



## WIRELESS ACCESS POINT SOFTWARE MANUAL

Models:

AN-100-AP-I-N  
AN-300-AP-I-N  
AN-500-AP-I-AC  
AN-700-AP-I-AC  
AN-700-AP-O-AC





## Table of Contents

<b>1 - About this Manual</b>	<b>5</b>
1.1 - Understanding Model Differences and Images	5
1.2 - Important Information	5
<b>2 - First Time Setup Tips</b>	<b>6</b>
<b>3 - Using OvrC With Your Device</b>	<b>6</b>
3.1 - What is OvrC?	6
3.2 - Claiming the WAP in OvrC	6
3.3 - OvrC Configuration	6
3.4 - OvrC WebConnect	7
<b>4 - Accessing the Web Interface without OvrC</b>	<b>8</b>
4.1 - EZ Access Method	8
4.2 - Configured System Name Access	9
4.3 - Issued IP Address Method	9
4.4 - Default IP Address Access	10
<b>5 - Web Interface Overview</b>	<b>12</b>
5.1 - Applying Changes in the Web Interface	13
<b>6 - System Status</b>	<b>14</b>
6.1 - System Information	14
6.2 - Wireless Information	14
6.3 - LAN Information	15
6.4 - System Log	15
<b>7 - Wireless Interface Status</b>	<b>16</b>
7.1 - Radio Status	16
7.2 - Utilization of SSID	17
Wireless Network	17
7.3 - Connected Clients	18
<b>8 - System Settings</b>	<b>19</b>
8.1 - System Information	19
8.2 - Date and Time Settings	20
8.3 - Time Zone Settings	21
<b>9 - LAN Settings</b>	<b>22</b>
9.1 - IP Settings	22
IP Address Setup: Best Practices	22
9.2 - Interface Settings	23
<b>10 - Wireless Settings</b>	<b>24</b>
10.1 - Radio Settings	24
10.2 - Utilization of SSID	25
10.3 - Global Wireless Settings	25
Fast Roaming Setup	26
10.4 - Wireless Networks	28
Configuring a New SSID	29



<b>10.5 - Wireless Security Options (SSID Encryption)</b>	30
WEP Mode	30
WPA-PSK Mixed and WPA2-PSK Modes	31
WPA and WPA2 Modes	32
<b>10.6 - Guest Network Setup</b>	33
<b>10.7 - Repeater Mode Setup</b>	35
<b>11 - Security Settings</b>	37
11.1 - User Accounts	37
11.2 - Access Control	38
11.3 - Email Alert	39
11.4 - Device Discovery	40
<b>12 - Schedule</b>	41
12.1 - Auto Reboot Settings	41
12.2 - Gateway Connection Monitor	42
12.3 - Wi-Fi Scheduler	43
Configuring Wi-Fi Scheduler	44
<b>13 - Ping Test</b>	45
13.1 - Running a Ping Test	45
<b>14 - Traceroute Test</b>	46
14.1 - Running a Traceroute Test	46
<b>15 - File Management</b>	47
15.1 - Configuration File	47
Backup Current Configuration	47
Upload New Configuration File	47
Restore Factory Defaults	48
Hardware Factory Default	48
Firmware	49
Firmware Update Instructions	49
<b>16 - Restart</b>	50
16.1 - Rebooting the Device	50
<b>17 - Logout</b>	51
17.1 - Logging Out	51
<b>18 - Advanced Menu</b>	52
18.1 - Advanced Wireless Settings	52
Radio Settings	52
Client Limit	53
18.2 - Wireless MAC Filter Settings	54
MAC Filter Schedule	55
Managing MAC Filter Lists	55
18.3 - WPS Settings	56
Connecting a Device Using WPS via Push Button	57
Connecting a Device Using WPS via PIN	58
18.4 - Site Survey	59
Running a Site Survey	59



<b>18.5 - Spectrum Analyzer</b>	60
Configuring Scan Settings	60
Running a Scan	60
Understanding Spectrum Analyzer Results	61
<b>18.6 - Wireless Traffic Shaping Settings</b>	63
<b>18.7 - SNMP Settings</b>	64
SNMPv2 Settings	64
SNMPv3 Settings	65
<b>18.8 - Spanning Tree Settings</b>	66
<b>18.9 - VLAN Settings</b>	67
<b>19 - Appendix</b>	68
<b>19.1 - Configuring Guest Networks with Fast Roaming</b>	68
<b>20 - 2-Year Limited Warranty</b>	71
<b>21 - Contacting Technical Support</b>	71

## 1 - About this Manual

This manual details setup and use of the built-in web interface software menus for all Araknis Wireless Access Points.

### 1.1 - Understanding Model Differences and Images

You may notice minor differences between the images and call-outs in the manual versus what you see in your interface. All differences in features or operation are noted. Exceptions that aren't noted in the manual:

- 100 series WAPs will indicate settings and information for the 2.4GHz channel only (no 5GHz support). 300/500/700 series will indicate settings and information for 2.4GHz and 5GHz channels.
- Indoor series WAPs will indicate settings and information for only LAN port 1 (no second LAN port is offered). Outdoor series WAPs will indicate settings and information for both LAN ports 1 and 2.

### 1.2 - Important Information

The symbols below are used to identify important information:

 **Pro Tip** - Pro tips add information that provides extra value, utility, or ease-of-use for the installer or end user of the product. These items are not required, but have been added for your convenience.

 **Note** - Notes emphasize information important to the installation, setup, or use of the product that is not essential to follow for safety of the equipment or user. These items usually contain essential information that, if missed, would cause the installer or end user extra work.

 **Caution** - The caution symbol is used to indicate information vital to the safety of the equipment in use with the product, or the product itself. Not following a caution may result in permanent damage to equipment that is not covered by warranty.

 **Warning** - Warnings indicate information vital to the safety of the installer or end user of the product. Not following a warning may result in permanent damage to equipment and serious injury or death of the installer or end user.

## 2 - First Time Setup Tips

- For jobs with multiple WAPs, consider using OvrC to complete SSID setup for all WAPs at once. See the OvrC app for more information.
- All Araknis access points transmit the same SSID, **araknis\_initial** by default. If multiple access points are being installed in the same network without using OvrC for SSID setup, power on and complete network setup for one device at a time to avoid confusion about which access point you are connected to. Always change the SSID and admin password during initial setup.
- Araknis Networks recommends using DHCP IP settings in equipment, with IP address reservations in the router.
- Always change the login credentials for all devices during initial setup to prevent unwanted access or changes.

## 3 - Using OvrC With Your Device

The built-in menus can be used to configure any basic or advanced feature, but for the best experience, we recommend claiming your product in OvrC and checking out the features offered there too.

### 3.1 - What is OvrC?

OvrC is a professional cloud-based solution that helps you monitor your devices in the field and provide focused customer care. Remote access saves you time and money on unnecessary calls, while the app's ease of use and agility keep you from experiencing the usual network setup frustrations. OvrC and Araknis work perfectly together to help you get the job done. Go to [ovrc.com](http://ovrc.com) to learn more and get started.

You can access your OvrC account in two ways:

- **Mobile App** - Access your account from your smart phone or tablet. Visit the app store from your device and search for the OvrC app (not the home app).
- **Web App** - Access your account from a computer web browser ([app.ovrc.com](http://app.ovrc.com)).

### 3.2 - Claiming the WAP in OvrC

1. Connect the WAP to the Internet.
2. Open your OvrC mobile or web app.
3. Create or select a customer and location.
4. Add the device (MAC address and Service Tag numbers needed for authentication).

### 3.3 - OvrC Configuration

Many of the settings in your device can also be configured from the OvrC app, and more features are being added all the time. For example, if you have multiple WAPs to configure on one LAN, SSID settings for all devices can be set at one time.

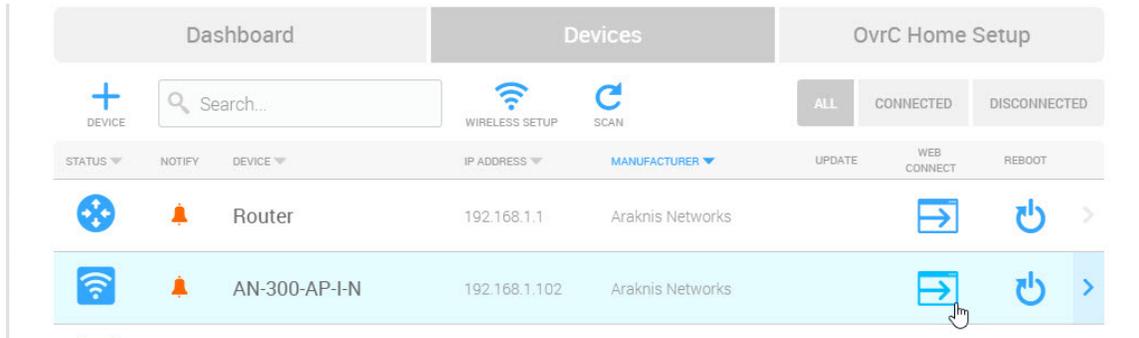
See the OvrC mobile or web app for all of the latest features and settings.

### 3.4 - OvrC WebConnect

The WebConnect feature enables you to access the local interface of your WAP from anywhere, right from your OvrC account device list. No port forwarding or other setup is required.

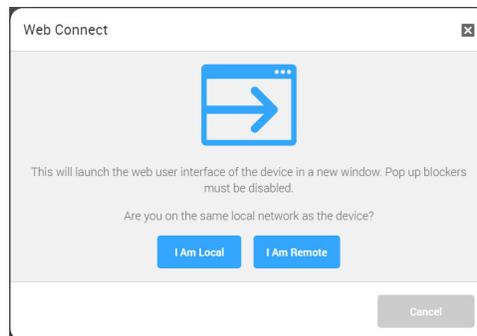
1. Open your OvrC web or smartphone app and find the WAP in the device list.

Figure 1. OvrC Device List



2. Click the **WebConnect** button. You may need to disable pop-up blockers in your browser.
3. When the pop-up appears, select the appropriate option:
  - **I Am Local** - Use if on the same LAN as the device.
  - **I Am Remote** - Use if on a different LAN to access the WAP from over the Internet.

Figure 2. WebConnect Access



4. Once you click the button, a new browser tab/window will load the login page for the WAP. You may now log in as normal.
  - **Default Login Credentials** - Username: *araknis*; Password: *araknis*

## 4 - Accessing the Web Interface without OvrC

There are several ways to access the WAP's web interface without using OvrC:

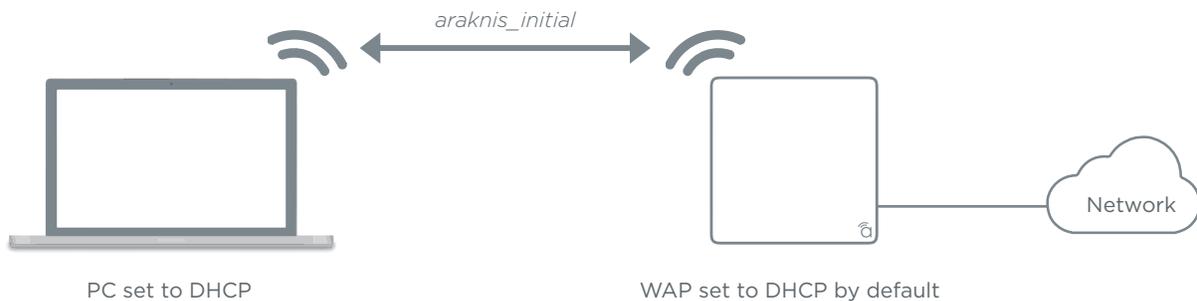
- **EZ Access Method** - Used for initial setup. Connect your computer to the access point using Wi-Fi.
- **Configured System Name Access** - Enter the device name instead of the IP address to access the web interface.
- **DHCP/Static IP Address Method** - Enter the IP address issued to the WAP, or the default IP address, (192.168.20.253).

### 4.1 - EZ Access Method

Connect and access the web interface without any cable connections or network card setting changes.

**Note** - The WAP must be connected to a network with a functioning DHCP server for EZ Access setup. After the WAP is powered on, startup usually takes two to four minutes to complete. Wait for the Status LED to turn solid before beginning setup.

Figure 3. Default SSID



1. Power on the WAP. If you have several, power them on and set them one at a time to avoid confusion.
1. Disconnect all network cables from your computer.
2. Set the wireless network card to obtain an IP address automatically (DHCP mode).
3. Connect your computer to the wireless network SSID named **araknis\_initial**. If you see more than one, power off all but one WAP.
4. Open a web browser and enter the configuration address for your device:
  - AN-100-AP-I-N enter: <http://config.an-100-ap-i-n.wap/>
  - AN-300-AP-I-N enter: <http://config.an-300-ap-i-n.wap/>
  - AN-500-AP-I-AC enter: <http://config.an-500-ap-i-ac.wap/>
  - AN-700-AP-I-AC enter: <http://config.an-700-ap-i-ac.wap/>
  - AN-700-AP-O-AC enter: <http://config.an-700-ap-o-ac.wap/>
5. Enter your login credentials and log in.
  - **Default Login Credentials** - Username: **araknis**; Password: **araknis**

## 4.2 - Configured System Name Access

**Note** - Araknis EZ Access (Security Menu>Device Discovery) must be enabled for this method to work. See section [11.4 - Device Discovery \(p.40\)](#) for more information.

1. See section [8 - System Settings \(p.19\)](#) to set the system name, then apply the settings. After configuration, the WAP web interface may be accessed using the system name.
2. Open a web browser and enter the configuration address for your WAP in this format (Example System Name = *smith100*):
  - Enter into address bar: *http://config.smith100.wap/*
3. Enter your login credentials and log in.
  - **Default Login Credentials** - Username: *araknis*; Password: *araknis*

## 4.3 - Issued IP Address Method

Connect your computer to the wired or wireless network and enter the IP address issued to the access point by the network.

1. Use one of these methods to find the IP address of the WAP:
  - Check the client table on your router
  - Use a network scanner (e.g. Fing) to sniff the network. The Araknis WAP manufacturer field will display **Snap AV**.
  - See the highlighted field in the figure below for an example of an Araknis device being identified.

**Figure 4.** Fing IP Scanner Example

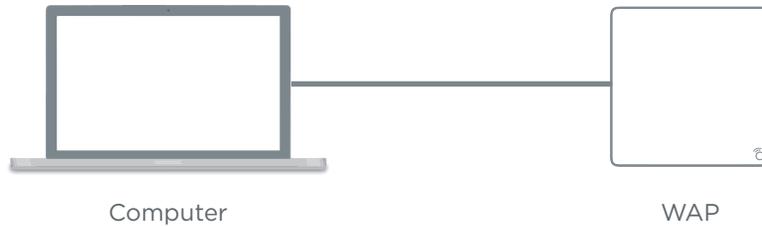


2. Once the IP address is found, enter it in your web browser and log in. (Default: *araknis/araknis*)

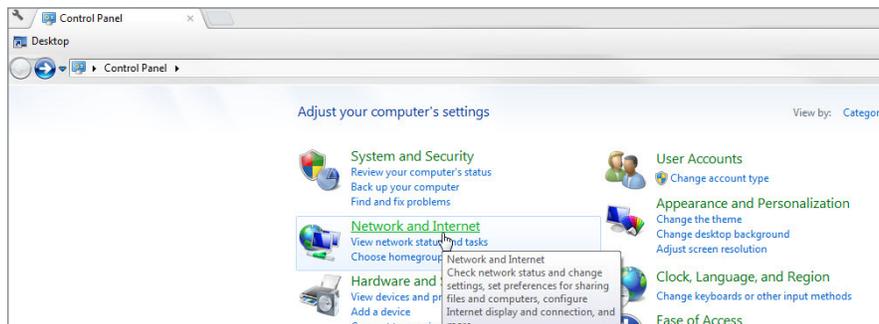
## 4.4 - Default IP Address Access

Access the interface using the default IP address, **192.168.20.253**. Use this method if the access point is not issued an IP address on the network or if access is required while not connected to a network.

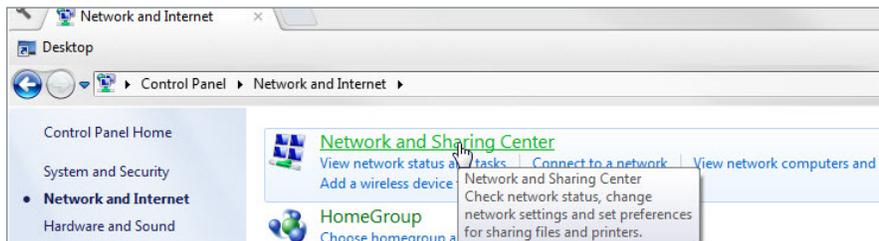
1. Connect your PC to the WAP using a network patch cable.



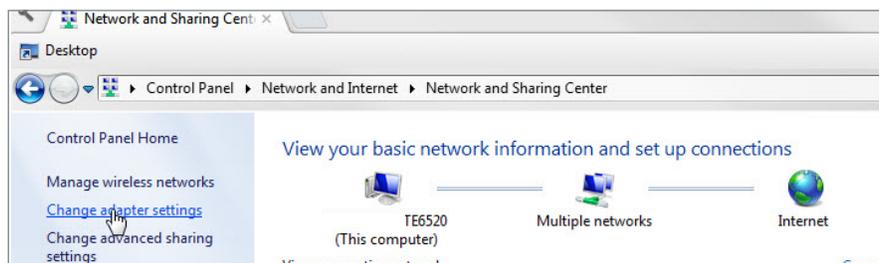
2. On your PC, open the Control Panel and click **Network and Internet**.



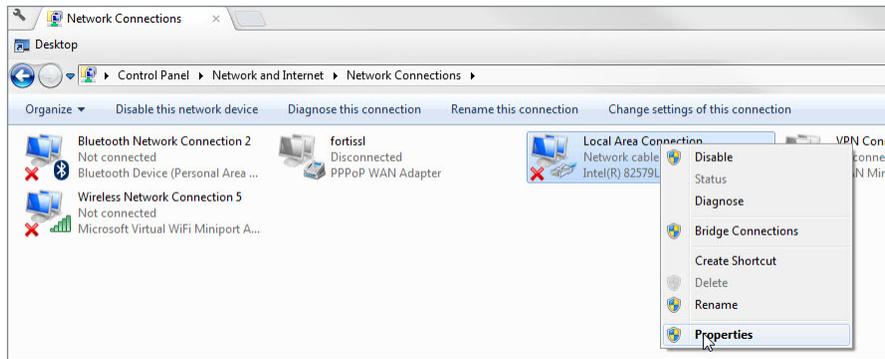
3. Click **Network and Sharing Center**.



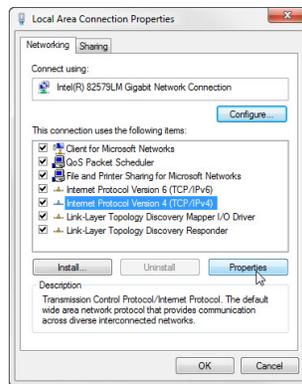
4. In the left bar, click **Change adapter settings**.



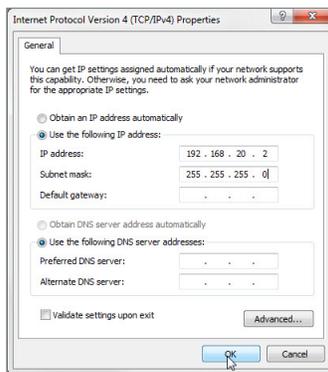
- Right-click the icon for the wired network connection in use and click **Properties**.



- Click to highlight **Internet Protocol Version 4 (TCP/IPv4)**, then click **Properties**.



- In the General tab, click **Use the following IP address:** and enter the IP address and subnet mask.
  - IP Address: **192.168.20.2**
  - Subnet Mask: **255.255.255.0**



- Click **OK** to close **Internet Protocol Version 4 (TCP/IPv4) Properties**, then click **OK** to close **Wireless Network Connection Properties**.
- Open a web browser and navigate to **http://192.168.20.253/**.
- Enter your login credentials and log in.
  - Default Login Credentials** – Username: **araknis**; Password: **araknis**

## 5 - Web Interface Overview

Figure 5. Web Interface Layout

The screenshot shows the Araknis Networks web interface. At the top left is the Araknis Networks logo. The top bar (C) displays 'CLOUD SERVER: Connected', 'System Time: 2017-06-14 09:57:34', and 'System Uptime: 20:33:38'. The main navigation menu (A) on the left includes sections for STATUS, SETTINGS, MAINTENANCE, and ADVANCED. The main window (B) displays the 'SYSTEM STATUS' page, which is divided into three sections: System Information, Wireless Information, and LAN Information.

**System Information**

System Name	AN-700-AP-O-AC
Service Tag	ST17190064138412
Firmware Version	1.0.00
Management VLAN ID	Untagged

**Wireless Information**

	2.4GHz	5GHz
MAC Address	D4:6A:91:5D:82:C9	D4:6A:91:5D:82:CA
Number of Networks	1	1
Number of Connected Clients	0	0
Operation Mode	Access Point	Access Point
TX	0 Bytes	414016 Bytes
RX	0 Bytes	0 Bytes

**LAN Information**

	LAN1	LAN2		
Speed	1Gbps	Not Connected	IP Address	192.168.6.74
Duplex	Full	--	Subnet Mask	255.255.254.0
MAC Address	D4:6A:91:5D:82:C7	D4:6A:91:5D:82:C8	Default Gateway	192.168.6.1
TX	6230902 Bytes	0 Bytes	Primary DNS	192.168.6.1

- **A - Main Navigation Menu**  
Use the submenus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the access point. Click **Apply Changes** to review and apply changes saved in menus.
- **B - Main Window**  
The main window displays the currently selected submenu.
- **C - Top Bar**  
The top bar displays the current connection status to the OvrC server, the current internally-set system time, and the current system uptime in DAYS:HOURS:MINUTES.

**Note** - 100 Series WAPs will indicate settings and information for the 2.4GHz channel only (no 5GHz support). 300/500/700 Series will indicate settings and information for 2.4GHz and 5GHz channels.

Indoor series WAPs will indicate settings and information for only LAN port 1 (no second LAN port is offered). Outdoor series WAPs will indicate settings and information for both LAN ports 1 and 2.

## 5.1 - Applying Changes in the Web Interface

1. After making changes to settings on a menu page, click the **Save** button on the menu to hold the new settings in the Apply Changes field.
2. After all desired changes have been made, click **Apply Changes** to review the new settings.
3. Click **Apply** to make the changes or **Revert** to cancel the changes.

Figure 6. Applying Changes

The figure consists of two screenshots of the Araknis Networks web interface, illustrating the process of applying changes.

**Top Screenshot: LAN SETTINGS**

The interface shows the 'LAN SETTINGS' page. The left sidebar contains a navigation menu with 'SETTINGS' selected. The main content area is divided into 'IP Settings' and 'Interface Settings'. The 'IP Settings' section includes fields for IP Address (192.168.20.253), Subnet Mask (255.255.255.0), Default Gateway (192.168.20.253), Primary DNS (8.8.8.8), and Secondary DNS (8.8.8.8). The 'DHCP' section has an 'Enable' checkbox. The 'Interface Settings' section includes 'Speed' (Auto) and 'Duplex' (Full) dropdown menus. At the bottom right, there are 'Save' and 'Cancel' buttons. A red box highlights the 'Apply Changes: 4' button at the bottom left.

**Bottom Screenshot: APPLY CHANGES**

The interface shows the 'APPLY CHANGES' page. The left sidebar contains a navigation menu with 'MAINTENANCE' selected. The main content area is titled 'Unsaved' and contains an 'Unsaved changes list' box with the following text:

```
dhcp.cf@02a28d.resolvfile=/tmp/resolv.conf
network.lan.proto=static
network.lan.accept_ra=0
network.lan.dns=8.8.8.8 8.8.8.8
```

At the bottom right, there are 'Apply' and 'Revert' buttons. A red arrow points from the 'Apply Changes: 4' button in the top screenshot to the 'Apply' button in this screenshot.

## 6 - System Status

The System Status screen provides a real-time summary of access point system information, and is the first screen that appears when you log into the access point web interface. Use the screen to verify settings and operation of your device.

Figure 7. System and Wireless Information

System Information		
System Name	AN-700-AP-O-AC	
Service Tag	ST17190064138412	
Firmware Version	1.0.00	
Management VLAN ID	Untagged	
Wireless Information		
	2.4GHz	5GHz
MAC Address	D4:6A:91:5D:82:C9	D4:6A:91:5D:82:CA
Number of Networks	1	1
Number of Connected Clients	0	0
Operation Mode	Access Point	Access Point
TX	0 Bytes	414016 Bytes
RX	0 Bytes	0 Bytes

### 6.1 - System Information

Displays current information about the WAP's system settings.

Path – Status, System, System Information

#### Parameters

- **System Name** – Name assigned to the system. Used for configured name access.
- **Service Tag** – Internal tracking number used to track every product sold by Araknis Networks.
- **Firmware Version** – Current version of firmware running on the access point.
- **Management VLAN ID** – VLAN that must be used to access the web interface.

### 6.2 - Wireless Information

Displays current information about the wireless radio channel(s) in use.

Path – Status, System, Wireless Information

#### Parameters

- **MAC Address** – Media Access Control (MAC) address. The 2.4GHz and 5GHz channels each have individual MAC addresses.
- **Number of Networks** – Number of active wireless networks (i.e. SSID's) configured on the radio interface.
- **Number of Connected Clients** – Number of currently connected wireless clients on all configured networks using the radio interface.
- **Operation Mode** – Indicates whether the radio is configured as an access point or a repeater.
- **TX** – Amount of data, in bytes, transmitted on the radio interface since the last power cycle.
- **RX** – Amount of data, in bytes, received on the radio interface since the last power cycle.

Figure 8. LAN Information and System Log

**LAN Information**

	LAN1	LAN2		
Speed	1Gbps	Not Connected	IP Address	192.168.6.74
Duplex	Full	--	Subnet Mask	255.255.254.0
MAC Address	D4:6A:91:5D:82:C7	D4:6A:91:5D:82:C8	Default Gateway	192.168.6.1
TX	6230902 Bytes	0 Bytes	Primary DNS	192.168.6.1
RX	38629808 Bytes	0 Bytes	Secondary DNS	

**System Log**

```

Jun 14 09:25:09 AN700OUTDOOR user.warn kernel: FWLOG: [73813745] WAL_DBGID_SECURITY_MCAST_KEY_SET ( 0x2 )
Jun 14 09:25:09 AN700OUTDOOR user.warn kernel: TXRX: sec spec for peer 8e6ff000 (d4:6a:91:5d:82:ca): mcast key of type 6
Jun 14 09:25:09 AN700OUTDOOR user.warn kernel: Setting vdev param = 1f, value = 2
Jun 14 09:25:09 AN700OUTDOOR user.warn kernel: Keydata=0xec 0x38 0xc8 0x32 0x93 0xec 0x8d 0x68 0x73 0xc5 0x8b 0x9f 0xe2 0x6f
Jun 14 09:25:09 AN700OUTDOOR user.warn kernel: Keyix=2 Keylen=16 Keyflags=1 Cipher=4
Jun 14 09:25:09 AN700OUTDOOR user.warn kernel: wmi_unified_vdev_install_key_send Setting Key for Macaddress:0xca825d916ad4
Jun 14 09:08:12 AN700OUTDOOR daemon.notice miniupnpd[1202]: / not found, responding ERROR 404
Jun 14 08:25:10 AN700OUTDOOR user.warn kernel: FWLOG: [70127353] WAL_DBGID_SECURITY_MCAST_KEY_SET ( 0x1 )
Jun 14 08:25:09 AN700OUTDOOR user.warn kernel: TXRX: sec spec for peer 8e6ff000 (d4:6a:91:5d:82:ca): mcast key of type 6
Jun 14 08:25:09 AN700OUTDOOR user.warn kernel: Setting vdev param = 1f, value = 1
    
```

### 6.3 - LAN Information

Displays current LAN connection parameters.

Path – Status, System, LAN Information

#### Parameters

- **Speed** – Indicates negotiated LAN speed between the access point and the wired network.
- **Duplex** – Indicates the negotiated duplex setting between the access point and the wired network.
- **MAC address** – The MAC address assigned to the LAN port. LAN port 1 MAC address is always primary.
- **TX** – Amount of data, in bytes, transmitted over the wired network connection.
- **RX** – Amount of data, in bytes, received from the wired network connection.
- **IP Address** – Access point IP address issued by the network router.
- **Subnet Mask** – Access point subnet mask.
- **Default Gateway** – Network router IP address.
- **Primary DNS** – Indicates the primary DNS for the device.
- **Secondary DNS** – Indicates the secondary DNS for the device.

### 6.4 - System Log

The System Log records changes to configuration, connections, security conditions, and more.

Path – Status, System, System Log

#### Parameters

- **Save Log** – Click to view the log as a text file or save the log for future reference.
- **Clear Log** – Click to permanently delete to contents of the System Log.

## 7 - Wireless Interface Status

Provides a detailed look at wireless settings and performance for radio status and settings, wireless network configuration and connected client status.

### 7.1 - Radio Status

Provides a detailed look at radio settings and performance.

Figure 9. Radio Status

Radio Status		
	2.4GHz	5GHz
Interface Status	Enabled	Enabled
Operation Mode	Access Point	Access Point
Wireless Mode	? 802.11 B/G/N	802.11 A/N
Channel Bandwidth	? 20MHz	40MHz
Channel Selection	? 6	Auto
Operating Channel	? Channel 6	Channel 161
Channel Frequency	? 2.437 GHz	5.805 GHz
TX	0 Bytes	0 Bytes
RX	0 Bytes	0 Bytes

Path - Status, Wireless interface, Radio Status

#### Parameters

- **Interface Status** - Indicates whether the wireless antenna is enabled or disabled.
- **Operation Mode** - Indicates whether the antenna is operating in Access Point or Repeater mode.
- **Wireless Mode** - Indicates the Wi-Fi protocol(s) currently in use with the band frequency.
- **Channel Bandwidth** - Indicates the current channel bandwidth.
- **Channel Selection** - Indicates the current channel setting.
- **Operating Channel** - Indicates the current operating channel.
- **Channel Frequency** - Indicates the frequency of the operating channel.
- **TX** - Amount of data transmitted in bytes.
- **RX** - Amount of data received in bytes.

## 7.2 - Utilization of SSID

Details the use and availability of SSID's configured in the WAP.

Figure 10. Utilization of SSID Status

Utilization of SSID		
	2.4GHz	5GHz
SSID's Used	1	2
SSID's Available	7	6

Path - Status, Wireless interface, Wireless Network

### Parameters

- **SSID's Used** - Number of SSID's currently in use by devices connected to the access point.
- **SSID's Available** - Number of SSID's available for use.

### 7.2.1 - Wireless Network

The Wireless Network table provides a detailed look at wireless network settings.

Figure 11. Wireless Network Status

Wireless Network							
Wireless Network(SSID) ▲	Enabled	Interface	Security ?	VLAN ID	MAC Address	Broadcast SSID ?	Client Isolation ?
HomeLan1	Yes	2.4GHz	WPA2/PSK AES		D4:6A:91:32:3B:57	Yes	No
HomeLan1	Yes	5GHZ	WPA2/PSK AES		D4:6A:91:32:3B:58	Yes	No
Repeater	Yes	5GHZ	WPA2/PSK AES		D6:6A:91:32:3B:58	No	No

Path - Status, Wireless interface, Wireless Network

### Parameters

- **Wireless Network (SSID)** - Network names (SSID's) being transmitted by the access point.
- **Enabled** - Indicates whether the wireless network is enabled or disabled.
- **Interface** - Indicates the operating frequency of the wireless network.
- **Security** - Indicates the security mode selected for the wireless network.
- **VLAN ID** - Indicates the VLAN ID for the wireless network.
- **MAC address** - MAC address of the wireless channel used by the network.
- **Broadcast SSID** - Indicates whether the SSID is visible to Wi-Fi devices and discovery tools.
- **Client Isolation** - Indicates whether access point client devices connected to different SSID's can communicate with each other.

### 7.3 - Connected Clients

The Connected Clients table provides a detailed look at connected wireless clients. All devices connected to any SSID on the access point will be displayed in the list.

Figure 12. Connected Client Status

Connected Clients							Refresh
Status	Wireless Network(SSID) ▾	Device Name ▾	MAC Address ▾	TX(KBytes) ▾	RX(KBytes) ▾	RSSI(dbm) ?	Release
<input checked="" type="checkbox"/>		android-195ba27c3ee030	58:3F:54:7D:67:88				Deny

Path – Status, Wireless interface, Connected Clients

#### Parameters

- **Status** – Indicates whether the client is currently connected. Green indicates that the client is connected to the SSID.
- **Wireless Network (SSID)** – Indicates the SSID being used by a connected wireless client.
- **Device Name** – Name either pulled from or assigned to the client.
- **MAC address** – Indicates the MAC address of a connected wireless client.
- **TX (KBytes)** – Amount of data, in kilobytes, transmitted to a connected wireless client.
- **RX (KBytes)** – Amount of data, in kilobytes, received from a connected wireless client.
- **RSSI (dBm)** – Indicates the wireless signal strength between the access point and the connected client. The color of the table field indicates signal quality: green=strong, yellow=medium, and red=weak.
- **Release** – Click the **Deny** button to drop a client from the network.

**i Pro Tip** – The closer RSSI (dBm) value is to 0, the stronger the signal is, and the closer to -100, the weaker the signal is.

## 8 - System Settings

### 8.1 - System Information

The System Information screen allows configuration of admin and access settings.

Figure 13. System Information

System Information	
System Name	an300
Admin Username	admin
Admin Current Password	<input type="password"/>
Admin New Password	<input type="password"/>
Confirm Admin New Password	<input type="password"/>
System LED	<input checked="" type="radio"/> ON <input type="radio"/> OFF
Management VLAN	<input type="radio"/> Untagged <input type="radio"/> Tagged 4096
Country	United States

Path – Settings, System, System Information

#### Parameters

- **System Name** – Enter a meaningful name such as *SmithHome* or *SmithBasement*. Limited to 32 characters, including spaces.
- **Admin Username** – Enter a username for logging into the access point. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.  
*Default: araknis*
- **Admin Current Password** – Enter the current login password when changing the password.  
*Default: araknis*
- **Admin New Password** – Enter a new login password. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.
- **Confirm Admin New Password** – Confirm a new login password (enter same password as above).
- **System LED** – Turn the Status LED ON or OFF.  
*Default: ON*
- **Management VLAN** – The VLAN ID from where the WAP web interface must be accessed.  
*Default: Untagged*

**Caution** – Changing the management VLAN could cause a loss of access to the web interface. Move the computer to the new management VLAN or reset the WAP to regain connectivity (see section [4.2 - Configured System Name Access \(p.9\)](#)).

- **Country** – Select the country of the install location to comply with local standards. Setting is not available for the AN-700-AP-O-AC outdoor WAP.  
*Default: United States*

#### Configuration Instructions

1. Configure the system information settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 8.2 - Date and Time Settings

Configure the system date and time settings. System time will be displayed in various menus and logs.

**i** **Pro Tip** – We strongly recommend using the default auto setting for date and time. Manual settings may not remain accurate after power outages or resets. Be sure to set the time zone and DST settings correctly. See the next page for instructions.

Figure 14. Date and Time Settings

Path – Settings, System, Date and Time Settings

### Parameters

- **Manually Set Date and Time** – Select to manually set date and time.
  - **Date** – Enter the year, month and date (four digits for year; two digits for month, two digits for date)
  - **Time** – Enter the hour and minutes for the correct current time. Use a mobile device or satellite clock for accuracy.
- **Synchronize with PC** – Click this button to automatically sync the access point to a connected computer.
- **Automatically Get Date and Time** – Automatically get date and time from a 3rd-party web server.
  - **NTP Server** – Select an NTP (Network Time Protocol) Server to set reference standard date and time.  
*Default: time.nist.gov (recommended)*

### Configuration Instructions

1. Configure the desired time settings. We recommend using the default settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.
3. Be sure to configure the time zone and DST settings correctly too. See the next page for instructions.

## 8.3 - Time Zone Settings

Configure the time zone and DST settings for the install location.

Figure 15. Time Zone Settings

**Time Zone**

Time Zone: UTC-05:00 Eastern Time (US & Canada)

Enable Daylight Saving

Start: March 2nd Sun 02:00

End : November 1st Sun 02:00

Save Cancel

Path – Settings, System, Date and Time Settings

### Parameters

- **Time Zone** – Select the appropriate time zone from the drop-down.
- **Enable Daylight Saving** – Select to enable. DST start/end can change from year to year. Be sure to update this information.
  - Start – Select the month, date, day and time Daylight Saving Time starts from the drop-downs.
  - End – Select the month, date, day and time Daylight Saving Time ends from the drop-downs.

### Configuration Instructions

1. Select the correct time zone for your install location.
2. Configure the DST settings as desired.
3. Click **Save**, then **Apply Changes** to enable the new settings.

## 9 - LAN Settings

### 9.1 - IP Settings

Configure access point IP address settings.

Figure 16. IP Settings

IP Settings	
IP Address	192.168.20.253
Subnet Mask	255.255.255.0
Default Gateway	192.168.20.253
Primary DNS	8.8.8.8
Secondary DNS	8.8.8.8
DHCP	<input type="checkbox"/> Enable

Path - Settings, LAN, IP Settings

#### Parameters

- **IP Address** - Uncheck **DHCP Enable** to enter a static IP address for the device.
- **Subnet Mask** - Enter the subnet mask for the device.  
*Default: 255.255.255.0*
- **Default Gateway** - With DHCP disabled, enter the default gateway for the access point (network router IP address).
- **Primary DNS** - With DHCP disabled, enter the primary DNS for the device. This is typically the network router IP address.
- **Secondary DNS** - With DHCP disabled, enter the secondary DNS for the device. This is typically be the network router IP address.

 **Note** - Both primary and secondary DNS addresses are required if a static IP address is assigned.

- **DHCP** - Allows the access point to receive a DHCP IP address from the network router if DHCP is enabled. Uncheck the box to configure a static IP address.  
*Default: Enabled*

#### Configuration Instructions

1. Specify the IP settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

#### 9.1.1 - IP Address Setup: Best Practices

- We recommend leaving the WAP set to DHCP and reserving an IP address in the network router whenever possible.
- If using an unreserved DHCP address, be aware that it may change unexpectedly. Use OvrC to easily find the address again.
- If using a manually configured static IP address:
  - Use an IP address that is outside the DHCP server range to avoid duplicate addresses in the network.
  - Both primary and secondary DNS addresses are required.

## 9.2 - Interface Settings

Configure LAN speed and duplex settings for the LAN port(s).

Figure 17. Interface Settings

Interface Settings		
	LAN1	LAN2
Speed	 Auto ▾	Auto ▾
Duplex	 Full ▾	Full ▾

Path – Settings, LAN, Interface Settings

### Parameters

- **Speed** – Select LAN speed from Auto, 1Gbps (300/500/700 Series only), 100Mbps, 10Mbps, Disable (Disable turns the LAN Port OFF)  
*Default: Auto*
- **Duplex** – (10/100Mbps modes only) Select the duplex setting between the access point and the network router from Half or Full.  
*Default: Full*

 **Note** – We strongly recommend leaving auto Speed and Duplex settings in place unless you have a specific reason to change them such as troubleshooting or for compatibility with older equipment.

 **Note** – For the AN-700-AP-O-AC, we strongly recommend using the auto setting to avoid issues.

### Configuration Instructions

1. Configure the interface settings as desired.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 10 - Wireless Settings

### 10.1 - Radio Settings

Configure the access point's radio settings including wireless modes, operating channels, channel bandwidth, and extension channel.

Figure 18. Radio Settings

Radio Settings		
	2.4GHz	5GHz
Enable Interface	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes
Operation Mode	Access Point ▼	Access Point ▼
Wireless Mode	802.11 B/G/N ▼	802.11 A/N ▼
Operating Channel	Ch6-2.437GHz ▼	Auto ▼
Channel Bandwidth	20 MHz ▼	40 MHz ▼
Extension Channel	Upper Channel ▼	

Path - Settings, Wireless, Radio Settings

#### Parameters

- Enable Interface** - Check or uncheck to enable or disable the radio interface.  
*Default: Yes.*
- Operation Mode** - Set the radio to Access Point or Repeater mode. See [10.7 - Repeater Mode Setup \(p.35\)](#) for repeater setup instructions.  
*Default: Access Point*
- Wireless Mode** - Select the wireless mode for the radio.  
*Default: 2.4GHz - 802.11b/g/n; 5GHz - 802.11a/n (300), 802.11ac/n (500/700).*
- Operating Channel** - Select the desired Wi-Fi channel. Use a different channel than other WAPs on the network. On the 2.4GHz radio, there are only three non-overlapping channels: 1, 6 and 11. Select a channel as far away from close-numbered channels as possible.  
*Default: Auto.*

**Pro Tip** - In a multi-WAP environment, put adjacent WAPs on channels as far apart as possible. A spectrum analyzer tool (such as Metageek's Chanalyzer Pro) is recommended for providing insight into the network setup. See the [Araknis Guide to Successful Wi-Fi Installation](#) on the product page support tab for more information.

- Channel Bandwidth** - Select the desired channel bandwidth. Smaller values allow greater range and larger values provide greater throughput. The combination setting allows the WAP to decide.  
*Default: 2.4GHz - 20MHz; 5GHz - 40MHz (300), 80MHz (500/700)*
- Extension Channel** - Specify whether the channel extends above or below the normal 20MHz range. Only applies when the Channel Bandwidth is set higher than 20MHz.  
*Default: 2.4GHz - Upper Channel; 5GHz - Lower Channel.*

#### Configuration Instructions

1. Configure the radio settings as desired.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 10.2 - Utilization of SSID

Details the use and availability of SSID's configured in the WAP.

Figure 19. Utilization of SSID Status

Utilization of SSID		
	2.4GHz	5GHz
SSID's Used	1	2
SSID's Available	7	6

Path – Settings, Wireless, Utilization of SSID

### Parameters

- **SSID's Used** – Number of SSID's currently in use by devices connected to the access point.
- **SSID's Available** – Total number of SSID's available.

## 10.3 - Global Wireless Settings

Configure Band Steering and Fast Roaming.

Figure 20. Global Wireless Settings

Global Settings	
Band Steering	<input type="checkbox"/> OFF <small>NOTE: Band Steering is not supported in repeater mode.</small>
Fast Roaming	<input type="checkbox"/> ON <small>NOTE: Fast Roaming is not supported on the radio in use as the repeater.</small>

Path – Settings, Wireless, Global Wireless Settings

### Parameters

- **Band Steering** – (300/500/700 Series only) This feature pushes clients to the 5 GHz radio if a client is compatible. We recommend enabling this feature for the best performance. Click the button to toggle between on and off.
- **Fast Roaming** – This feature allows clients to seamlessly switch between multiple WAPs transmitting the same SSID based on which WAP will provide the best signal at any time. See section [10.3.1 - Fast Roaming Setup \(p.26\)](#) for setup requirements and instructions.

### Configuration Instructions

1. Configure the settings as desired.
2. Click **Save**, then **Apply Changes** to enable the new settings.

### 10.3.1 - Fast Roaming Setup

This powerful feature, known in Araknis products as Fast Roaming, is essential for building reliable Wi-Fi networks with multiple access points. After a client joins a Wi-Fi network, they don't always stay close to the WAP they originally connected to.

Without Fast Roaming, the client will remain connected to one WAP until signal is lost, then find a new connection. Fast Roaming tells the client when to move the connection, then makes the switch with minimal delay. This keeps clients on the fastest and most reliable WAP at all times.

#### Installation Notes and Frequently Asked Questions

- **WEP security mode does NOT work with Fast Roaming.**  
Configure SSIDs using other encryption modes.
- **How do I configure the locations of WAPs for the best performance?**  
Use a site analyzer tool to determine ideal WAP locations. For the best performance, use more WAPs closer together and reduce the transmit power some to avoid interference (Advanced Wireless Settings).
- **Does it matter what operating channel is used?**  
If you aren't using Auto Operating Channel selection, use a different wireless radio channel in each WAP to lower the amount of interference each device encounters.
- **Do fast roaming and band steering work together?**  
Yes, configure each one based on individual needs. Remember, some devices may not be compatible with these features.
- **How do I set up Guest Networks with Fast Roaming enabled?**  
The guest network feature is not ideal for use with Fast Roaming since each WAP creates a new DHCP server for clients connected to that SSID. Instead, create a separate VLAN and assign SSIDs for guest use. See section [19.1 - Configuring Guest Networks with Fast Roaming \(p.68\)](#) for setup instructions.
- **Is this a proprietary technology for Araknis Networks?**  
No. Fast Roaming utilizes the standard IEEE 802.11r and 802.11k to negotiate handoff with the client. Only clients that support 802.11r/k are able to perform best in this environment.
- **Do any other WAP brands that support Handoff work with Araknis Fast Roaming?**  
We don't guarantee compatibility with any other brands, but will list them if we find any that are.
- **Does any equipment NOT work with Fast Roaming/Handoff?**  
Gen 1 Apple iOS products won't work. Most newer iOS devices work correctly. Check the product page support tab for recent updates on compatibility issues.

## Special Setup Requirements

- Two or more WAPs, all with wired LAN connections
- All WAPs set to Access Point operating mode with Fast Roaming enabled
- Same SSID configuration on each WAP

## Configuration Instructions

1. In the first WAP, go to the Settings, Wireless menu and configure the desired SSID's.

Wireless Networks							
Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation	Delete	
<input checked="" type="checkbox"/> Yes	Low Signal Strength!	Both	WPA2-PSK	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable		
<input checked="" type="checkbox"/> Yes	Outdated	Both	WPA2-PSK	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable		
<input checked="" type="checkbox"/> Yes		2.4GHz	Open	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable		

2. On the same menu page, under Global Settings, turn Fast Roaming ON.

Global Settings	
Band Steering	<input type="checkbox"/> OFF <small>NOTE: Band Steering is not supported in repeater mode.</small>
Fast Roaming	<input checked="" type="checkbox"/> ON <small>NOTE: Fast Roaming is not supported on the radio in use as the repeater.</small>

3. Click **Save**, then complete the **Apply Changes** process to enable the new settings.
4. Repeat steps 1-3 in the remaining WAPs.
5. After setup, test the new settings using several client devices. You should see the client device listed in each WAP's Connected Clients table (Path: Status, Wireless Interface).

Connected Clients							Refresh
Status	Wireless Network(SSID)	Device Name	MAC Address	TX(KBytes)	RX(KBytes)	RSSI(dbm)	Release
<input checked="" type="checkbox"/>	Low Signal Strength!	android-1958e62764ee00f0	58:3F:54:F0:67:98	911	843	-54	<input checked="" type="checkbox"/> Yes

**Save** **Cancel**

## Troubleshooting

If certain devices don't work once Fast Roaming is enabled, try turning Fast Roaming off and checking for connection again. The device might be incompatible with Fast Roaming.

## 10.4 - Wireless Networks

The Wireless Networks menu allows configuration of access point wireless networks (SSID's), security settings, band steering and channel isolation.

**Note** - Be sure to change the SSID. The default settings are not secure.

Figure 21. Wireless Networks

Wireless Networks							
Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation	Delete	
<input checked="" type="checkbox"/> Yes	<input type="text" value="HomeLan1"/>	<input type="text" value="Both"/>	<input type="text" value="WPA2-PSK"/>	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable		
<input checked="" type="checkbox"/> Yes	<input type="text" value="Repeater"/>	<input type="text" value="5GHz"/>	<input type="text" value="WPA2-PSK"/>	<input type="checkbox"/> Yes	<input type="checkbox"/> Enable		

**Add**

Path - Settings, Wireless, Wireless Networks

### Parameters

- Enable** - Select **Yes** to turn a wireless network ON.  
*Default: Yes (Checked)*
- Name (SSID)** - Enter the network name for the network being configured. Be sure to change the default SSID; the settings are not secure.  
*Default: araknis\_initial (Blank when adding a new network).*
- Interface** - Select 2.4GHz/5GHz or Both Channel Frequency.  
*Default: Both, (2.4GHz when adding a network).*
- Security Mode** - Configure the security mode for each wireless network. Select a security mode from the drop-down to open the Wireless Security Setup Window. See section [10.5 - Wireless Security Options \(SSID Encryption\) \(p.30\)](#) for wireless security setup options.  
*Default: Open*
- Broadcast SSID** - Select whether or not to publicly display the SSID to nearby Wi-Fi devices.  
*Default: Yes*
- Channel Isolation** - Select to prevent communication between wireless clients on different SSID's. Enable this setting if you don't want Wi-Fi clients on the SSID to "see" each other, such as in a public place.  
*Default: Not selected.*
- Add** - Click to add a wireless network.
- Delete** - Click to delete a wireless network. The first SSID cannot be deleted.

### 10.4.1 - Configuring a New SSID

Wi-Fi setup varies depending on the application and the security method(s) used. To learn more about general setup, see the [Araknis Guide to Successful Wi-Fi Installation](#) on the product page support tab.

1. From the Wireless Settings page, scroll to the Wireless Networks menu.
2. Click **Add** if you are creating a new SSID, otherwise modify the settings for the default SSID.
3. Configure these following fields as desired:
  - A. **Name (SSID)** - Enter the desired name for the SSID.
  - B. **Interface** - Select the desired interface, either **2.4 GHz**, **5 GHz**, or **both**. We recommend using **Both** unless requirements specify a certain frequency.
  - C. **Broadcast SSID** - Select whether or not the SSID will be visible to in-range devices. If you uncheck the box, users will need to manually enter the SSID to connect.
  - D. **Client Isolation** - Check the box to prevent devices on the SSID from seeing each other. Enable this setting for SSIDs that will be accessed by unknown users.
4. Click the Security Mode drop-down and select an option.
5. A new window will appear with settings for the security mode. The settings vary depending on the mode. Refer to the proper section and configure the wireless settings as desired, then click Save to return to the main screen.
  - **Open** - Not recommended. Anyone that can find or see the SSID may connect.
  - **WEP** - [10.5.1 - WEP Mode \(p.30\)](#)
  - **WPA-PSK or WPA2-PSK** - [10.5.2 - WPA-PSK Mixed and WPA2-PSK Modes \(p.31\)](#)
  - **WPA or WPA2** - [10.5.3 - WPA and WPA2 Modes \(p.32\)](#)
6. The SSID is configured. Click **Save**, then **Apply Changes** for the new settings to take effect.

## 10.5 - Wireless Security Options (SSID Encryption)

### 10.5.1 - WEP Mode

**Note** - WEP encryption may only be used on the first configured SSID and only if WPS is disabled. See section [18.3 - WPS Settings \(p.56\)](#) for more information about WPS.

**Caution** - It is not recommended to use WEP for SSID security. WEP mode is outdated and far less secure than the other options available, and only included to guarantee connectivity for legacy wireless devices. Use WPA or WPA2 mode unless a device only supports WEP.

Figure 22. Wireless Security - WEP Mode

Wireless Security	
Name (SSID)	"HomeLan1"
Security Mode	WEP
Auth Type	Open System
Input Type	Hex
Key Length	64-bit (10 hex digits or 5 ASCII char)
Default Key	1
Key1	<input type="text"/>
Key2	<input type="text"/>
Key3	<input type="text"/>
Key4	<input type="text"/>

#### Parameters

- **Name (SSID)** - The name of the SSID being configured.
- **Security Mode** - Displays the current selected mode. Select a different encryption mode from the drop-down.
- **Auth Type** - Select Open System or Shared Key mode from the drop-down:
- **Input Type** - Select Hex or ASCII from the drop-down.
- **Key Length** - Select 64 or 128 bit encryption from the drop-down.
- **Default Key** - Select which of the 4 keys is the default value.
- **Key (1-4)** - Enter up to 4 unique identification keys for WEP.
- **Save** - Click to save changes to the Wireless Security Settings for this network. The window will close.
- **Cancel** - Click to cancel changes. The window will close.

## 10.5.2 - WPA-PSK Mixed and WPA2-PSK Modes

Figure 23. Wireless Security – WPA-PSK and WPA2-PSK Modes

Wireless Security	
Name (SSID)	"WAP2"
Security Mode	WPA2-PSK
Encryption	AES
Passphrase	.....
Group Key Update Interval	3600

### Parameters

- **Name (SSID)** – The name of the network being configured.
- **Security Mode** – Displays the current selected mode. Select a different encryption mode from the drop-down.
- **Encryption** – WPA2-PSK: AES; WPA2-PSK Mixed: Both (TKIP+AES).
- **Passphrase** – Enter the appropriate passphrase for the wireless network being configured. If using the ASCII format, the password must be 8-63 characters in length. If using HEX, the password must be 64 HEX characters in length.  
*Default: Blank*
- **Group Key Update Interval** – Enter a value to specify how often in seconds the Group key changes.  
RANGE: 30-3600 seconds.  
*Default: 3600 (60 minutes)*
- **Save** – Click to save changes to the Wireless Security Settings for this network. The window will close.
- **Cancel** – Click to cancel changes. The window will close.

### 10.5.3 - WPA and WPA2 Modes

**Note** - For RADIUS setup, refer to the instructions provided for the server.

**Figure 24.** Wireless Security – WPA-PSK and WPA2-PSK Modes

Wireless Security	
Name (SSID)	"araknia_initial"
Security Mode	WPA2
Encryption	AES
Group Key Update Interval	3600
Radius Server	
Radius Port	1812
Radius Secret	
Radius Accounting	Disable
Radius Accounting Server	
Radius Accounting Port	1813
Radius Accounting Secret	
Interim Accounting Interval	600

Save Cancel

- **Name (SSID)** – The name of the network being configured.
- **Security Mode** – Select a different encryption mode from the drop-down.
- **Encryption** – WPA2: AES; WPA Mixed: Both (TKIP+AES).
- **Group Key Update Interval** – Enter how often the Group Key changes (from 30-3600 seconds).  
*Default: 3600 (60 minutes)*
- **Radius Server** – Enter the Radius Server IP address.  
*Default: Blank*
- **Radius Port** – Enter the Radius Server connection port number.  
*Default: 1812 (This is a dedicated TCP/UDP port and typically should not be changed.)*
- **Radius Secret** – Enter the Radius Server connection secret.  
*Default: Blank*
- **Radius Accounting** – Enable or disable Radius Accounting.  
*Default: Disable*
- **Radius Accounting Server** – Enter the Radius Accounting Server IP address.  
*Default: Blank*
- **Radius Accounting Port** – Enter the Radius Accounting Server connection port number.  
*Default: 1813 (This is a dedicated TCP/UDP port and typically should not be changed.)*
- **Radius Accounting Secret** – Enter the Radius Accounting Server connection secret.  
*Default: Blank*
- **Interim Accounting Interval** – Enter a value for how often accounting data will be sent, in seconds.  
RANGE: 60-600 seconds.  
*Default: 600 (10 minutes)*
- **Save** – Click to save changes. The window will close.
- **Cancel** – Click to cancel changes. The window will close.

## 10.6 - Guest Network Setup

Used to give guests limited wireless network access by using different security credentials and SSIDs.

Figure 25. Guest Network

Guest Network					
Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation
<input type="checkbox"/>					
Yes	Araknis-2.4_GuestNetwork	2.4GHz	Open	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Enable
<input type="checkbox"/>					
Yes	Araknis-2.4_GuestNetwork	5GHz	Open	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Enable
Manual IP Settings					
Gateway IP Address		192.168.200.1			
Subnet Mask		255.255.255.0			
Automatic DHCP Server Settings					
Starting IP Address		192.168.200.100			
Ending IP Address		192.168.200.200			
WINS Server IP		0.0.0.0			

Path – Settings, Wireless, Guest Network

### Parameters

- **Enable** – Check the box to enable a guest network.  
*Default: Disabled*
- **Name (SSID)** – Enter an SSID for the guest network.  
*Default: Araknis-2.4\_GuestNetwork*
- **Interface** – Displays the wireless radio used for the guest network (2.4 or 5.0 GHz).
- **Security Mode** – Select a security mode for the SSID. Guest networks are limited to Open, WPA-PSK Mixed and WPA2-PSK encryption modes.  
*Default: Open*
- **Broadcast SSID** – Select whether or not to publicly display the SSID to nearby Wi-Fi devices.  
*Default: Not selected*
- **Channel Isolation** – Select to prevent communication between wireless clients on different SSID's of the guest network.  
*Default: Selected*
- **Manual IP Settings** – Settings for the guest network DHCP server. All guest clients are placed on a different subnet as configured in this area.
  - **Gateway IP Address** – Enter the Guest Network Gateway IP address.  
*Default: 192.168.200.1*
  - **Subnet Mask** – Enter the subnet mask for the Guest Network Gateway.  
*Default: 255.255.255.0*
- **Automatic DHCP Server Settings** – Configure the IP addresses issued to guest clients.
  - **Starting IP Address** – Enter the lowest address available for the Guest Network.  
*Default: 192.168.200.100*
  - **Ending IP Address** – Enter the highest address available for the Guest Network.  
*Default: 192.168.200.200*
  - **WINS Server IP** – Enter the IP address for the WINS Server for the Guest Network.  
*Default: 0.0.0.0*

## Best Practices and Guidelines

- For models with 2.4 and 5GHz radios: With Band Steering enabled, the 2.4 and 5 GHz networks automatically share SSID settings. If Band Steering is not enabled, provide guests with passwords to both the 2.4 and 5GHz network for seamless operation.
- Guest networks are limited to Open, WPA-PSK Mixed and WPA2-PSK encryption modes. See section [10.5.2 - WPA-PSK Mixed and WPA2-PSK Modes \(p.31\)](#) for encryption setup details.

## Configuration Instructions

 **Note** - These instructions only apply if the Fast Roaming feature will not be used for the guest network. To use Fast Roaming on a guest network, see section [19.1 - Configuring Guest Networks with Fast Roaming \(p.68\)](#).

1. Configure the wireless settings for the guest network as desired.
2. The default IP settings allow 101 clients to join. Adjust the number to the desired limit by changing the starting and ending IP addresses.
3. Click **Save**, then **Apply Changes** to enable the new settings.

## 10.7 - Repeater Mode Setup

Repeater mode is used when more Wi-Fi coverage is needed but there is no way to get cables from the wired LAN to new WAP locations. One WAP physically connected to the LAN communicates wirelessly with the repeater WAP(s) and clients connect to the WAPs like normal.

Since repeater mode uses Wi-Fi for communicating with both clients and the LAN, users will have an overall slower experience using their client device. Assume that available bandwidth to a client will be halved for each “hop” the signal completes from WAP to WAP before reaching the wired LAN.

**Pro Tip** – It is always better for performance to hardwire a WAP than use repeater mode, since speeds will be halved with this mode.

### Special Setup Requirements

- At least one WAP with a wired LAN connection
- Additional WAP(s) with local power but no LAN connection (must be in range of the wired WAP)
- SSID configuration on each WAP

### Frequently Asked Questions

- **Do Fast Roaming and Repeater mode work together?**  
Not for the radio being used as a repeater. Fast Roaming is not required for repeater mode.
- **Can repeater WAPs be used as a wireless bridge? (LAN port to switch or client device)**  
Yes. Connect an Ethernet patch cable from the Ethernet port on the repeater WAP to the client device LAN port.
- **Can multiple unwired repeater WAPs connect to one wired WAP?**  
Yes.
- **If a 300/500/700 series WAP is configured using one radio in repeater mode, can I configure more SSIDs on the other radio?**  
Yes. All traffic will be sent to the wired LAN over the repeater antenna.
- **Can an all Araknis WAPs work together using Repeater mode?**  
Yes.

### Configuration Instructions

1. Configure the wired WAP normally, with the radio(s) set to Access Point mode. Optionally, configure an SSID just for the repeater WAP connection on the 2.4 or 5 GHz antenna.

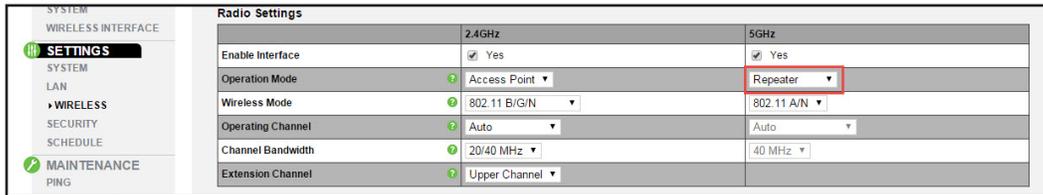
The screenshot shows the configuration interface for a wireless access point. On the left is a navigation menu with options: SYSTEM, WIRELESS INTERFACE, SETTINGS (highlighted), SYSTEM, LAN, WIRELESS, SECURITY, SCHEDULE, MAINTENANCE, and PING. The main area is titled 'Radio Settings' and contains two columns for 2.4GHz and 5GHz configurations. Below this is a 'Wireless Networks' table.

		2.4GHz	5GHz
Enable Interface	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Yes
Operation Mode	Access Point	Access Point	Access Point
Wireless Mode	802.11 B/G/N	802.11 A/N	802.11 A/N
Operating Channel	Auto	Auto	Auto
Channel Bandwidth	20/40 MHz	40 MHz	40 MHz
Extension Channel	Upper Channel		

Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation	Delete
<input checked="" type="checkbox"/> Yes	House WiFi	Both	WPA2-PSK	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable	
<input checked="" type="checkbox"/> Yes	Repeater	5GHz	WPA2-PSK	<input type="checkbox"/> Yes	<input type="checkbox"/> Enable	<input type="button" value="Delete"/>

- In the unwired repeater WAP, go to Settings, Wireless, Radio Settings and set the 2.4 or 5 GHz radio to Repeater mode (to connect to the SSID from the wired WAP).



- Scroll down to the Repeater table on the same page and enter the SSID from the wired WAP in step 1.



- Repeater SSID** - Enter an SSID name for the repeater WAP connection.
  - Interface** - Displays the interface frequency set for repeater mode.
  - Security** - Enter the security credentials for the SSID from the wired WAP in step 1.
  - Target SSID** - Enter the SSID from the wired WAP configured in step 1.
  - Preferred BSSID** - (Optional) enter the MAC address of the radio for the Target SSID. This is required if there are multiple WAPs transmitting the same SSID.
- Click Apply and then Apply Changes to enable the new settings.
  - After setup, connect to each SSID on each WAP and confirm that your client device operates as expected.

## 11 - Security Settings

The Security Settings screen allows configuration of who can log into the access point interface and what level of privileges they have, how the device can be accessed, email notification of system status and warnings, and device discovery.

### 11.1 - User Accounts

The User Accounts menu allows configuration of who can log into the access point and what level of privileges they have.

Figure 26. User Accounts

User Accounts						
Select	Username	Privilege Level	Password	Confirm Password	Delete	
<input type="checkbox"/>	admin	admin	*****	*****		

Path – Settings, Security, User Accounts

#### Parameters

- **Select** – Select to allow editing of the selected table entry.  
*Default: Not selected*
- **Username** – Click the Edit button to access the settings on a selected User Account. Enter a new username for logging into the access point. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.  
*Default: araknis (Blank when adding a new account)*
- **Privilege Level** – Indicates the level of device management for the logged in user. The first user is always the admin, which cannot be changed. OPTIONS: Status, Status+Settings.  
*Default: admin Status+Settings when adding a new account)*
- **Password** – Enter a new login password. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.  
*Default: araknis (Blank when adding a new account)*
- **Confirm Password** – Confirm a new login password (enter same password as above).  
*Default: araknis (Blank when adding a new account)*
- **Delete** – Click the icon to delete a specific user account.
- **Add** – Click to add a new user account.
- **Edit** – Click the **Select** check box in the left column of a user account and click **Edit** to modify the account.

#### Configuration Instructions

1. Specify the user account settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 11.2 - Access Control

Allows configuration of how the access point interface may be accessed.

Figure 27. Access Control

Access Control	
HTTP Port	<input type="text" value="80"/>
Web Access	<input type="button" value="Enable"/>
Telnet	<input type="button" value="Disable"/>
SSH	<input type="button" value="Disable"/>

Path - Settings, Security, Access Control

### Parameters

- **HTTP Port** - Enter device web server port to connect.  
*Default: 80*

**Pro Tip** - Assign a unique port number to enable remote access to the access point web interface via port forwarding on the network router.

- **Web Access** - Select Enable or Disable to enable or disable the ability to modify the device via Web Browser.  
*Default: Enabled*

**Caution** - Disabling web access will cause a loss of connection to the web interface. If this occurs, regain connectivity by restoring the hardware to factory default settings. (Press Reset button for 10 seconds.)

- **Telnet** - Enable or Disable the ability to modify the device via a command line interface (CLI) through a telnet session.  
*Default: Disabled*
- **SSH** - Enable or Disable the ability to modify the device via a command line interface (CLI) with a secure channel.  
*Default: Disabled*

### Configuration Instructions

1. Specify the access control settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 11.3 - Email Alert

The Email Alert menu allows configuration of the email notification system for status and warnings.

Figure 28. Email Alert Setup Example

Email Alert	
Status	<input type="checkbox"/> Enable
From	<input type="text"/>
To	<input type="text"/>
Subject	[Email-Alert][an300][D4:6A:91:32:3B:56] Configuration Changed
Email Account	
Username	<input type="text"/>
Password	<input type="password"/>
SMTP Server	<input type="text"/>
	Port: 25
Security Mode	None ▼
<b>Send Test Mail</b>	

Path – Settings, Security, Email Alerts

### Parameters

- **Status** – Select Enable to send email notifications in the event of certain abnormal conditions.  
*Default: Not selected*
- **From** – Enter the email address of the sender.  
*Default: Blank*
- **To** – Enter the email address of the recipient.  
*Default: Blank*
- **Subject** – Information regarding the nature of the system condition.  
*Default: [Email-Alert][araknis][88:DC:96:1D:33:6B][Configuration Changed]*
- **Email Account** –
  - **Username** – Enter the username for the email account (Outlook, Gmail, etc.) sending the alert.  
*Default: Blank*
  - **Password** – Enter the password for the email account (Outlook, Gmail, etc.) sending the alert.  
*Default: Blank*
  - **SMTP Server** – Enter the SMTP Server and Port Number of the email client sending emails.  
*Default: SMTP Server Blank; Port: 25*
  - **Security Mode** – Select a security mode for sending Email Alerts. None, SSL/TLS, STARTTLS  
*Default: None*
- **Send Test Email** – Click the button to send a test email to confirm Email Alert settings.

### Configuration Instructions

1. Specify the email alert settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 11.4 - Device Discovery

The Device Discovery menu allows configuration of how or if the access point can search for and connect to network devices via Bonjour and UPnP.

Figure 29. Device Discovery

Device Discovery		
Bonjour		Disable ▾
UPnP		Disable ▾
Araknis EZ Access		Disable ▾

Path – Settings, Security, Device Discovery

### Parameters

- Bonjour** – Enable to allow the access point to search for and connect to network devices running Apple iOS and OS X. Bonjour can also be run on devices running a Microsoft OS.  
*Default: Indoor models: Disabled; outdoor models: Enabled*
- UPnP** – Enable to allow the access point to search for and connect to network devices via UPnP Protocol (Universal Plug and Play).  
*Default: Disable*
- Araknis EZ Access** – Use a URL to access the web interface (see section [4.2 - Configured System Name Access \(p.9\)](#)).  
*Default: Enable*

 **Caution** – Araknis EZ Access and VLANs (in the WAP) may not be enabled at the same time. Use the IP address to access the WAP if VLANs are configured.

### Configuration Instructions

- Specify the device discovery settings.
- Click **Save**, then **Apply Changes** to enable the new settings.

## 12 - Schedule

Use the schedule settings menu to configure automated features including auto reboot, auto ping, and Wi-Fi access schedules for different SSID's.

### 12.1 - Auto Reboot Settings

The WAP can be set to reboot at specified times on a daily or weekly schedule. Rebooting the WAP will help ensure the best network performance by keeping the system memory clear and ending unnecessary connections.

Figure 30. Auto Reboot Settings

Auto Reboot Settings ?	
Status ?	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <small>NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Auto Reboot Settings.</small>
Date	Every: <input type="checkbox"/> Sunday <input type="checkbox"/> Monday <input type="checkbox"/> Tuesday <input type="checkbox"/> Wednesday <input type="checkbox"/> Thursday <input type="checkbox"/> Friday <input type="checkbox"/> Saturday
Time	0 : 0 (24-Hour)

Path – Settings, Schedule, Auto Reboot Settings

#### Parameters

- **Status** – Enable or Disable Auto Reboot.  
*Default: Disable*
- **Date** – Check the boxes for the day(s) WAP should reboot on.
- **Time** – Enter the time for the reboot to take place in 24 hour format. (00:00=midnight; subtract 12 hours from 24 hour time for standard time 17:00-12:00=5:00pm)

#### Configuration Instructions

1. Enable Auto Reboot.
2. Set the desired days and time for reboots to occur.
3. Click **Save**, then **Apply Changes** to enable the new settings.

## 12.2 - Gateway Connection Monitor

Use auto ping to help ensure the WAP maintains network connectivity. Configure the WAP to ping the gateway, and if the ping results fall outside the desired settings, reboot the system.

Figure 31. Gateway Connection Monitor Settings

Gateway Connection Monitor	
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <small>NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the Auto Ping Gateway Settings.</small>
Gateway IP Address	<input type="text"/> <b>Get Current Gateway IP</b>
Delay Between Timeouts	<input type="text" value="30"/> second(s) (10..60)
Timeout Attempts Before Reboot	<input type="text" value="10"/> time-out(s) (3..10)
Ping Delay After Auto Reboot	<input type="text" value="15"/> minute(s) (5..30)
Reboot Attempts	<input type="text" value="5"/> reboot(s) (0..10, 0=Infinite reboot)

Path – Settings, Schedule, Gateway Connection Monitor

### Parameters

- **Status** – Enable or Disable Auto Reboot.  
*Default: Disable*
- **Gateway IP Address** – Displays the gateway IP address to be pinged, usually the router.
- **Get Current Gateway IP** – Click to pull the current IP address of the gateway.
- **Delay Between Timeouts** – How many seconds the WAP waits to try a new ping after a timeout.  
*Default: 30 seconds*
- **Timeout Attempts Before Reboot** – Number of timeouts that must occur before a reboot occurs.  
*Default: 10*
- **Ping Delay After Auto Reboot** – How many minutes before the WAP pings again after a reboot.  
*Default: 15 minutes*
- **Reboot Attempts** – Number of reboots before WAP stops attempting auto reboot.  
*Default: 5*

### Configuration Instructions

1. Enable Gateway Connection Monitor.
2. Set the desired days and time for reboots to occur.
3. Click **Save**, then **Apply Changes** to enable the new settings.

## 12.3 - Wi-Fi Scheduler

The Wi-Fi Scheduler is used to configure when wireless networks are available for use. The scheduler is based on a 24-hour clock (00:00 = 12:00AM, the start of a given day).

Figure 32. Wi-Fi Scheduler

Wi-Fi Scheduler			
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <small>NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.</small>		
Wireless Radio	2.4GHz ▾		
SSID Selection	araknis_initial ▾		
Schedule Templates	Choose a template ▾		
Schedule Table	Day	Availability	Duration
	Sunday	available ▾	00 : 00 ~ 24 : 00
	Monday	available ▾	00 : 00 ~ 24 : 00
	Tuesday	available ▾	00 : 00 ~ 24 : 00
	Wednesday	available ▾	00 : 00 ~ 24 : 00
	Thursday	available ▾	00 : 00 ~ 24 : 00
	Friday	available ▾	00 : 00 ~ 24 : 00
	Saturday	available ▾	00 : 00 ~ 24 : 00

Path – Settings, System, Wi-Fi Scheduler

### Parameters

- **Status** – Enable or Disable the Wi-Fi Scheduler.  
*Default: Disable*
- **Wireless Radio** – Select 2.4GHz or 5GHz for the channel frequency to be scheduled.  
*Default: 2.4GHz.*
- **SSID Selection** – Select the SSID to be scheduled.
- **Schedule Templates** – Create different Wi-Fi schedules using templates as detailed below:
  - **Choose a Template** – Select the template that matches the schedule requirements.
    - **Always Available** – 00:00-24:00. The wireless network is always ON.
    - **Available 8-17 Daily** – 08:00-17:00. The wireless network is ON at 8:00AM and OFF at 5:00PM.
    - **Available 8-17 Daily Except Weekends** – 08:00-17:00. The wireless network is ON at 8:00AM and OFF at 5:00PM Monday-Friday and always OFF on Saturday and Sunday.
    - **Custom Schedule** – Allows custom configuration of the wireless network ON/OFF schedule based upon user requirements.
- **Schedule Table** – Modify template schedules or make custom schedules. See the configuration instructions for setup.
  - **Day** – Day of the week being configured.
  - **Availability** – Select whether the device is **Available** for the set duration, or **Unavailable** for the specified day.
  - **Duration** – Time setting from start to finish for availability in 24 hour format. 00:00=midnight; subtract 12 hours from 24 hour time for standard time 17:00-12:00=5:00pm;)

### 12.3.1 - Configuring Wi-Fi Scheduler

Application example: The 2.4GHz SSID, “Market 2”, needs to be made available during the hours of 8AM to 6PM Monday through Friday, 10AM to 5PM on Saturdays, and unavailable the rest of the week.

Figure 33. Wi-Fi Scheduler Menu

Wi-Fi Scheduler			
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <small>NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.</small>		
Wireless Radio	2.4GHz ▾		
SSID Selection	Market 2 ▾		
Schedule Templates	Available 8-17 daily ▾		
Schedule Table	Day	Availability	Duration
	Sunday	available ▾	08 :00 ~ 17 :00
	Monday	available ▾	08 :00 ~ 17 :00
	Tuesday	available ▾	08 :00 ~ 17 :00
	Wednesday	available ▾	08 :00 ~ 17 :00
	Thursday	available ▾	08 :00 ~ 17 :00
	Friday	available ▾	08 :00 ~ 17 :00
	Saturday	available ▾	08 :00 ~ 17 :00

1. Enable the Wi-Fi Scheduler feature.
2. Select the wireless frequency and SSID for scheduling. *In our example, we will select **2.4GHz** frequency, and the SSID, **Market 2**.*
3. Select an option from the Schedule Templates drop-down to use. *In our example, we will select Available 8-17 Daily, since this template is closest to the schedule needed.*
4. Change the Schedule Table to work on the desired schedule. *In our example, we will make the following changes:*
  - *Sunday: Set to **Unavailable** so that no access is available the entire day.*
  - *Monday-Friday: Set to **Available** and enter a duration of **08:00 - 18:00** (8AM-6PM)*
  - *Saturday: Set to **Available** and enter a duration of **10:00 - 17:00** (10AM-5PM)*
5. Click **Save** at the bottom of the System Information screen. Click **Apply Changes** to enable the new schedule. The figure below shows the configured and applied settings.

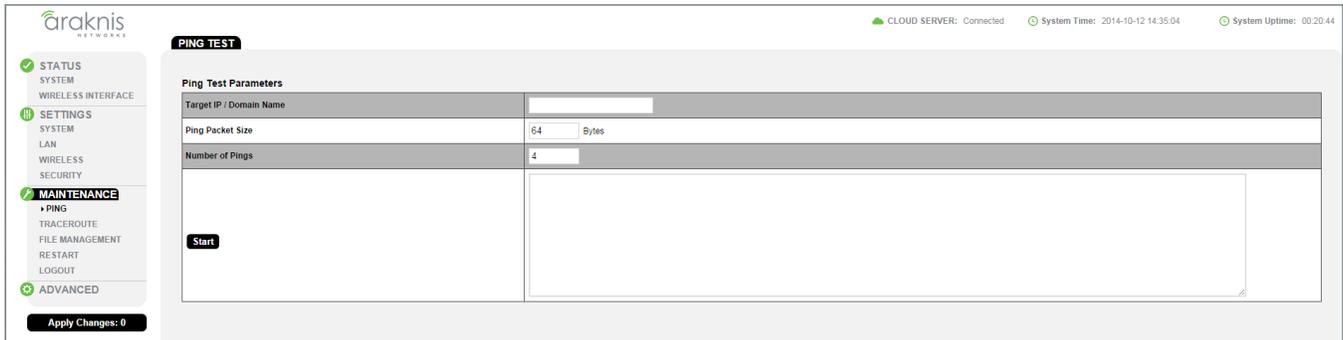
Figure 34. Wi-Fi Scheduler Setup Complete

Wi-Fi Scheduler			
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <small>NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.</small>		
Wireless Radio	2.4GHz ▾		
SSID Selection	Market 2 ▾		
Schedule Templates	Available 8-17 daily ▾		
Schedule Table	Day	Availability	Duration
	Sunday	unavailable ▾	08 :00 ~ 18 :00
	Monday	available ▾	08 :00 ~ 18 :00
	Tuesday	available ▾	08 :00 ~ 18 :00
	Wednesday	available ▾	08 :00 ~ 18 :00
	Thursday	available ▾	08 :00 ~ 18 :00
	Friday	available ▾	08 :00 ~ 18 :00
	Saturday	available ▾	10 :00 ~ 17 :00

## 13 - Ping Test

Determine whether a particular IP address can be reached across an IP network.

Figure 35. Ping Test



Path – Maintenance, Ping

### Parameters

- **Target IP / Domain Name** – Enter the IP address of a device or web page to determine if it can be reached.
- **Ping Packet Size** – Enter the packet size of each ping. Maximum size: 65535.  
*Default: 64 Bytes*
- **Number of Pings** – Enter the number of ping attempts.  
*Default: 4*
- **Start** – Click the Start button to send the Ping. Ping Test results will be displayed in the text frame. Ideal results: Same number of packets transmitted/received, 0% packet loss.

### 13.1 - Running a Ping Test

1. Specify the ping test settings.
2. Click **Start**. The test will run.
3. The screen will refresh with the results once the test is complete.

## 14 - Traceroute Test

Display the route and delays for data packets to/from a destination on an IP network.

Figure 36. Traceroute Test



Path – Maintenance, Traceroute

### Parameters

- **Target IP / Domain Name** – Enter the IP address of a device or web page to show the path of communication to that device or website.
- **Start** – Click the Start button to start Traceroute. Traceroute Test results will be displayed in the text frame.
- **Stop** – Click the Stop button to stop Traceroute.

### 14.1 - Running a Traceroute Test

1. Specify the traceroute test settings.
2. Click **Start**.
3. Click **Stop** to end the test, or wait until it completes.
4. The screen will refresh with the results once the test is complete.

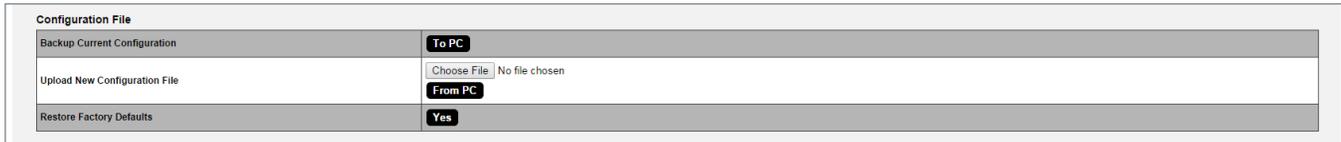
## 15 - File Management

Use the File Management screen to back up or restore settings and apply firmware updates.

### 15.1 - Configuration File

Use the Configuration File menu to back up or restore settings to the access point.

Figure 37. Configuration File



Path - Maintenance, File Management, Configuration File

#### 15.1.1 - Backup Current Configuration

Save the access point's current configuration settings to a ".tar" format compressed archive on your computer.

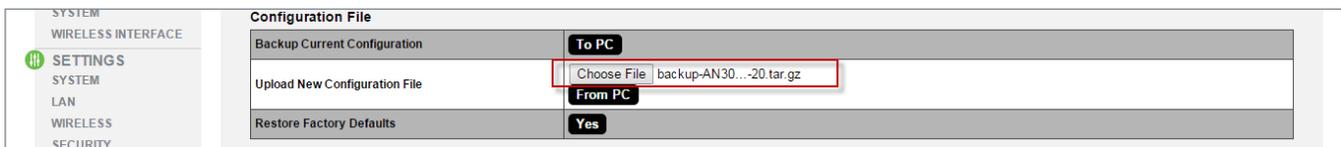
1. Click the To PC button and select a location to save the file.
2. Name the file and save it to your computer.

#### 15.1.2 - Upload New Configuration File

Restore previously saved configuration settings to the access point to restore settings.

1. Click the Choose File button and select a configuration file (".tar" file type) from the Open window.
2. The file name will appear to the right of the Choose File button as shown below Figure 38. Uploading a New Configuration File

Figure 38. Uploading a New Configuration File



3. Click the From PC button to upload the configuration file. Wait while the Rebooting screen opens and loads the selected configuration. When the upload is finished, the Authentication Required (Log In) window will open.
4. Log in and confirm Configuration settings.

### 15.1.3 - Restore Factory Defaults

Use the File Management screen to restore default settings.

**Note** - When restoring factory defaults, the SSID, IP address, subnet mask, and gateway IP address will also be reset. Reconnect to the access point using the instructions beginning in section [4.1 - EZ Access Method \(p.8\)](#).

Figure 39. Restore Factory Defaults



**Path** - Maintenance, File Management, Configuration File, Restore Factory Defaults

**Note** - All current settings will be permanently lost if not backed up. See Backup Current Configuration, above, to backup current settings prior to executing Restore to Factory Defaults.

#### Configuration Instructions

1. Click the **Yes** button to restore the access point to factory default settings. The red ALERT message will appear.
2. Click **Confirm** to restore factory defaults. Wait while the rebooting screen is open and loading the selected configuration. When the configuration upload is finished, the login window will appear.
3. Enter the username and password. (*araknis; araknis*)
4. Confirm the new configuration settings.

### 15.1.4 - Hardware Factory Default

If restoring factory defaults does not restore proper functionality to the device, a hardware reset may be performed to reload the original base configuration file (saved in the access point’s memory).

#### Configuration Instructions

1. Using a paper clip or other small, blunt tool press the reset button located on the top of the access point for 30 seconds.
2. After two to four minutes, the WAP will reboot. Restart the setup process or upload a previously saved configuration.

## 15.1.5 - Firmware

Use the Firmware menu to upload new firmware to the device.

Figure 40. Firmware

Firmware	
Current Firmware Version	v0.9.9.2
Date Activated	2014-10-03 02:41:07 -00:40
Upload New Firmware	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/>

Path – Maintenance, File Management, Firmware

### Parameters

- **Current Firmware Version** – Indicates the current running firmware version.
- **Date Activated** – Date the current firmware was uploaded and activated.

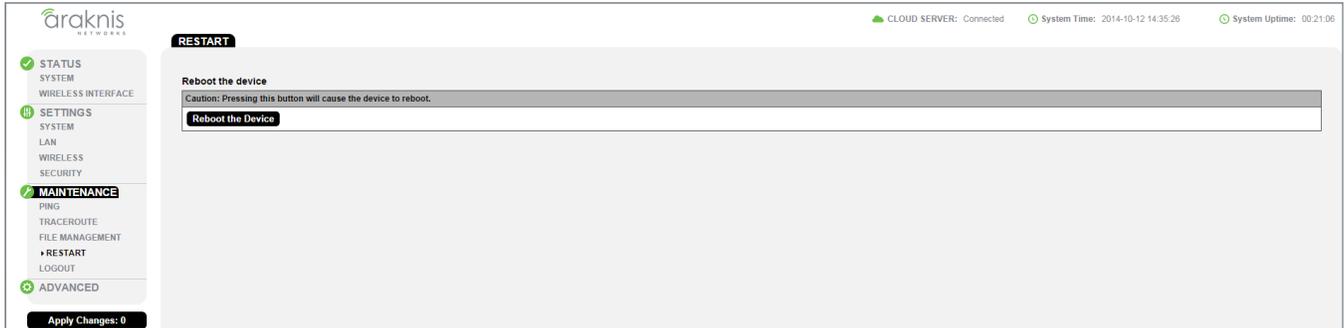
### 15.1.5.1 - Firmware Update Instructions

1. Click the **Browse** button to navigate to where the firmware file is saved.
2. Select the file and then press Enter/Return on the computer keyboard or click **Open** on the Upload menu. (The firmware file name should appear next to the Upload New Firmware File **Browse** button.)
3. Click **Upload**. The Upload Firmware Information screen will open.
4. Click **Upgrade**. Wait while the new firmware loads. When the configuration upload is finished, the login screen will appear.
5. Enter the username and password.
6. Confirm the firmware version.

## 16 - Restart

Reboot the access point.

Figure 41. Restart



Path - Maintenance, Restart

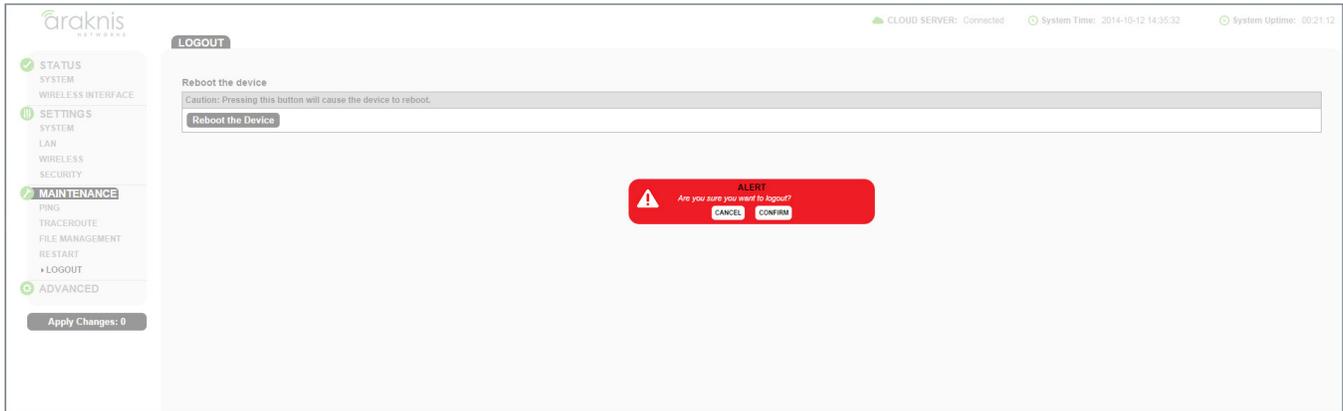
### 16.1 - Rebooting the Device

1. Click the **Reboot the Device** button. The message, “This will reboot the device and may take a few seconds...” will appear.
2. Click **OK** to reboot (or **Cancel** to return to the Restart Screen).
3. Wait while the access point reboots. When the device has rebooted, the login screen will appear.

## 17 - Logout

Logout can be used to change the user currently logged into setup. After working in the setup screens, a logged in user can simply close the browser tab or click Logout. Closing the browser tab will close the setup screen completely, Logout will end the session for the logged in user and open the Authentication Required (Log In) window.

Figure 42. Logout Alert



Path – Maintenance, Logout

### 17.1 - Logging Out

1. From any screen, click **Logout** in the system menu. The Logout ALERT will appear on screen.
2. Click **Cancel** to return to the setup screen; click **Confirm** to log the current user out.

## 18 - Advanced Menu

 **Note** - Advanced menu settings should not require any changes for most applications.

### 18.1 - Advanced Wireless Settings

#### 18.1.1 - Radio Settings

The Advanced Wireless Settings menu allows configuration of radio settings for unit of measure, data rate, power and RTS/CTS Threshold.

Figure 43. Radio Settings

Radio Settings			
Transmit Power Unit	<input type="radio"/> dBm <input type="radio"/> mW		
Data Rate	2.4GHz <input type="text" value="Auto"/>	5GHz <input type="text" value="Auto"/>	
Transmit Power	Full 100%-29 dBm		Full 100%-29 dBm
RTS/CTS Threshold (Range:1-2346)	<input type="text" value="2346"/>		

Path - Advanced, Wireless Settings, Radio Settings

#### Parameters

 **Note** - The settings below apply to all indoor models. Outdoor models lack the settings marked with an asterisk (\*).

- **Transmit Power Unit\*** - Select the preferred unit of measure. OPTIONS: dBm, mW.  
*Default: dBm.*
- **Data Rate** - Select a setting from the drop-down to set the available transmit data rate permitted for connected clients. A lower data rate reduces throughput, but increases the transmission range. OPTIONS: See drop-down list.  
*Default: Auto.*
- **Transmit Power\*** - Select a setting from the drop-down to set the radio power. Higher power will improve performance but can cause interference with other access points in close range on the same channel. Also, a higher coverage range corresponds with lower throughput (i.e. to achieve the highest transmit power, the connection must run at the lowest data rate). Set this value as low as possible (for adequate coverage) to get the maximum wireless speed/data throughput. OPTIONS: See drop-down list. Values are in dBm or mW based on Transmit Power Unit setting.  
*Default: 100/300/500: Full 100% -29dBm; 700: Full 100% -28dBm*
- **RTS/CTS Threshold (Range: 1-2346)** - Enter a value for the threshold package size for RTS/CTS (request to send/clear to send). A lower number increases the frequency that the packets are sent and consumes more bandwidth. RANGE: 1-2346.  
*Default: 2346*

#### Configuration Instructions

1. Change the settings as desired.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.1.2 - Client Limit

The Advanced Wireless Settings screen allows configuration of client limit by band, (2.4GHz/5GHz).

Figure 44. Client Limit Settings

Client Limit		2.4GHz	5GHz
Enable		<input type="checkbox"/> Yes	<input type="checkbox"/> Yes
Max Client No.		127	127

Path – Advanced, Wireless Settings, Client Limit

### Parameters

- **Enable** – Select to enable Client Limit, by channel.  
*Default: Not Selected.*
- **Max Client No.** – Set the maximum number of clients that can be connected to a channel at a given time.  
RANGE: 1-127.  
*Default: 127.*

 **Pro Tip** – It is recommended to design the wireless network so that each access point handles about 30 clients at a given time.

### Configuration Instructions

1. Specify the client limit settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.2 - Wireless MAC Filter Settings

The Wireless MAC Filter determines if wireless clients (such as computers, tablets, smart phones) can access the wireless network as defined by client MAC address. Authorized clients can be configured and viewed in the MAC Filter List.

Figure 45. MAC Filter Settings

WIRELESS MAC FILTER SETTINGS		
<b>MAC Filter Settings</b>		
Enable MAC Filter	<input type="checkbox"/> Yes	
Filter Mode	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	
<b>MAC Filter List</b>		
No.	MAC address	Delete
<b>Add</b>		

Path – Advanced, MAC Filter, MAC Filter Settings

### Parameters

- **Enable MAC Filter** – Select Yes to enable MAC Filtering.  
*Default: Not Selected.*
- **Filter Mode** – Select which settings are being modified.
  - **Allow** – Wireless clients in this list are allowed access to the wireless network.
  - **Deny** – Wireless clients in this list are not allowed access to the wireless network.
- **No.** – The client number for a device being filtered by MAC address.
- **MAC address** – The MAC address of the client.
- **Add** – Click to add a new client.
- **Delete** – Click to delete an existing client. (Only appears once an entry exists.)

## 18.2.1 - MAC Filter Schedule

Figure 46. MAC Filter Schedule

**MAC Filter Scheduler**

Status  Enable  Disable  
NOTE: Please ensure that the Time Zone Settings are synced with your local time when enabling the MAC Filter Scheduler.

Schedule Templates: Custom schedule

Day	Availability	Start / End Time
Sunday	Available <input type="text" value="from"/>	00:00 ~ 24:00
Monday	Available <input type="text" value="from"/>	00:00 ~ 24:00
Tuesday	Available <input type="text" value="from"/>	00:00 ~ 24:00
Wednesday	Available <input type="text" value="from"/>	00:00 ~ 24:00
Thursday	Available <input type="text" value="from"/>	00:00 ~ 24:00
Friday	Available <input type="text" value="from"/>	00:00 ~ 24:00
Saturday	Available <input type="text" value="from"/>	00:00 ~ 24:00

### Parameters

- **Status** - Enable or disable the schedule for the selected list (Allow or Deny).
- **Schedule Templates** - Create different Wi-Fi schedules using templates as detailed below:
  - **Choose a Template** - Select the template that matches the schedule requirements.
    - **Always Available** - 00:00-24:00. The wireless network is always ON.
    - **Available 8-17 Daily** - 08:00-17:00. The wireless network is ON at 8:00AM and OFF at 5:00PM.
    - **Available 8-17 Daily Except Weekends** - 08:00-17:00. The wireless network is ON at 8:00AM and OFF at 5:00PM Monday-Friday and always OFF on Saturday and Sunday.
    - **Custom Schedule** - Allows custom configuration of the wireless network ON/OFF schedule based upon user requirements.
- **Schedule Table** - Modify template schedules or make custom schedules. See the configuration instructions for setup.
  - **Day** - Day of the week being configured.
  - **Availability** - Select whether the device is **Available** for the set duration, or **Unavailable** for the specified day.
  - **Duration** - Time setting from start to finish for availability in 24 hour format. 00:00=midnight; subtract 12 hours from 24 hour time for standard time 17:00-12:00=5:00pm;)

## 18.2.2 - Managing MAC Filter Lists

1. Check **Yes** to enable the MAC filter.
2. Select which list to modify, either Allow or Deny.
3. Add or remove the desired client(s).
4. Modify the schedule for the list if desired.
5. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.3 - WPS Settings

WPS (Wi-Fi Protected Setup) allows setup of WPS-equipped Wi-Fi devices. Instead of sharing the SSID and security credentials with a client, WPS connected clients using a push button or PIN entry method.

**Note** - This feature is not recommended for use because WPS can be exploited to gain access to a network if left enabled.

**Note** - WPS and MAC Filter lists may not be used together. One must be disabled for the other to work.

Figure 47. WPS Settings Menu

WPS Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Self-PIN Code	32940077
SSID	7000D_Rack6
Authentication Mode	WPA2/PSK AES
WPS via Push Button	<input type="button" value="Start"/>
WPS via PIN	<input type="text"/> <input type="button" value="Start"/>

Path - Advanced, WPS

### Parameters

- **Status** - Enable or disable WPS.  
*Default: Disabled*
- **Current Configuration** - Displays whether the WPS feature is configured or not.
  - **Release Configuration** - The primary SSID in the WAP will be reset to default if Release Configuration is clicked and then settings are applied.
- **Self-PIN Code**- The WPS pin generated by the WAP.
- **SSID** - Displays SSID used for WPS. Will always be the first SSID in the list on the Wireless Settings page; WPS cannot be used unless this SSID is enabled (checked).
- **Authentication Mode** - Displays authentication mode for the SSID.
- **WPS via Push Button** - Click to connect a device using WPS Push Button. See section [18.3.1 - Connecting a Device Using WPS via Push Button \(p.57\)](#) for instructions.
- **WPS via PIN** - Used to connect a device using WPS via PIN. See section [18.3.2 - Connecting a Device Using WPS via PIN \(p.58\)](#) for instructions.

### 18.3.1 - Connecting a Device Using WPS via Push Button

#### Specific Setup Requirements

- Client device equipped with WPS Push Button
- Administrator access to the WAP interface

#### Configuration Instructions

1. Power on the WPS enabled client device to be connected.
2. Log into the WAP web interface as an administrator and navigate to Advanced, WPS. Enable WPS if it is disabled (remember to complete the Apply Settings process).

Figure 48. Using WPS Push Button

WPS Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Current Configuration	Configured <b>Release Configuration</b>
Self-PIN Code	43389988
SSID	HomeLan1
Authentication Mode	WPA2/PSK AES
Encryption Key	Atlll4said
WPS via Push Button	<b>Start</b>
WPS via PIN	<input type="text"/> <b>Start</b>
<b>Save</b>	

3. Press the WPS button on the client device, then click the WPS via Push Button Start button in the WAP interface.
4. The device will connect. Test connectivity to the device to ensure Wi-Fi operation. WPS-connected devices will appear in the Wireless Interface Status page Connected Clients list.

## 18.3.2 - Connecting a Device Using WPS via PIN

### Specific Setup Requirements

- Client device equipped with WPS via PIN
- Administrator access to the WAP interface

### Configuration Instructions

1. Power on the WPS enabled client device to be connected.
2. Find the WPS setup menu and record the device's WPS PIN.
3. Log into the WAP web interface as an administrator and navigate to Advanced, WPS. Enable WPS if it is disabled (remember to complete the Apply Settings process).

Figure 49. Using WPS PIN

WPS Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Current Configuration	Configured <b>Release Configuration</b>
Self-PIN Code	43389988
SSID	HomeLan1
Authentication Mode	WPA2/PSK AES
Encryption Key	Ahll4said
WPS via Push Button	<b>Start</b>
WPS via PIN	<input type="text"/> <b>Start</b>

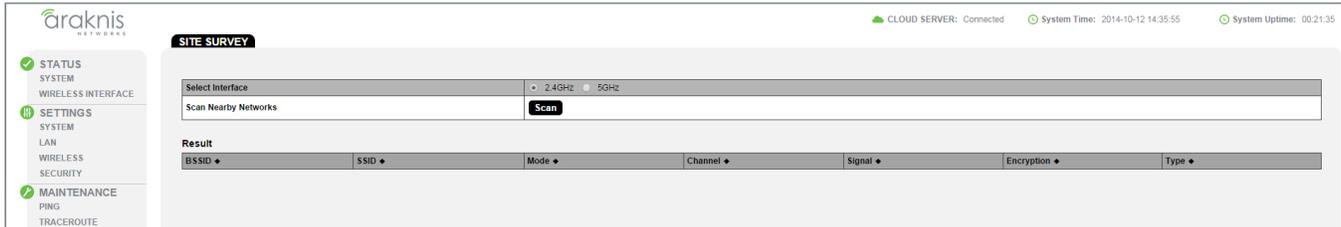
**Save**

4. In the WAP interface, enter the WPS PIN from the client device in the WPS via PIN field, then click Start.
5. The device will connect. Test connectivity to the device to ensure Wi-Fi operation. WPS-connected devices will appear in the Wireless Interface Status page Connected Clients list.

## 18.4 - Site Survey

The access point provides a convenient on-board Wi-Fi detection tool commonly known as a Wi-Fi sniffer that can be used to detect the presence of other 2.4GHz and 5GHz wireless networks. Parameters such as their modes, channels, security settings, signal strengths, encryptions, and types can be identified. Having this information can be useful during setup to avoid conflicts with other networks in the wireless neighborhood.

Figure 50. Site Survey



Path – Advanced, Site Survey

### Parameters

- **Select Interface** – Select whether to scan for 2.4GHz or 5GHz networks.
- **Scan Nearby Networks** – Click the Scan button to begin a scan.
- **Result** – Displays information about found networks after the scan is complete.
  - **BSSID** – Basic Service Set Identification. Indicates the MAC address of a detected 2.4GHz or 5GHz neighboring access point.
  - **SSID** – Service Set Identifier. Indicates the network name of a wireless network that a specific device is connected to.
  - **Mode** – Indicates how a device is being used such as WAP or repeater.
  - **Channel** – Indicates the channel a specific device is transmitting on.
  - **Signal** – RSSI or Received Signal Strength Indicator. Indicates the signal strength of a detected network as received by the device.
  - **Encryption** – Indicates the security mode encryption of a detected device.
  - **Type** – Indicates the wireless mode of the detected device.

### 18.4.1 - Running a Site Survey

1. Specify which interface to scan.
2. Click **Start** to scan. Results will be displayed once the test is complete.

## 18.5 - Spectrum Analyzer

Analyze Wi-Fi channel interference at different frequencies and power levels. This information can help determine what channel settings to use for the best Wi-Fi performance.

Figure 51. Spectrum Analyzer Settings

Select Interface	<input type="radio"/> 2.4GHz <input checked="" type="radio"/> 5GHz
Scan Bandwidth	20-40MHz
Scan Channel	Channel 6 (2437 MHz)
RSSI Filter	<input type="text" value="-85"/> (-95~-65)
Scan Action	<input type="button" value="Play/Pause"/> <input type="button" value="Stop"/>

Elapsed time: 00:00:09

Path – Advanced, Site Survey, Result

### Parameters

- **Select Interface** - 2.4 or 5 GHz antenna.
- **Scan Bandwidth** - Based on the setting of the selected wireless antenna.
- **Scan Channel** - Based on the setting of the wireless antenna
- **RSSI Filter** - Select an RSSI filter value to use in testing. Using a value closer to zero will eliminate results from weaker signals. The default value is recommended for most environments.
- **Scan Action** -
  - **Start** - Click to begin a scan.
  - **Play/Pause** - Click to pause an in-progress scan. Click again to resume the scan.
  - **Stop** - Click to stop a scan.
- **Elapsed Time** - Amount of time since the Start button was pressed.

### 18.5.1 - Configuring Scan Settings

The Spectrum Analyzer uses scan settings based on the configuration of the 2.4 or 5 GHz radio interface. To change the Scan Bandwidth and Channel settings, change them on the Wireless Settings menu.

If the channel is set to auto, the scan will be performed using the channel currently in use.

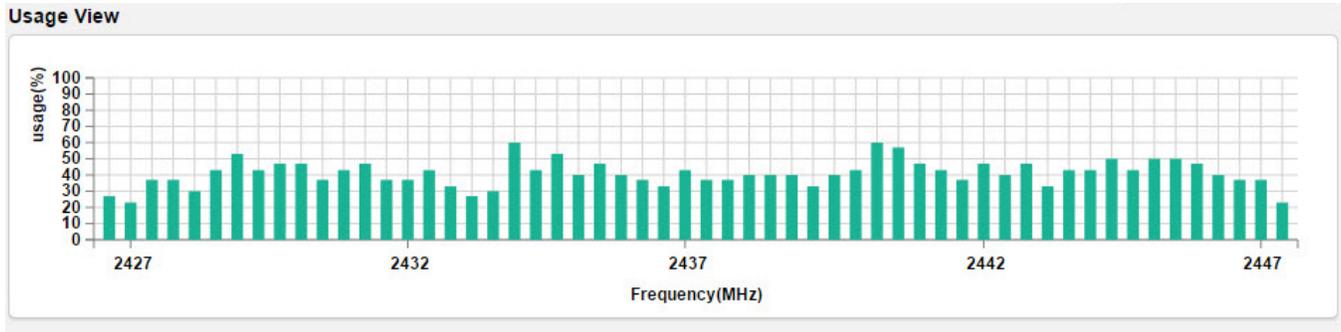
### 18.5.2 - Running a Scan

Click Start to begin a scan. The Elapsed Time counter will begin updating every 3-5 seconds. After about 20 seconds, the Usage, Waveform, and Real-time View graphs will begin to display results from the scan. The graphs will update multiple times throughout the scan, and each time the previous results are overwritten. Use the Play/Pause button to pause the test and review results in detail.

### 18.5.3 - Understanding Spectrum Analyzer Results

#### Usage View

Figure 52. Spectrum Analyzer Usage View

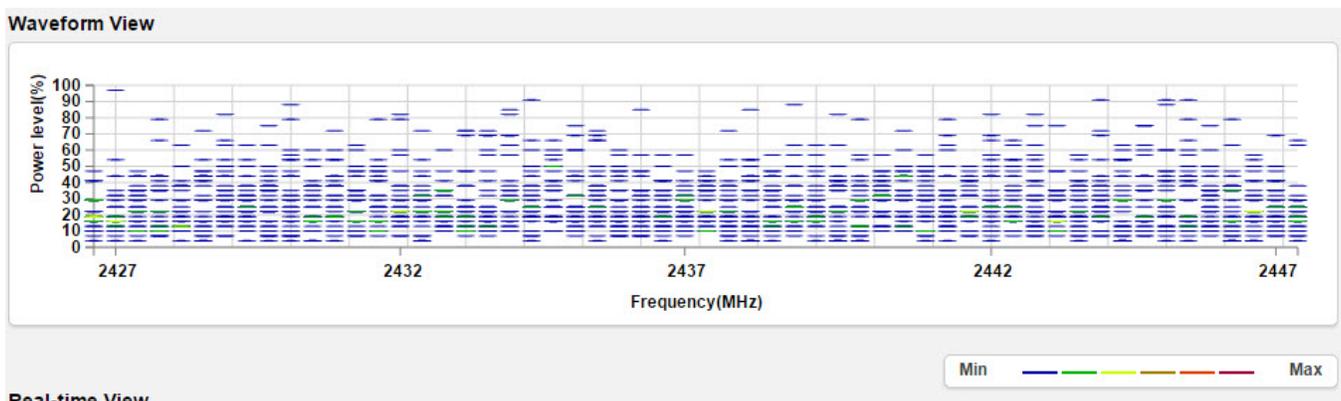


The Usage View displays approximate bandwidth use around the scanned channel. Higher values indicate higher use. Ideally, the channel selected for use will display little to no usage.

If your results are similar to the graph shown, try reducing the RSSI filter (closer to zero) to see if spikes of activity become more obvious at certain frequencies. As long as client devices connect at stronger RSSI values than the selected scan setting, wireless traffic should not be adversely affected by the activity indicated on the graph.

#### Waveform View

Figure 53. Spectrum Analyzer Waveform View

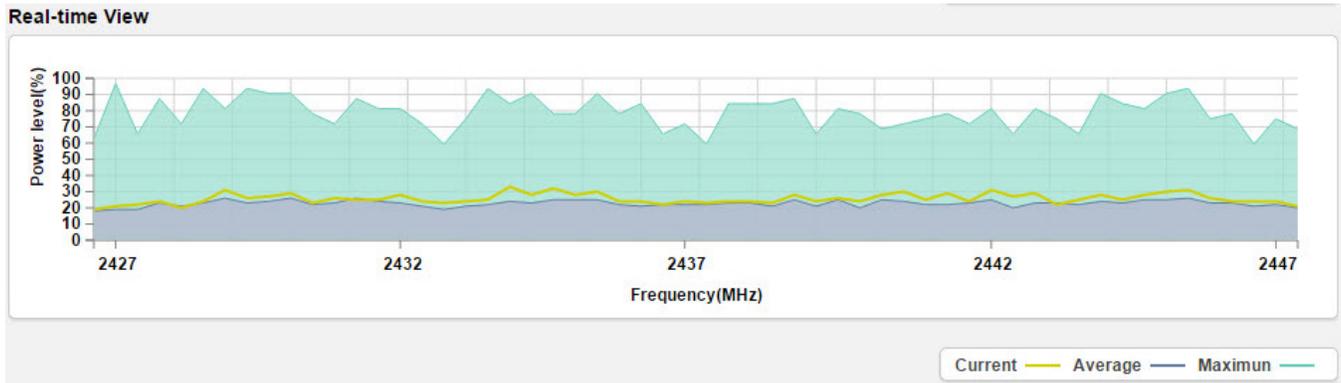


The Waveform view shows the aggregate energy recorded at each scanned frequency. Marks on the graph represent the power level at which signals are being recorded, and the color of the mark roughly estimates how much data is flowing at that level.

For the best performance, avoid using frequencies where colors indicate high traffic (see scale in bottom right of image).

## Real-time View

Figure 54. Spectrum Analyzer Real-time View



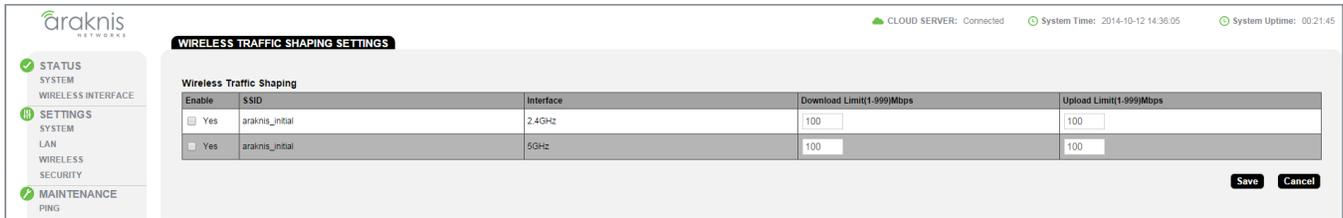
The Real-time view indicates the current, average, and maximum power level of scanned signals since the scan was started:

- **Current** – Average power level shown in the Waveform view. If the current reading is closer to the maximum than the average, the frequency should typically be avoided.
- **Average** – Average power of Waveform view data since since the scan began. This view averages across time as well as data points for any one frequency. Avoid frequencies with spikes above the rest of the graph.
- **Maximum**– Maximum power of Waveform view data since since the scan began. This is the maximum recorded at any given time and frequency of the current scan. Compare to the average and current reading to determine if a channel should be avoided.

## 18.6 - Wireless Traffic Shaping Settings

Traffic shaping is used to regulate packet flow to control wireless network saturation and reduce latency.

Figure 55. Wireless Traffic Shaping Settings



Path – Advanced, Traffic Shaping

### Parameters

- **Enable** – Select to enable Traffic Shaping on the 2.4GHz and/or 5GHz band.
- **SSID** – Indicates the network to which Traffic Shaping will be applied.
- **Interface** – Indicates 2.4GHz or 5GHz band.
- **Download Limit** – Enter a value to regulate download speed.  
*Default: 100Mbps.*
- **Upload Limit** – Enter a value to regulate upload speed.  
*Default: 100Mbps.*

### Configuration Instructions

1. Specify the wireless traffic shaping settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.7 - SNMP Settings

Simple Network Management Protocol (SNMP) is an IP network protocol that can be used to monitor network devices, audit network usage, detect network faults or inappropriate access, and, in some cases, configure remote devices.

### 18.7.1 - SNMPv2 Settings

Figure 56. SNMPv2 Settings

SNMPv2 Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Contact	<input type="text"/>
Location	<input type="text"/>
Port	161 <input type="text"/>
Community Name (Read Only)	public <input type="text"/>
Community Name (Read Write)	private <input type="text"/>
Trap Destination	
Port	162 <input type="text"/>
IP Address	<input type="text"/>
Community Name	public <input type="text"/>

Path – Advanced, SNMP, SNMPv2

#### Parameters

- **Status** – Select Enable to enable SNMPv2. Select Disable to disable SNMPv2.  
*Default: Enable*
- **Contact** – Enter the name of the person managing the SNMPv2 server.  
*Default: Blank*
- **Location** – Enter the physical location of the SNMPv2 server.  
*Default: Blank*
- **Port** – Indicates the port number for SNMPv2 'listening'.  
*Default: 161 (This is a dedicated TCP/UDP port and typically should not be changed.)*
- **Community Name (Read Only)** – Indicates the password for SNMPv2 read only access.  
*Default: Public. 'Public' is a typical default of SNMP v2 devices for Read Only.*
- **Community Name (Read Write)** – Indicates the password for SNMPv2 read/write access.  
*Default: Private.*
- **Trap Destination** – An SNMPv2 Trap is a notification of a network event such as a fault or security event. The Trap Destination is typically the IP address of the SNMP server where trap messages will be sent.
  - **Port** – Indicates the SNMPv2 port number for 'receiving traps'.  
*Default: 162 (This is a dedicated TCP/UDP port and typically should not be changed.)*
  - **IP Address** – IP address of the SNMPv2 server that will receive SNMP traps.
  - **Community Name** – Indicates the password for the SNMPv2 trap community.

#### Configuration Instructions

1. Specify the SNMPv2 settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.7.2 - SNMPv3 Settings

Figure 57. SNMPv3 Settings

SNMPv3 Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Username	<input type="text" value="admin"/> (1-31 Characters)
Authorized Protocol	MD5 ▾
Authorized Key	<input type="text" value="12345678"/> (8-32 Characters)
Privacy Protocol	DES ▾
Privacy Key	<input type="text" value="12345678"/> (8-32 Characters)
Engine ID	<input type="text"/>

Path – Advanced, SNMP, SNMPv3

### Parameters

- **Status** – Select Enable to enable SNMPv3. Select Disable to disable SNMPv3.  
*Default: Enable*
- **Username** – Enter a username for SNMPv3 implementation. RANGE: 1-31 Characters.  
*Default: admin.*
- **Authorized Protocol** – Select the desired protocol from the drop-down.  
OPTIONS: MD5, SHA, None.  
*Default: MD5*
- **Authorized Key** – Enter an authentication key. This key acts as an electronic signature to authenticate an SNMPv3 message. RANGE: 8-32 Characters.  
*Default: 12345678*
- **Privacy Protocol** – Select the desired protocol from the drop-down. OPTIONS: DES, None.  
*Default: DES*
- **Privacy Key** – Enter a Privacy Key. This acts as an encryption for the data within a SNMPv3 message. RANGE: 1-8 Characters.  
*Default: 12345678*
- **Engine ID** – Enter an Engine ID. The Engine ID identifies where a SNMPv3 message is **coming from**.  
*Default: Blank*

### Configuration Instructions

1. Specify the SNMPv3 settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.8 - Spanning Tree Settings

Spanning Tree Protocol (STP) is an IP network protocol that prevents undesirable loops caused by multiple active paths between network devices when multiple switches or bridges are used on a network.

Figure 58. Spanning Tree Settings

The screenshot shows the 'Spanning Tree Protocol (STP) Settings' page. At the top right, it displays 'CLOUD SERVER: Connected', 'System Time: 2014-10-12 14:36:26', and 'System Uptime: 00:22:06'. The left sidebar contains a navigation menu with categories like STATUS, SETTINGS, MAINTENANCE, and ADVANCED. The main content area features a table for STP settings:

Spanning Tree Protocol (STP) Settings	
Status	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Hello Time	<input type="text" value="2"/> seconds (1-10)
Max Age	<input type="text" value="20"/> seconds (6-40)
Forward Delay	<input type="text" value="4"/> seconds (4-30)
Priority	<input type="text" value="32768"/> (0-65535)

At the bottom right of the settings table, there are 'Save' and 'Cancel' buttons.

Path – Advanced, SNMP, Spanning Tree

### Parameters

- **Status** – Enable or Disable STP.  
*Default: Disable*
- **Hello Time** – Enter a value for Hello Time. This setting will determine how often in seconds the access point will send the Hello Message to network switches and bridges to assess network topology. RANGE: 1-10 seconds.  
*Default: 2 seconds*
- **Max Age** – Enter a duration for Max Age. This setting will determine how long the access point will wait for a Hello Message from another switch or bridge. If no message is received within the set duration, the device will be considered off-line and a new STP route will be configured. RANGE: 6-40 seconds.  
*Default: 20 seconds.*
- **Forward Delay** – Enter a value for Forward Delay. This setting will determine the length of time the access point will take to 'listen' to the network and either retain current topology or generate a new topology based upon network switch and bridge status. RANGE: 4-30 seconds.  
*Default: 4 seconds.*
- **Priority** – Enter a value for Priority from 0-65535. This setting will help determine which bridge is the root bridge, or essentially, the switch that controls the main road that network traffic is going to be routed around to avoid loops. In this game, the lowest score wins. The score is a total of MAC address, the Priority number and a bunch of tie-breaker values that determine the root bridge. Setting a lower Priority will help generate a lower score for a given switch.  
*Default: 32768.*

### Configuration Instructions

1. Specify the Spanning Tree settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 18.9 - VLAN Settings

A Virtual Local Area Network (VLAN) is a group of IP Network devices whose IP addresses have been set to run on a particular IP Network. These devices will typically only 'see' the other devices on their network and most likely the Internet. A VLAN ID or 'tag' can be assigned to data packets that pass through the access point to maintain the integrity of the VLAN by identifying which data belongs to which VLAN.

Figure 59. VLAN Settings

VLAN Isolation	SSID	Interface	VLAN ID
<input type="checkbox"/> Yes	araknis_inital	2.4GHz	
<input type="checkbox"/> Yes	araknis_inital	5GHz	

Path - Advanced, VLANS

### Parameters

- **VLAN Isolation** - Select Yes to assign a VLAN ID.  
*Default: Not selected.*
- **SSID** - Indicates the name of the network being tagged with the VLAN ID. Any wireless SSIDs that need to be tagged should be added in the Wireless Settings page under Wireless Networks. If a SSID does not appear in the VLAN Settings List, check the Wireless Settings page under Wireless Networks to see if it is enabled. If it is not, Enable, Save, then Apply Changes.
- **Interface** - Indicates the 2.4GHz or 5GHz Interface for a given SSID.
- **VLAN ID** - Enter a value for the VLAN ID. RANGE: 1-4094.  
*Default: Blank*

### Configuration Instructions

1. Specify the VLAN settings.
2. Click **Save**, then **Apply Changes** to enable the new settings.

## 19 - Appendix

### 19.1 - Configuring Guest Networks with Fast Roaming

The Guest Network feature is used to provide Internet access to clients while restricting them access from the main network using a separate DHCP server on a different subnet. This works well for WLANs with only one WAP. But when the job calls for a guest network on multiple WAPs with Fast Roaming for seamless handoff, the Guest Network feature is not the right solution.

In these installs, configure network SSIDs for guests on a separate VLAN. This allows the DHCP server in the router to handle guest client addresses on all the WAPs, which gives Fast Roaming to all guest network clients.

#### Setup Requirements

- Multiple WAPs with fast roaming required for Guest Network SSID
- Router with VLAN support (Araknis AN-300-RT-4L2W used for example)
- Managed Switch (Araknis AN-310-SW-R-8-POE used for example)

#### Step 1 – Configure the WAPs (repeat for all)

1. Log in as an Administrator.
1. In the Wireless Settings menu, configure Fast Roaming and SSIDs for primary WLAN clients like normal, then add SSID(s) for guest network use. (Use the same settings on each WAP!)

Apply Changes: 0

#### Global Settings

Band Steering	ON <input type="checkbox"/>	NOTE: Band Steering is not supported in repeater mode.
Fast Roaming	ON <input type="checkbox"/>	NOTE: Fast Roaming is not supported on the radio in use as the repeater.

#### Wireless Networks

Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation	Delete
<input checked="" type="checkbox"/>	Employee WiFi	Both	WPA2-PSK	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable	
<input checked="" type="checkbox"/>	Guest WiFi	Both	WPA2-PSK	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Enable	

2. In the WAP Advanced VLANs menu, configure the guest network SSID(s) on the desired VLAN. This example uses VLAN 2 for the guest network.

STATUS SYSTEM WIRELESS INTERFACE

SETTINGS SYSTEM LAN WIRELESS SECURITY SCHEDULE

MAINTENANCE PING

VLAN SETTINGS

#### VLAN Settings

Enable	SSID	Interface	VLAN ID
<input type="checkbox"/> Yes	Employee WiFi	2.4GHz	<input type="text"/>
<input type="checkbox"/> Yes	Employee WiFi	5GHz	<input type="text"/>
<input checked="" type="checkbox"/> Yes	Guest WiFi	5GHz	2
<input checked="" type="checkbox"/> Yes	Guest WiFi	2.4GHz	2

Save
Cancel

3. Be sure to apply changes after all settings have been changed. Set up in the WAPs is now complete. Continue to the next section and complete managed switch setup.

## Step 2 – Configure the Managed Switch

1. Log in and go to the VLAN Settings menu.
2. Click Add to create a new VLAN for the guest network SSID(s).

The screenshot shows the 'VLAN SETTINGS' page in the Araknis Networks management interface. At the top, there are status indicators: 'CLOUD SERVER: Connected', 'System Time: 2016-04-12 10:12:03', and 'System Uptime: 42d 22:55:13'. On the left, a navigation menu includes 'STATUS', 'SYSTEM', 'PORTS', 'SETTINGS', 'SYSTEM', 'PORTS', 'POE', and 'VLANs'. The main content area features a table with the following data:

VID	Name	Access Port	Trunk Port	Custom Port	Delete
1	default	1-8,SFP1-SFP2,LAG1-LAG8			
2	Guest WiFi		1,5-7		

Below the table, there is an 'Add' button, and at the bottom right, there are 'Apply' and 'Cancel' buttons.

*In this example, we have 3 WAPs to configure, connected to ports 5, 6, and 7 on the switch. Port 1 connects the managed switch to the router.*

3. Configure the settings for the VLAN:
  - A. **VLAN ID** – Enter the same ID number for the guest VLAN as used in the WAPs.
  - B. **Name** – Enter a name for the guest network VLAN.
  - C. **Access Port/Trunk Port** – Click one of the fields to open the selection box. Since the WAPs tag packets for both VLAN 1 and 2, you must configure each port on the switch with a connected WAP as a trunk port for VLAN 2. The port connecting the switch to the router must also be configured as a trunk port so the packets are not dropped.
4. Click Apply to save the changes. Managed switch setup is now complete. Continue to the next section and complete router setup.

### Step 3 – Configure the Router

1. Log in and go to the Advanced VLANs menu.
2. Click Add to create a new VLAN entry.

Cloud Service: Connected System Time: 2016-03-15 17:44:17 System Uptime: 39d 06:03:29

**VLANs**

802.1Q LAN (VID range is 2-4092)

VLAN ID	Description	Inter VLAN Routing	Device Management	Route Binding	LAN1	LAN2	LAN3	LAN4	Delete
1	Default	Disabled	Enabled	None	UnTagged	UnTagged	UnTagged	UnTagged	
2	Guest WiFi	Disabled	Disabled	None	Tagged	Tagged	Tagged	Tagged	

Add Apply Cancel

3. Configure the settings for the VLAN:
  - A. **VLAN ID** – Enter the same ID number for the guest VLAN as used in the other devices (VLAN 2 in this example).
  - B. **Description** – Enter the same information used in the VLAN Name field of the managed switch.
  - C. **Inter VLAN Routing** – Set to Disabled for a guest network so guests don’t get access to the rest of the network.
  - D. **Device Management** – Select Disabled so that guest clients can’t access the router management interface.
  - E. **Route Binding** – Set whether routes use the WAN1 or WAN2 port. Leave set to none for link failover.
  - F. **LAN1/2/3/4** – Set all LAN ports to “Tagged” using the drop-downs.
4. Click Apply to save the settings. Configuration is complete.

### Step 3 – Test the Guest Network

To test guest network functionality, connect a device to the SSID and confirm that the IP address issued is on the new VLAN subnet.

Next, move around the job with the connected device. You should see the client device listed in each WAP’s Connected Clients table (Path: Status, Wireless Interface) as you move around the job.



## 20 - 2-Year Limited Warranty

Araknis Networks® products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to SnapAV or a designated service center with prior notification and an assigned return authorization number (RA).

## 21 - Contacting Technical Support

P: (866) 838-5052

E: [Techsupport@araknisnetworks.com](mailto:Techsupport@araknisnetworks.com)



© 2017 Araknis Networks®

170801-1130