
MAC Address	Radioname	Interface	Uptime	TX Rate	RX Rate	Info	Signal	Noise	SNR	Signal Quality

- None -

Status > Wireless

Spectrum

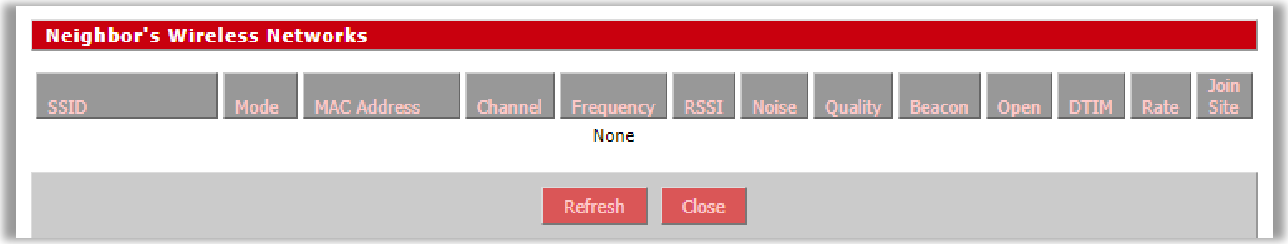
The spectral scan will show which frequencies have a lot of interference across either the 2.4GHz or 5GHz. No channel numbers are provided in the scan window. The x-axis represents frequencies in Hertz (Hz). The y-axis represents power drop in dB for noise. The higher numbers are better. Blue dots represent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



Time between updates: 6000 milliseconds

Status > Wireless > Spectral Scan

Site Survey



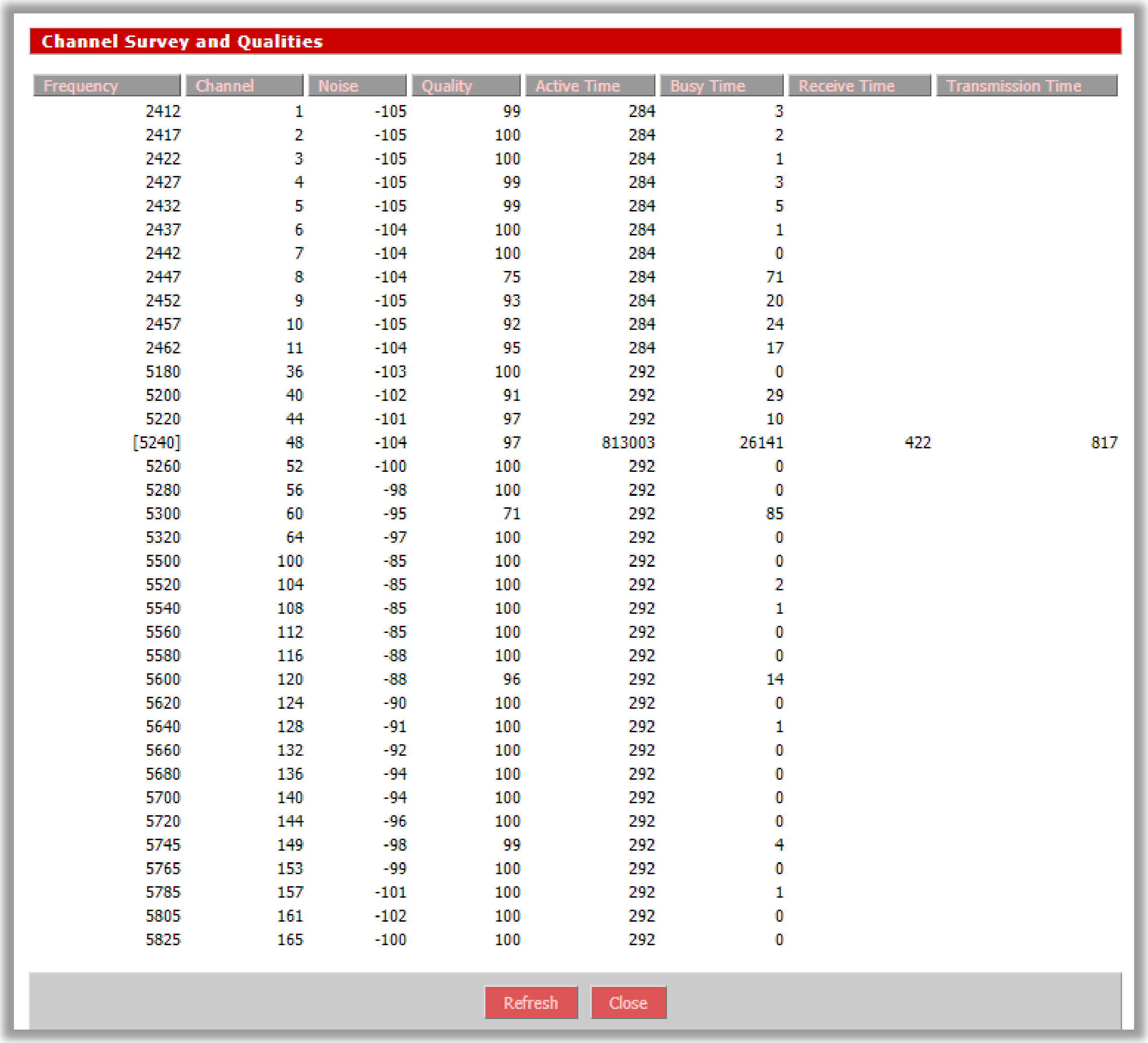
Neighbor's Wireless Networks

SSID	Mode	MAC Address	Channel	Frequency	RSSI	Noise	Quality	Beacon	Open	DTIM	Rate	Join Site

None

Status > Wireless > Site Survey

Channel Survey



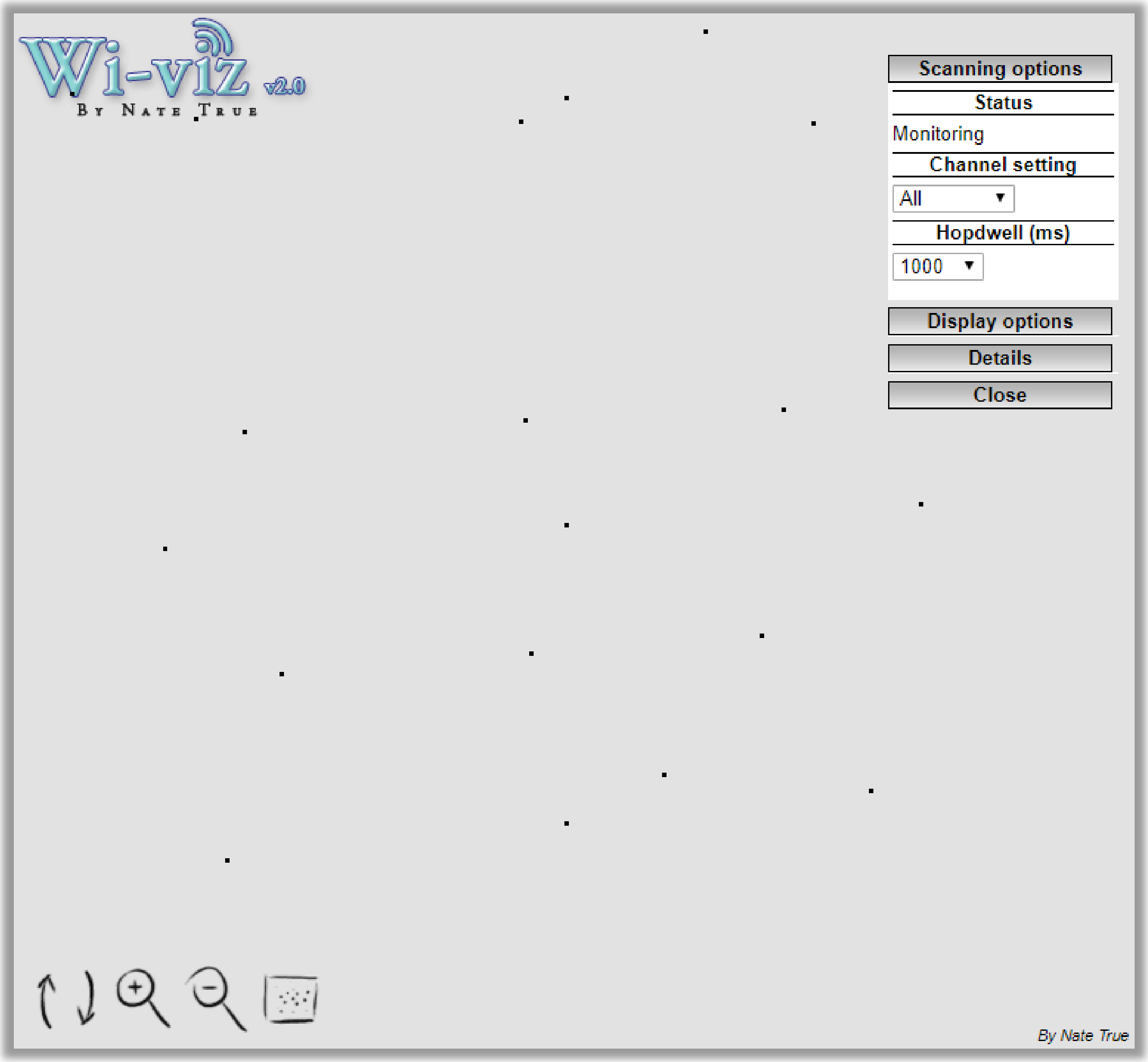
Channel Survey and Qualities

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

Status > Wireless > Channel Survey

Wiviz Survey

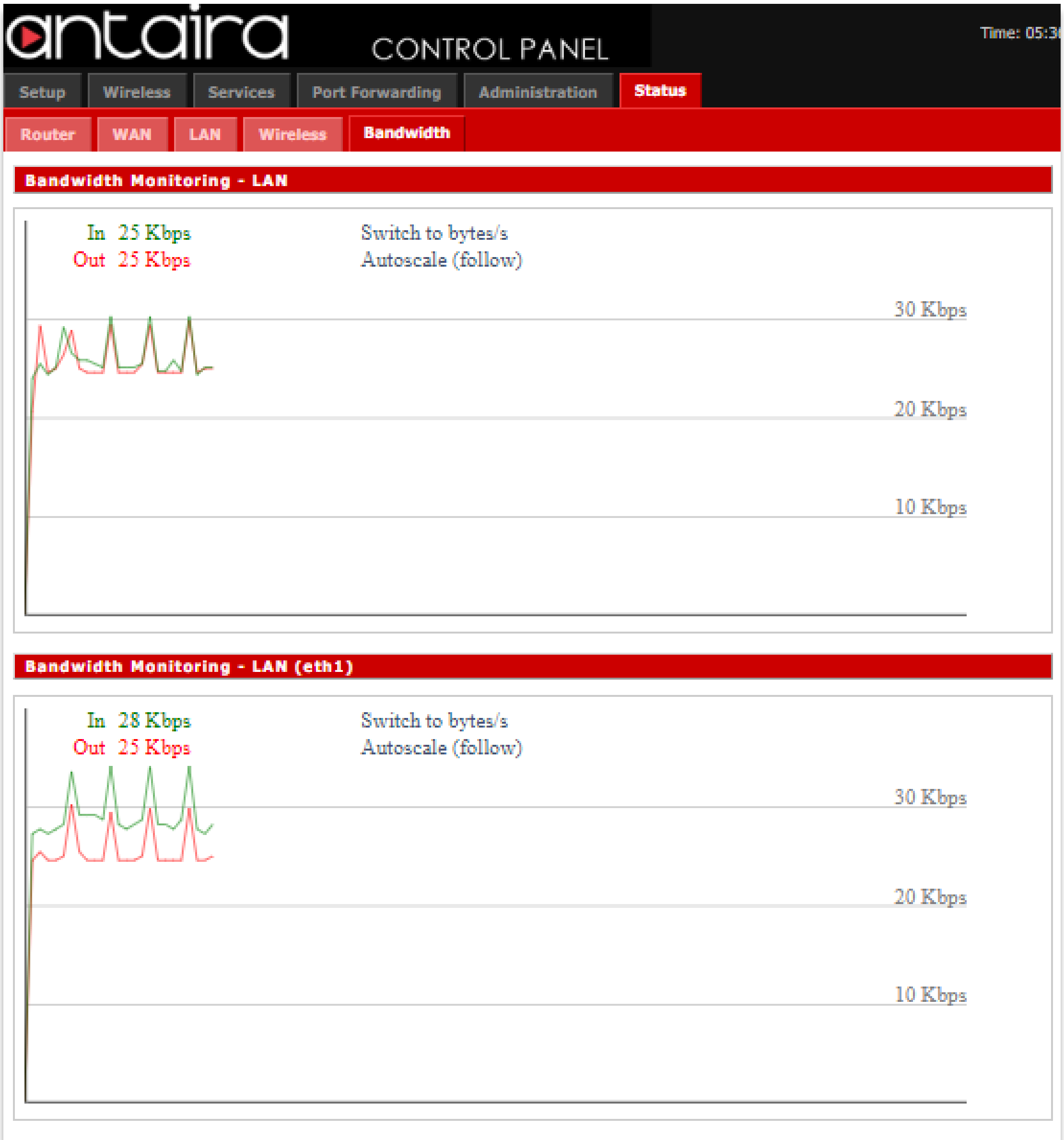
Wiviz is an open source GPL project that allows you to use your router to see other networks. The interface scans for networks and shows signal strength and effects of antenna adjustment in real time.



Status
Monitoring
Channel setting
All
Hopdwell (ms)
1000

Status > Wireless > Wiviz Survey

7.5 Bandwidth



Bandwidth Monitoring - LAN

In 25 Kbps
Out 25 Kbps

Bandwidth Monitoring - LAN (eth1)

In 28 Kbps
Out 25 Kbps

Status > Bandwidth