



WIRELESS ACCESS POINT  
PRODUCT MANUAL

Models:  
AN-100-AP-I-N  
AN-300-AP-I-N





## 1 - About this Manual

This manual was created to provide a reference for installers and end users of Araknis Networks™ products. It provides all known information regarding the installation, setup, use, and maintenance of the product. The symbols below are used to identify important information:



**Pro Tip** - Pro tips are included in sections of the manual to add information that provides extra value, utility, or ease-of-use for the installer or end user of the product. Pro tips may also link to extra information that will provide a better understanding of application, technology or use of the product or feature in question. 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. Notes may be located before or in the midst of the section to which they apply, depending on the type of information. These items usually contain essential information, like the size or dimension of a separate part required, or a critical step in the process, that, if missed, would cause the installer or end user extra work to overcome.



**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. Cautions are always provided before the information they relate to. Not following a caution will almost always 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. Warnings are always provided before the information they relate to. Not following a warning may result in permanent damage to equipment and serious injury or death of the installer or end user.



## Table of Contents

1 -	About this Manual	2
2 -	Welcome to Araknis Networks™	6
	2.1 - Features	6
	2.2 - Package Contents	6
3 -	Hardware Overview	7
	3.1 - Top	7
	3.2 - Bottom	7
	3.3 - Side	7
4 -	Mounting Location - General Guidelines	8
5 -	Wiring Requirements	9
	5.1 - Network Cable Requirements	9
	5.2 - PoE Requirements	9
	5.3 - Power Requirements for Non-PoE Application	9
	5.4 - Wiring Instructions	9
	Wiring Diagram	10
6 -	Mounting the Access Point	11
	6.1 - Table Top/Shelf	11
	6.2 - Junction Box Mounting	11
	Instructions	11
	6.3 - Wall or Ceiling Drywall Mounting Instructions	12
	6.4 - Ceiling Tile Mounting Instructions	12
7 -	Power-On and Operation	13
	7.1 - Status LED Operation	13
8 -	Introduction to Network Setup	14
9 -	Accessing the Web Interface	14
	9.1 - EZ Access Method (Default)	15
	9.2 - Configured System Name Access	16
	9.3 - DHCP/Static IP Address Method	17
	Finding the IP Address of the Access Point	17
	Default IP Address Access	18
10 -	Web Interface Overview	21
	10.1 - Applying Changes in the Web Interface	22
11 -	System Status	23
	11.1 - System Information	23
	11.2 - Wireless Information	24
	11.3 - LAN Information	25
	11.4 - System Log	25
12 -	Wireless interface Status	26
	12.1 - Radio Status	26
	12.2 - Utilization of SSID	27
	Wireless Network	27



12.3 - Connected Clients	28
13 - System Settings	29
13.1 - System Information	29
13.2 - Date and Time Settings	30
13.3 - Time Zone	31
14 - LAN Settings	32
14.1 - IP Settings	32
14.2 - Interface Settings	33
15 - Wireless Settings	34
15.1 - Radio Settings	34
15.2 - Utilization of SSID	35
15.3 - Global Wireless Settings	35
Fast Roaming Mode	36
Fast Roaming Setup Instructions	37
Fast Roaming Troubleshooting	37
15.4 - Wireless Networks	38
15.5 - Wireless Security Setup (SSID Encryption)	39
WEP Mode	39
WPA-PSK Mixed and WPA2-PSK Modes	40
WPA and WPA2 Modes	41
15.6 - Guest Network	42
15.7 - Configuring the WAP as a Repeater	44
Repeater Mode Setup Instructions	45
16 - Security Settings	46
16.1 - User Accounts	46
16.2 - Access Control	47
16.3 - Email Alert	48
16.4 - Device Discovery	50
17 - Schedule	51
17.1 - Auto Reboot Settings	51
17.2 - Gateway Connection Monitor	52
17.3 - Wi-Fi Scheduler	53
Configuring Wi-Fi Scheduler	54
18 - Ping Test	55
19 - Traceroute Test	56
20 - File Management	57
20.1 - Configuration File	57
Backup Current Configuration	57
Upload New Configuration File	57
Restore Factory Defaults	58
Hardware Factory Default	58
Firmware	59
21 - Restart	60



22 - Logout	61
23 - Advanced Menu	62
23.1 - Advanced Wireless Settings	62
Radio Settings	62
Client Limit	63
23.2 - Wireless MAC Filter Settings	64
MAC Filter Settings	64
MAC Filter List	65
23.3 - WPS Settings	66
Connecting a Device Using WPS via Push Button	67
Connecting a Device Using WPS via PIN	68
23.4 - Site Survey	69
23.5 - Spectrum Analyzer	70
Configuring Scan Settings	70
Running a Scan	70
Understanding Spectrum Analyzer Results	71
23.6 - Wireless Traffic Shaping Settings	73
23.7 - SNMP Settings	74
SNMPv2 Settings	75
SNMPv3 Settings	76
23.8 - Spanning Tree Settings	77
23.9 - VLAN Settings	78
24 - Appendix	79
24.1 - Configuring Guest Networks with Fast Roaming	79
25 - Troubleshooting	82
25.1 - Hardware Reset Procedure	82
26 - Software Defaults	83
26.1 - Basic Menus	83
26.2 - Advanced Menus	84
27 - Table of Figures	85
28 - Specifications	87
29 - CE Warning	90
30 - AN-100-AP-I-N FCC Statement	90
31 - AN-300-AP-I-N FCC Statement	93
32 - 2-Year Limited Warranty	97
33 - Contacting Technical Support	97



## 2 - Welcome to Araknis Networks™

Thank you for choosing an Araknis™ Wi-Fi access point. With sleek, unobtrusive housings, extensive features, unique easy setup, and convenient PoE power, these products are ideal for use in both residential and commercial applications.

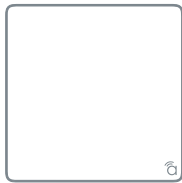
### 2.1 - Features

Feature	AN-100-AP-I-N	AN-300-AP-I-N
2.4GHz Radio	Yes	Yes
5GHz Radio	No	Yes
Concurrent Dual-band	No	Yes
Gigabit Ethernet	No	Yes
PoE Standard	802.3af	802.3af/at
WiFi Standard	802.11 b/g/n	802.11 a/b/g/n
OvrC Enabled	Yes	Yes
Antennas	2x2:2	2x2:2

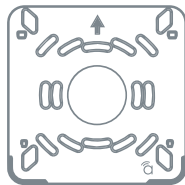
### 2.2 - Package Contents

\*Not Pictured: Wall Mount Template

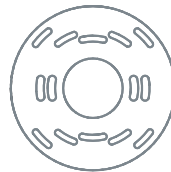
Figure 1. Package Contents



WAP



Mounting Bracket



Tile Ceiling Backing Plate



Quick Start Guide



LAN Cable



Tile Ceiling Mounting Hardware



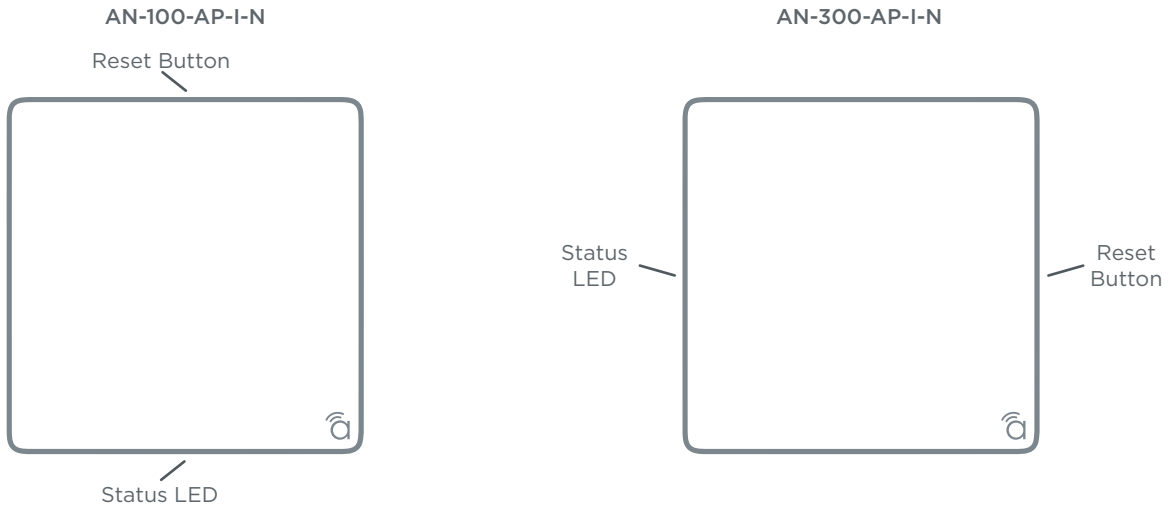
Drywall Mounting Hardware



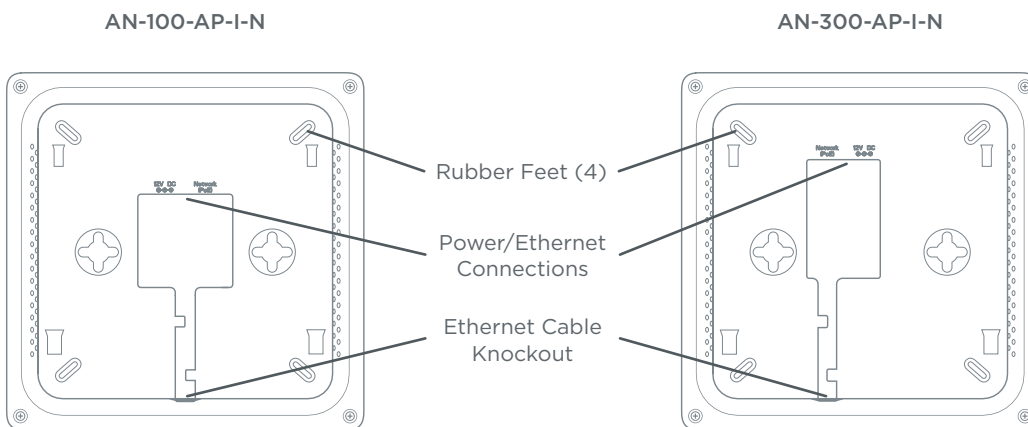
### 3 - Hardware Overview

Use these images to familiarize yourself with the physical layout of your access point.

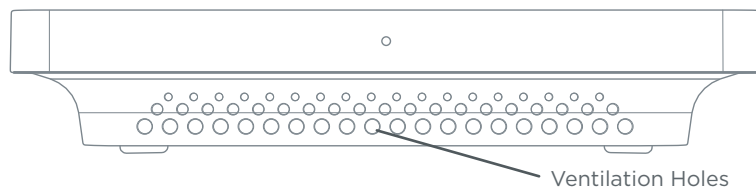
#### 3.1 - Top



#### 3.2 - Bottom



#### 3.3 - Side



## 4 - Mounting Location - General Guidelines

- Locate the access point in a central location. Higher mounting can provide better coverage.
- Avoid mounting near kitchens or rooms with large appliances that may give off EMI noise, which can reduce connection speed, and in extreme cases, block WiFi connectivity altogether.
- As a rule of thumb, each access point can cover about a 300 ft (100m) radius (actual performance varies based on multiple variables).
- Plan multiple access points at least 200 ft apart. Signal should overlap but only slightly.
- Use network site survey tools (not included) to determine mounting locations if possible. This will ensure you get the best coverage and performance from your installation.

**Pro Tip** - Professional site survey tools are available from vendors in the market such as Metageek and Fluke Networks.

Figure 2. Residential Access Point Location

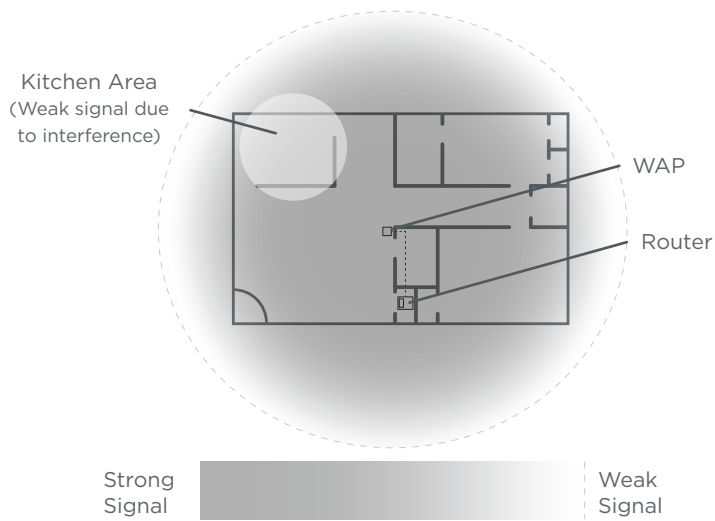
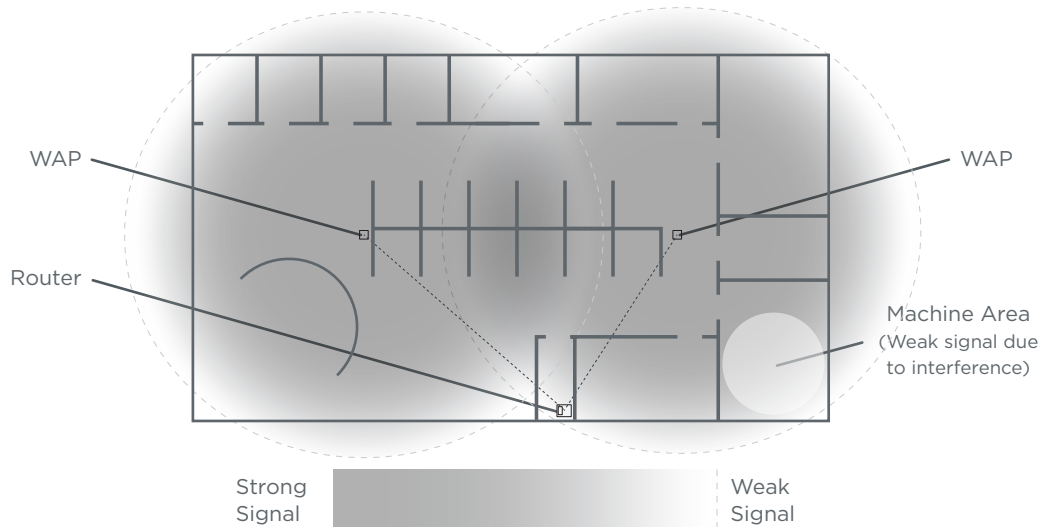


Figure 3. Small Commercial Access Point Location







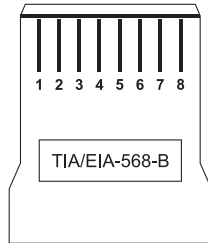
## 5 - Wiring Requirements

The access point must be connected to the local network and powered using PoE (Power over Ethernet) or 12V DC power. Install the required cabling and equipment according to the guidelines in this section.

### 5.1 - Network Cable Requirements

568B termination is recommended (Figure 4. EIA/TIA 568B Termination Pattern) Connect a Cat5e/6 straight-through cable between the access point and a local area network port on a switch or router.

Figure 4. EIA/TIA 568B Termination Pattern



Pin 1	White/Orange	Pin 5	White/Blue
Pin 2	Orange	Pin 6	Green
Pin 3	White/Green	Pin 7	White/Brown
Pin 4	Blue	Pin 8	Brown

(Gold pins facing up)



**Note** - Maximum cable length is 328 feet (100m). A repeater device is required for longer runs.

### 5.2 - PoE Requirements



**Caution** - Use an 802.3af/at compliant PoE injector, switch, or router to power the access point. Non-compliant devices can harm the access point and lead to unpredictable results.

### 5.3 - Power Requirements for Non-PoE Application

If PoE is not being used, connect a suitable power supply (not included) from a nearby outlet to the DC input of the access point.

- **AC Outlet** - 100-240V AC, 50/60Hz (AN-100: 0.3A; AN-300: 0.6A)
- **DC Input** - 12V DC 1A (AN-100); 2A (AN-300).

### 5.4 - Wiring Instructions

Plan a mounting location and install the wiring before installing the access point.



**Warning** - Do not connect any equipment to the wiring until every connection has been terminated and testing is complete.

1. For PoE installations, install a network cable from the PoE device to the access point and terminate both ends to the same pattern. The DC power supply is not needed.
2. For non-PoE installations, locate an outlet for the power supply.

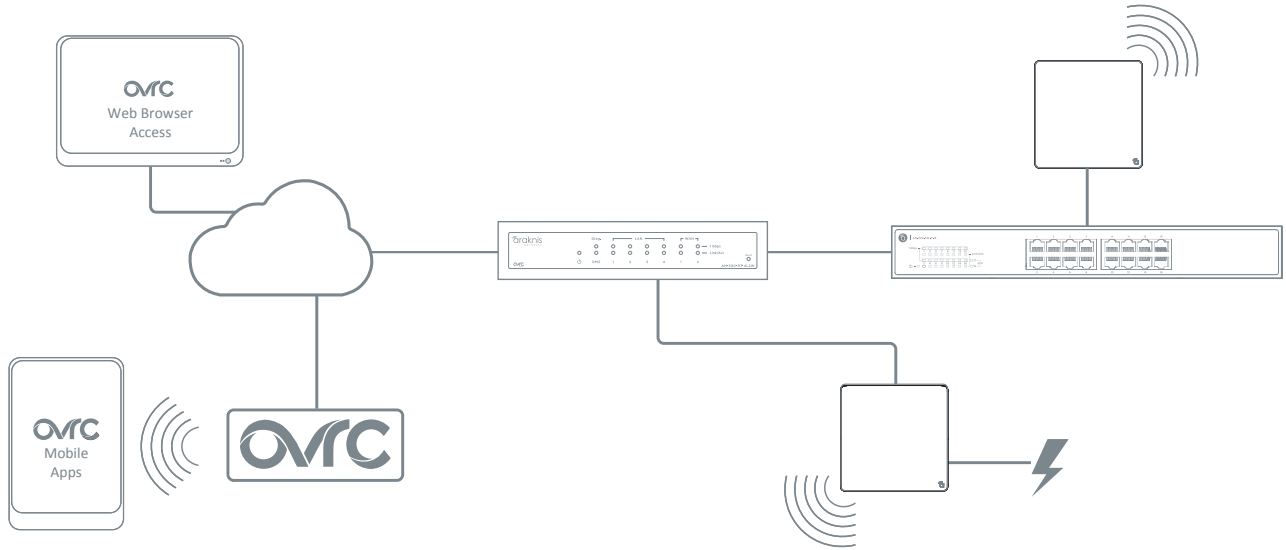


**Pro Tip** - If needed, extend a 2-conductor power wire from the power supply to the access point.



### 5.4.1 - Wiring Diagram

Figure 5. Network Wiring Diagram



## 6 - Mounting the Access Point

### 6.1 - Table Top/Shelf

The access point comes with rubber feet installed for placement on flat surfaces. The mounting bracket is not required for this application.

### 6.2 - Junction Box Mounting

The mounting bracket is compatible with most common junction box and plaster ring dimensions, including common ceiling box sizes:

- Single/Double Gang
- 4" Square Box
- 3" Octagonal Box
- 4" Octagonal Box

#### 6.2.1 - Instructions

1. Place the mounting bracket over the junction box and attach it loosely with 2 screws. (two 6-32 x 1" screws are included) Use the hole pattern on the bracket that best matches the box pattern. See Figure 6A, below.
2. Level or align the bracket with nearby objects for uniformity and tighten the screws enough to secure it. Avoid over-tightening and warping the bracket.
3. Connect the wiring to the access point and push any extra wiring back into the opening. See Figure 6B, below.
4. Snap the access point onto the bracket. See Figure 6C, below.

Figure 6. Junction Box Mounting

Figure 6A

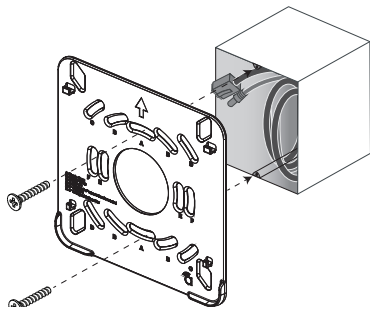


Figure 6B

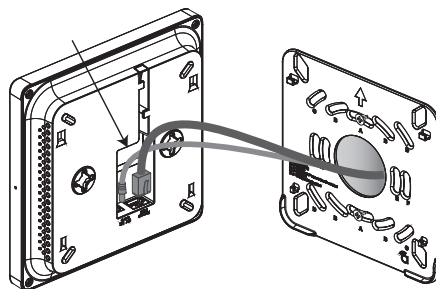
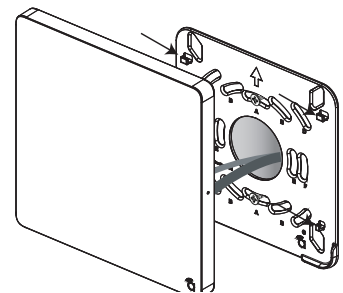


Figure 6C





### 6.3 - Wall or Ceiling Drywall Mounting Instructions

1. Place the bracket over the desired mounting location with the arrow on the bracket pointing up for wall mounting. See Figure 7A, below.
2. Mark the “C” or “D” slots on the mounting surface, then remove the bracket and thread one of the included drywall anchors into the center of each mark using a Phillips screwdriver.
3. Level or align the bracket with nearby objects and fasten it to the anchors using the two included anchor screws. Tighten the screws enough to secure the bracket. Avoid over-tightening and warping the bracket.
4. Connect the wiring to the access point and push any extra wiring back into the opening. See Figure 7B, below.
5. Snap the access point onto the bracket. See Figure 7C, below.

Figure 7. Drywall Mounting

Figure 7A

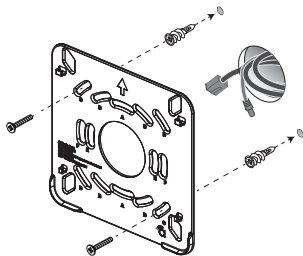


Figure 7B

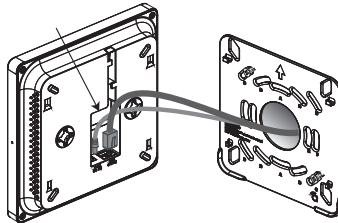
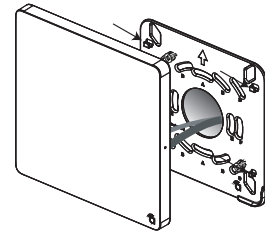


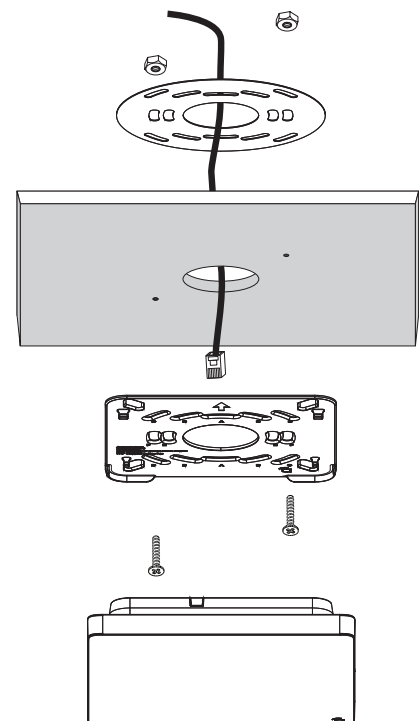
Figure 7C



### 6.4 - Ceiling Tile Mounting Instructions

1. Place the bracket over the desired mounting location and align it with nearby objects for uniformity.
2. Mark the “C” or “D” slots on the ceiling tile (and the center hole if needed for wiring).
3. Cut the opening with a keyhole saw. Use a drill to make clean holes for the mounting screws.
4. Place the ceiling backing plate and nuts on top of the tile as shown and fasten the mounting bracket to the tile using the included screws.
5. Connect the wiring to the access point and push any extra wiring back into the opening.
6. Snap the access point onto the bracket.

Figure 8. Ceiling Tile Mounting





## 7 - Power-On and Operation

Once the access point is powered, the status LED can be used to determine proper operation.

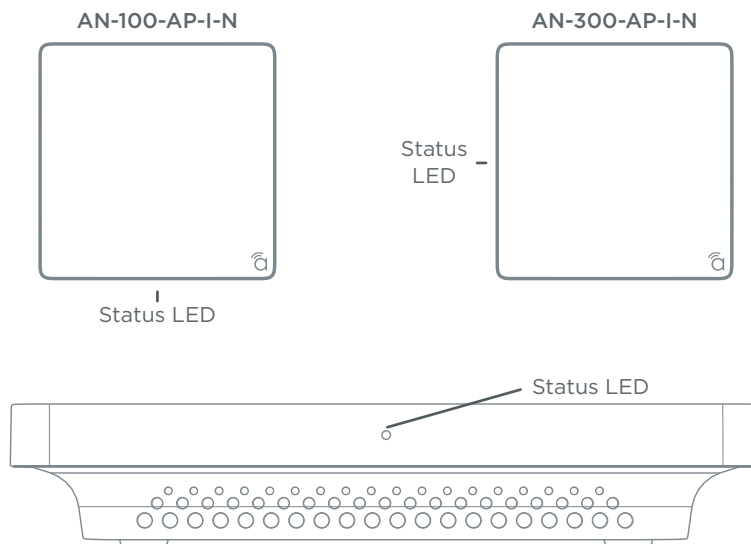


**Pro Tip** – Check the wireless network connection status in your PC to see if the default SSID, “araknis\_initial” is being broadcast. If so, you may continue to the next section to begin configuring device access and software setup.

### 7.1 - Status LED Operation

After installing the access point, connect the network and power cables and check the status LED. Once the LED remains illuminated (no more flashes), then the device is ready to be accessed for setup.

Figure 9. Status LED Location



- Blue LED:
  - Blinking: Device is not working correctly. Refer to the Troubleshooting section.
  - Solid: Device is operating correctly.



## 8 - Introduction to Network Setup

The access point setup menu is used to make network configuration changes. This section explains how to access and use the menu.

**!** **Warning** - All Araknis access points will transmit the same SSID, “araknis\_initial” by default. If multiple access points are being installed in the same network, 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 during initial setup.

## 9 - Accessing the Web Interface

There are several ways to access the web interface of the access point:

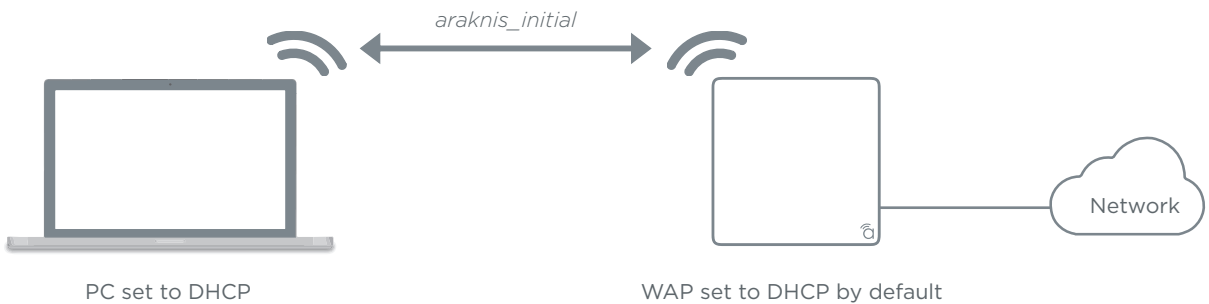
- **EZ Access Method** - Default method used for initial setup. Connect your computer to the access point using Wi-Fi.
- **Configured System Name Access** - Enter the device name instead of the IP address to access the web interface.
- **DHCP/Static IP Address Method** - Can be used any time. Connect your computer to the network wired or wirelessly and enter the IP address issued to the access point by the network, or the default IP address, (192.168.20.253).
- **OvrC Method** - OvrC gives you remote device management, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required. To add this device to your OvrC account:
  1. Connect the WAP to the Internet
  2. Log Into OvrC ([www.ovrc.com](http://www.ovrc.com))
  3. Add the Device (MAC address and Service Tag numbers needed for authentication)

## 9.1 - EZ Access Method (Default)

When the WAP is powered on for the first time, it transmits the default, unsecured SSID, “araknis\_initial”. Connect and access the web interface without any cable connections or network card setting changes.

**Note** - Make sure the WAP is connected to a network with a functioning DHCP server. 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.

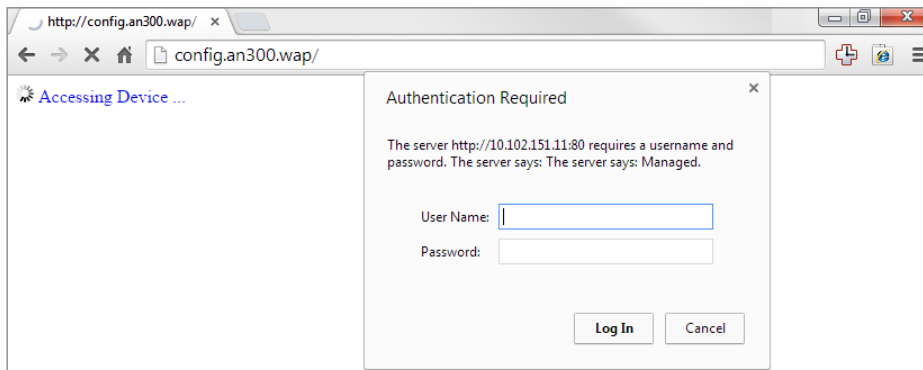
Figure 10. Default SSID



On your wireless network-enabled computer:

1. Disconnect any network cables from your computer.
2. Make sure the wireless network card is set to obtain an IP address automatically (DHCP mode).
3. Connect your computer to the wireless network named “araknis\_initial”.
4. Open a web browser and enter the configuration address for your device:
  - AN-100-AP-I-N enter: ***http://config.an100.wap/***
  - AN-300-AP-I-N enter: ***http://config.an300.wap/***
5. Enter the default login credentials:
  - Username: ***araknis***
  - Password: ***araknis***

Figure 11. EZ Setup Login Screen



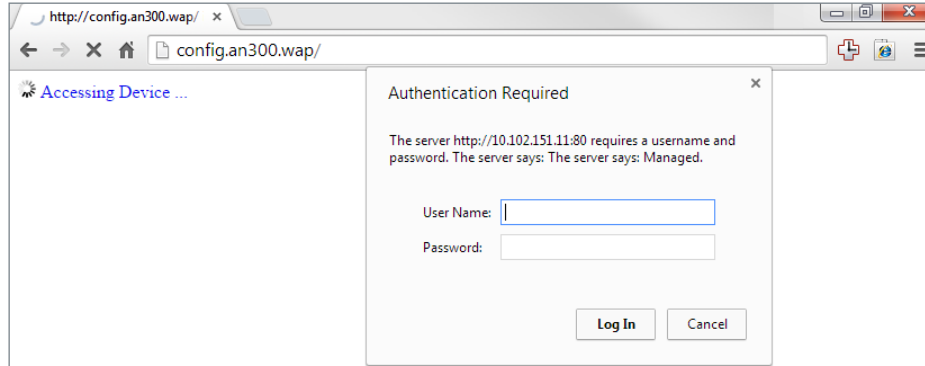


## 9.2 - Configured System Name Access

**Note** - “Araknis EZ Access” on page 50 must be enabled for this access method to work. The setting is enabled by default.

1. See section “13 - System Settings” on page 29 to set the system name.
2. Apply the settings. After configuration, the WAP web interface may be accessed using the system name.
3. 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/*
4. Enter the login credentials. (Default: *araknis/araknis*)

Figure 12. System Name Access





### 9.3 - DHCP/Static IP Address Method

Connect your computer to the network wired or wirelessly and enter the IP address issued to the access point by the network, or the default IP address, 192.168.20.253.

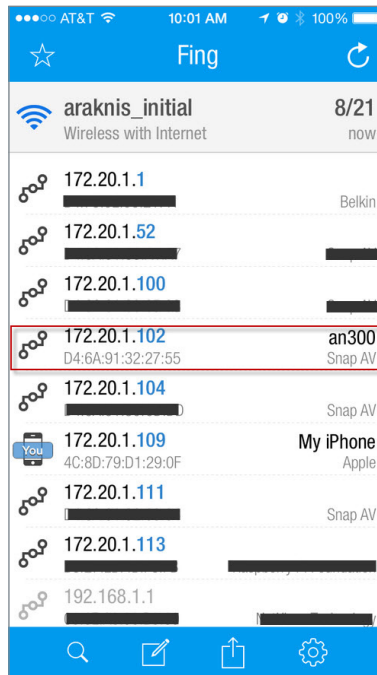
**Note** - If the WAP is not issued a DHCP IP address on the network, access the device using the default IP address.

#### 9.3.1 - Finding the IP Address of the Access Point

The WAP is configured to DHCP by default so that the DHCP server can assign an IP address when the WAP is connected to the network (the DHCP server is usually the router). This address can be used for accessing the web interface.

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 13.** Fing IP Scanner Example



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

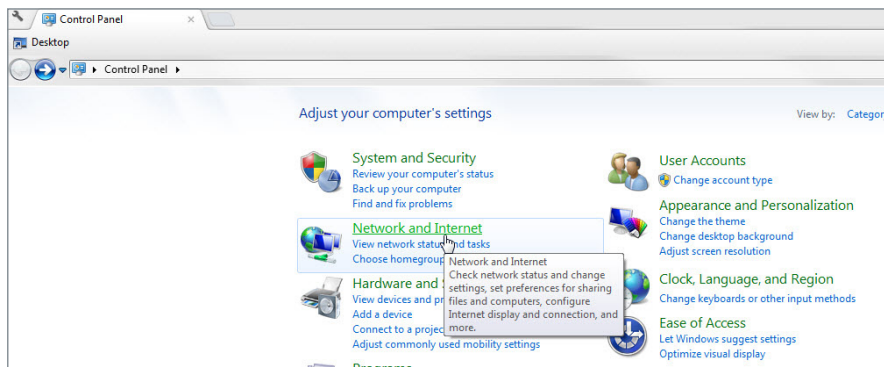
### 9.3.2 - Default IP Address Access

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.

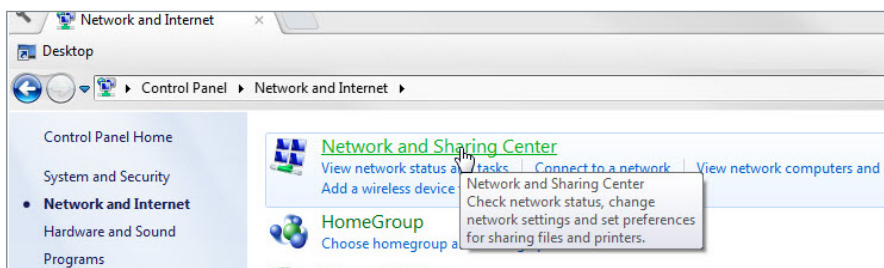
1. Connect your PC to the WAP using a network patch cable.



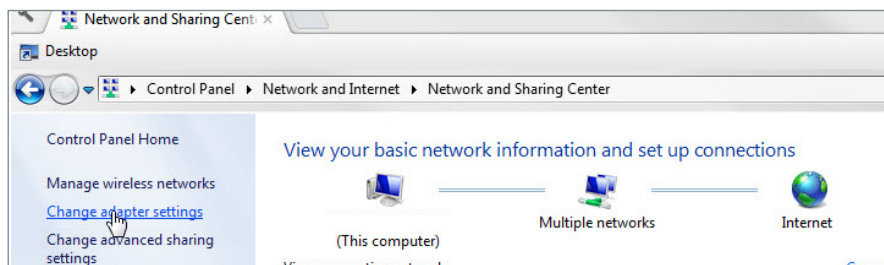
2. On your PC, open the Control Panel and left-click **Network and Internet**.



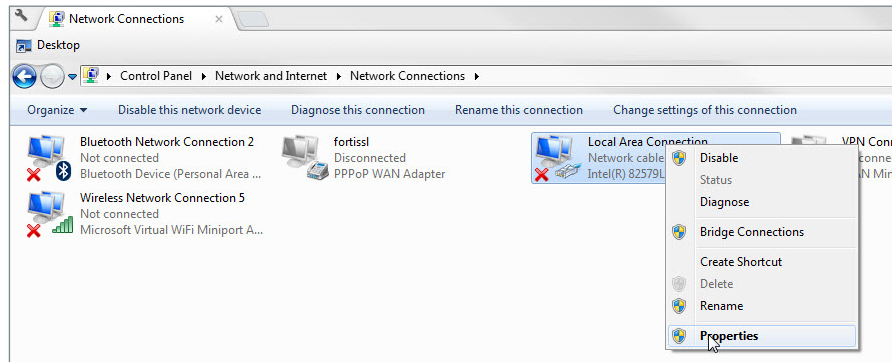
3. Left-click **Network and Sharing Center**.



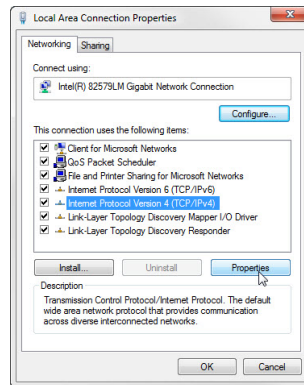
4. In the left bar, left-click **Change adapter settings**.



5. Right-click the icon for the wired network connection and left-click **Properties**.

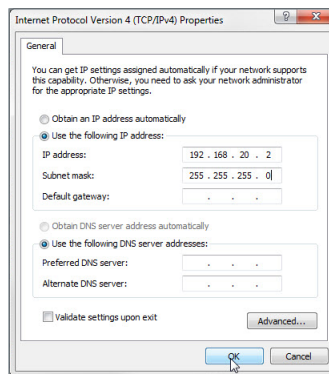


6. Left-click to highlight **Internet Protocol Version 4 (TCP/IPv4)**, then left-click **Properties**.



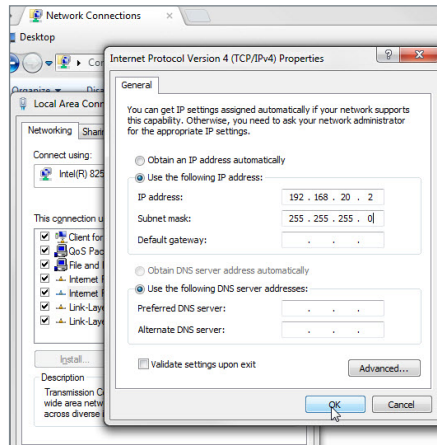
7. In the General tab, left-click **Use the following IP address:** and enter the IP address and subnet mask.

- IP Address: **192.168.20.2**
- Subnet Mask: **255.255.255.0**

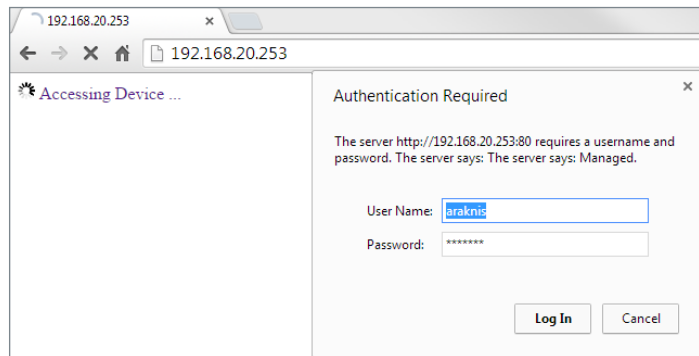




- Left-click **OK** to close **Internet Protocol Version 4 (TCP/IPv4) Properties**, then left-click **OK** to close **Wireless Network Connection Properties**.



- Open a web browser and navigate to <http://192.168.20.253/>. Log in using the default credentials:
  - Username: *araknis*
  - Password: *araknis*





## 10 - Web Interface Overview

Figure 14. Web Interface Layout

The screenshot shows the Araknis Networks web interface. On the left is a navigation menu (A) with sections: STATUS (checked), SETTINGS, MAINTENANCE, and ADVANCED. The main content area (B) displays 'SYSTEM STATUS' with three tables: System Information, Wireless Information, and LAN Information. The top bar (C) shows connection status, system time, and uptime.

System Information	
System Name	an300
Service Tag	ST1506165101841A
Firmware Version	1.1.04
Management VLAN ID	Untagged

	2.4GHz	5GHz
MAC Address	D4:6A:91:32:3B:57	D4:6A:91:32:3B:58
Number of Networks	1	2
Number of Connected Clients	0	0
Operation Mode	Access Point	Access Point
TX	0 Bytes	0 Bytes
RX	0 Bytes	0 Bytes

LAN Information			
Speed	1Gbps	IP Address	192.168.1.20
Duplex	Full	Subnet Mask	255.255.255.0
MAC Address	D4:6A:91:32:3B:56	Default Gateway	192.168.1.1
TX	111393608 Bytes	Primary DNS	192.168.1.1
RX	746239744 Bytes	Secondary DNS	

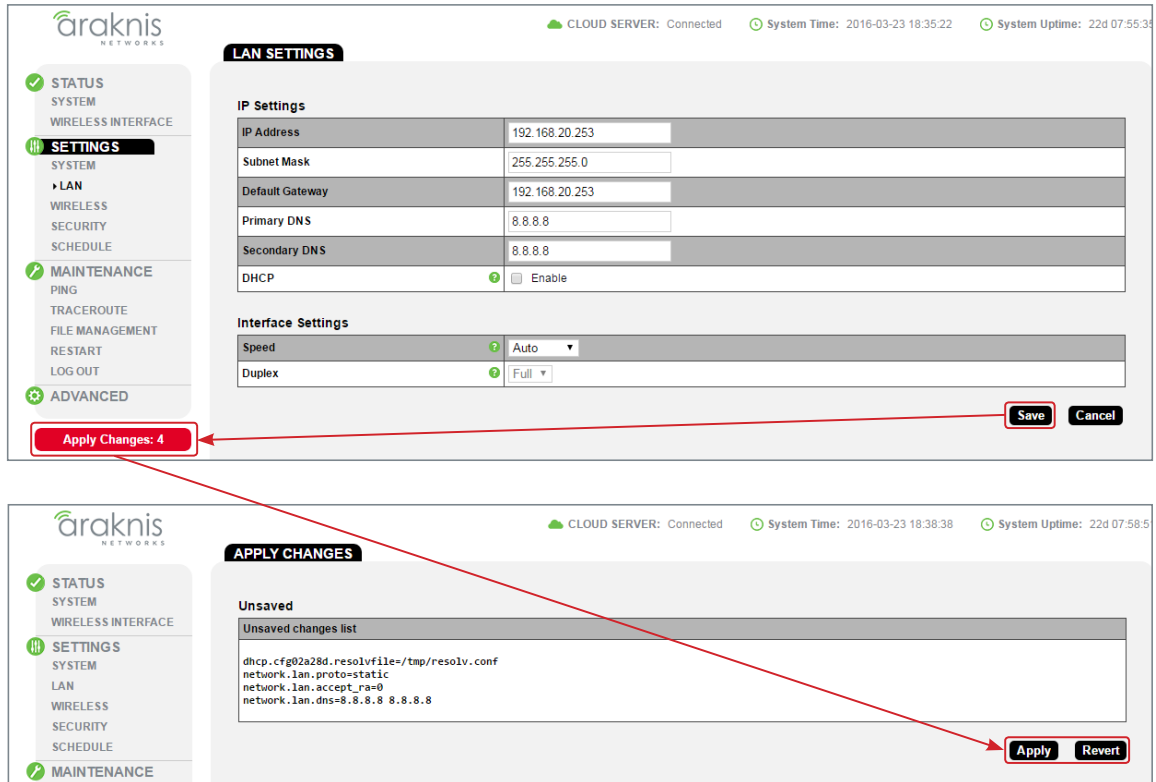
- **A - Main Navigation Menu**  
Use the submenus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the access point. Click **Apply Changes** to review and apply changes made in menus.
- **B - Main Window**  
The main window displays the currently selected submenu.
- **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.



## 10.1 - Applying Changes in the Web Interface

1. After making changes to settings on a menu page, left-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, left-click **Apply Changes** to review the new settings.
3. Left-click **Apply** to make the changes or **Revert** to cancel the changes.

Figure 15. Applying Changes





## 11 - 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.



**Note** - The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

### 11.1 - System Information

Displays current information about the WAP's system settings.

Figure 16. System Information Table

System Information	
System Name	an300
Service Tag	ST1506165101841A
Firmware Version	1.1.04
Management VLAN ID	Untagged

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.



## 11.2 - Wireless Information

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

Figure 17. Wireless Information

Wireless Information		
	2.4GHz	5GHz
MAC Address	D4:6A:91:32:3B:57	D4:6A:91:32:3B:58
Number of Networks	1	2
Number of Connected Clients	0	0
Operation Mode	Access Point	Access Point
TX	0 Bytes	0 Bytes
RX	0 Bytes	0 Bytes

Path – Status, System, Wireless Information

Parameters –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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 respective radio interface since the last power cycle.
- **RX** – Amount of data, in bytes, received on the respective radio interface since the last power cycle.





Figure 18. LAN Information and System Log

LAN Information			
Speed	1Gbps	IP Address	192.168.1.20
Duplex	Full	Subnet Mask	255.255.255.0
MAC Address	D4:6A:91:32:3B:56	Default Gateway	192.168.1.1
TX	111393608 Bytes	Primary DNS	192.168.1.1
RX	746239744 Bytes	Secondary DNS	

**System Log**

```

Mar 23 16:00:01 AN300 user.notice root: starting ntpclient
Mar 23 12:47:45 AN300 user.warn kernel: osif_forward_mgmt_to_app: Received frame length more than expected.
Mar 23 08:00:01 AN300 user.notice root: starting ntpclient
Mar 23 00:00:01 AN300 user.notice root: starting ntpclient
Mar 22 16:00:01 AN300 user.notice root: starting ntpclient
Mar 22 14:45:43 AN300 user.warn kernel: ath_net80211_dfs_clist_update: NOL clear = chan=8703cbd8, freq=5520, vht freq1=5000, fla
Mar 22 14:45:43 AN300 user.warn kernel: ath_net80211_dfs_clist_update: NOL clear = chan=8703cb9c, freq=5500, vht freq1=5000, fla
Mar 22 14:45:43 AN300 user.warn kernel: ath_net80211_dfs_clist_update: NOL clear = chan=8703cb88, freq=5500, vht freq1=5000, fla
Mar 22 14:45:43 AN300 user.warn kernel: ath_net80211_dfs_clist_update: NOL clear = chan=8703cb74, freq=5500, vht freq1=5000, fla
Mar 22 14:45:43 AN300 user.warn kernel: ath_net80211_dfs_clist_update: called, cmd=1, nollist=(null), nentries=0
Mar 22 14:45:43 AN300 user.warn kernel: ath_net80211_dfs_clist_update: NOL clear = chan=8703cbc4, freq=5520, vht freq1=5000, fla

```

### 11.3 - 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 access point network connection. This address may also be found on the access point’s service tag.
- **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.

### 11.4 - System Log

The System Log records changes to access point configuration, connections, security conditions, and more. The window will refresh with the most current activity when the System Status Page is opened.

**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.



## 12 - Wireless interface Status

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

### 12.1 - Radio Status

Provides a detailed look at radio settings and performance.

Figure 19. 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 –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **Interface Status** – Indicates whether the 2.4/5GHz wireless interface is enabled or disabled.
- **Operation Mode** – Access Point is the only mode currently supported.
- **Wireless Mode** – Indicates whether the wireless channel is in 802.11b/g/n or 802.11a/n mode.
- **Channel Bandwidth** – Set the bandwidth of the operating channel to 20MHz or 40MHz.
- **Channel Selection** – Select auto or manual channel selection mode of the wireless interface.
- **Operating Channel** – Indicates the selected channel for the wireless interface.
- **Channel Frequency** – Indicates the frequency of the selected channel.
- **TX** – Amount of data, in bytes, transmitted on each radio interface.
- **RX** – Amount of data, in bytes, received on each radio interface.



## 12.2 - Utilization of SSID

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

Figure 20. 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 –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

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

### 12.2.1 - Wireless Network

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

Figure 21. Wireless Network Status

Wireless Network							
Wireless Network(SSID) ▲	Enabled	Interface	Security ?	VLAN ID	MAC Address	Broadcast SSID ?	Client Isolation ?

Path – Status, Wireless interface, Wireless Network

### Parameters –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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.
- **Channel Isolation** – Indicates whether access point client devices connected to different SSID's can communicate with each other.



## 12.3 - 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 22. Connected Client Status

Repeater	Yes	5GHz	WPA2/PSK AES		D6:6A:91:32:3B:58	No	No
<b>Connected Clients</b> <span style="float: right;">Refresh</span>							
Status	Wireless Network(SSID) ▾	Device Name ▾	MAC Address ▾	TX(KBytes) ▾	RX(KBytes) ▾	RSSI(dBm) ?	Release
<input type="radio"/>		android-1958e62764ee00f0	58:3F:54:F0:67:98				Deny
<input type="radio"/>		Lenovo P...	5C:4D:08:58:D8:FA				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.
- **Interface** - Indicates the channel frequency of a connected wireless 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 **Yes** button to drop a client from the network.



**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.



## 13 - System Settings

### 13.1 - System Information

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

Figure 23. 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 may 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 “20.1.4 - Hardware Factory Default” on page 58).

- **Country** – Select the country of the install location to comply with local standards.  
*Default: United States*

#### Configuration Instructions –

1. Click **Settings, System**.
2. Specify the system information settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.



## 13.2 - Date and Time Settings

Allows configuration of the 'real world' time setting and how it is kept set correctly for all access point functions.

Figure 24. Date and Time Settings

**Date and Time Settings**

Manually Set Date and Time

Date: 2016 / 03 / 23

Time: 16 : 23 (24-Hour)

**Synchronize with PC**

Automatically Get Date and Time

NTP Server: time.nist.gov

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** – Select to automatically get date and time from various web resources.
  - **NTP Server** – Select an NTP (Network Time Protocol) Server to set reference standard date and time.  
*Default: time.nist.gov.*

### Configuration Instructions –

1. Click **Settings, System**.
2. Specify the date and time settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.



## 13.3 - Time Zone

Allows configuration of time zone settings.

Figure 25. Time Zone

Time Zone			
Time Zone:	UTC-05:00 Eastern Time (US & Canada)		
<input checked="" type="checkbox"/>	Enable Daylight Saving		
Start:	March	2nd	Sun 02:00
End :	November	1st	Sun 02:00

Save Cancel

Path – Settings, System, Time Zone

### 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. Click **Settings, System**.
2. Specify the time zone and DST settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.





## 14 - LAN Settings

### 14.1 - IP Settings

The IP Settings menu is used to configure access point IP address settings. In default mode, the IP Settings screen will show the DHCP IP address and default subnet mask.


Figure 26. 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

 **Note** - By default, DHCP is enabled. DHCP is set to be disabled in this image to illustrate all the available options in the menu.

Path - Settings, LAN, IP Settings

#### Parameters -

 **Note** - DHCP is the default setting. If a static IP address has been assigned, but DHCP is selected, the assigned IP address and subnet mask will be grayed out. To confirm the WAP IP address, see: System Status screen/LAN Information/IP address.

- **IP Address** - Uncheck DHCP Enable to enter a static IP address for the device. A static IP address is recommended.

 **Warning** - Use an IP address that is outside the DHCP server range to avoid duplicate addresses in the network.

- **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 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. **Un-check** the box to configure a static IP address (recommended).  
*Default: Enabled*





### Configuration Instructions -

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

## 14.2 - Interface Settings

The Interface Settings menu is used to configure LAN speed and duplex settings.

Figure 27. Interface Settings

Interface Settings	
Speed	Auto
Duplex	Full

Save Cancel

**Path** - Settings, LAN, Interface Settings

### Parameters -

- **Speed** - Select LAN speed from Auto, 1Gbps (300 Series only), 100Mbps, 10Mbps, 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*

### Configuration Instructions -

1. Click **Settings, LAN**.
2. Specify the interface settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.



## 15 - Wireless Settings

### 15.1 - Radio Settings

The Radio Settings screen allows configuration of the access point's radio settings including wireless modes, operating channels, channel bandwidth, and extension channel.

Figure 28. Radio Settings

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

Path - Settings, Wireless, Radio Settings

#### Parameters -



**Note** - The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **Enable Interface** - Enable or disable the radio interface.  
*Default: Yes.*
- **Operation Mode** - Set the radio to Access Point or Repeater mode. See “15.7 - Configuring the WAP as a Repeater” on page 44 for Repeater mode setup instructions.  
*Default: Access Point*
- **Wireless Mode** - Select the wireless mode for the radio. OPTIONS: 2.4GHz: 802.11b/g/n, 802.11b/g, 802.11b, 802.11g, 802.11n; 5GHz: 802.11a/n; 802.11a; 802.11n.  
*Default: 2.4GHz - 802.11b/g/n; 5GHz - 802.11a/n.*
- **Operating Channel** - Select the desired Wi-Fi channel. Use a different channel than other APs 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.

- **Channel Bandwidth** - Select 20/40MHz for auto select; Select 20MHz for better performance as needed; select 40MHz for greater speed as needed. This option is only available in 802.11n modes.  
*Default: 2.4GHz - 20MHz; 5GHz - 40MHz.*
- **Extension Channel** - Only available when Wireless Mode is set to an 802.11n mode and channel Bandwidth is set to 20/40MHz or 40MHz. Extends the 20MHz channel to an Upper or Lower channel to achieve 40MHz bandwidth.  
*Default: 2.4GHz - Upper Channel; 5GHz - Lower Channel.*



## 15.2 - Utilization of SSID

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

Figure 29. 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 –





**Note** - The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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.

## 15.3 - Global Wireless Settings

Configure Band Steering and Fast Roaming.

Figure 30. Global Wireless Settings

Global Settings		
Band Steering	 OFF	<small>NOTE: Band Steering is not supported in repeater mode.</small>
Fast Roaming	 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** - (AN-300 model 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 "15.3.1.1 - Fast Roaming Setup Instructions" on page 37 for setup requirements and instructions.



### 15.3.1 - Fast Roaming Mode

This powerful feature, known in Araknis products as Fast Roaming, is essential for building reliable WiFi networks with multiple access points. After a client joins a WiFi 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.

#### 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

#### Installation Notes

- **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 "24.1 - Configuring Guest Networks with Fast Roaming" on page 79 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 at [www.snapav.com](http://www.snapav.com) for recent updates on compatibility issues.



### 15.3.1.1 - Fast Roaming Setup 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="radio"/> OFF <small>NOTE: Band Steering is not supported in repeater mode.</small>
Fast Roaming ?	<input checked="" type="radio"/> ON <small>NOTE: Fast Roaming is not supported on the radio in use as the repeater.</small>

3. Click Save and then Apply Changes 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

### 15.3.1.2 - Fast Roaming 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.




## 15.4 - 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 31. Wireless Networks

Wireless Networks						
Enable	Name (SSID) ?	Interface ?	Security Mode ?	Broadcast SSID ?	Client Isolation ?	Delete
<input checked="" type="checkbox"/> Yes	HomeLan1	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	

**Path** - Settings, Wireless, Wireless Settings, Wireless Networks

### Parameters -

 **Note** - The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **Enable** - Select **Yes** to turn a wireless network ON.  
*Default: Yes (Checked)*
- **Name (SSID)** - Enter the network name for the network being configured.  
*Default: araknis\_initial; (Blank when adding a new network).*

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

- **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 "15.5 - Wireless Security Setup (SSID Encryption)" on page 39 for wireless security setup instructions.  
*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.  
*Default: Not selected.*
- **Add** - Click to add a wireless network.
- **Delete** - Click to delete a wireless network.

## 15.5 - Wireless Security Setup (SSID Encryption)

The Wireless Security menu opens during the setup of an existing or new wireless network. The options change with the encryption method, so each type of encryption is described in a separate section.

### 15.5.1 - WEP Mode


 **Caution** – WEP mode is outdated and not secure. It is not recommended to use WEP for SSID security. Use WPA or WPA2 mode if possible.

Figure 32. 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"/>

**Save** **Cancel**

**Path** – Settings, Wireless, Wireless Networks, Security Mode

#### Parameters –

- **Name (SSID)** – The name of the network being configured.
- **Security 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 to the Wireless Security Settings for this network. The window will close.



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

Figure 33. 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

**Save** **Cancel**

**Path** – Settings, Wireless, Wireless Networks, Security Mode

### Parameters –

- **Name (SSID)** – The name of the network being configured.
- **Security 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 to the Wireless Security Settings for this network. The window will close.



### 15.5.3 - WPA and WPA2 Modes

Figure 34. Wireless Security – WPA-PSK and WPA2-PSK Modes

Wireless Security	
Name (SSID)	"araknis_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

- **Name (SSID)** – The name of the network being configured.
- **Security Mode** – Select a different encryption mode from the drop-down.
- **Encryption** – Cannot be modified. 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.

## 15.6 - Guest Network

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

**i** **Pro Tip** – For models with 2.4 and 5.0 Ghz radios: If the guest is using an 802.11b/g device, (2.4GHz) they will only need the password to the 2.4GHz Network. If the guest is using an 802.11a/n device (5GHz) they will need the password to the 5GHz Network, and if the guest is using a device that can connect on both 2.4GHz and 5GHz, (iOS devices) they should have both.

**i** **Pro Tip** – Fast Roaming will not work for SSIDs created using the Guest Network feature. To create guest SSIDs with Fast Roaming, see section \_\_\_\_\_

Figure 35. Guest Network

Guest Network					
Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation
<input type="checkbox"/>	Araknis-2.4_GuestNetwork	2.4GHz	Open	<input checked="" type="checkbox"/> Yes	<input checked="" type="checkbox"/> Enable
<input checked="" type="checkbox"/>	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; Araknis-5.0\_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.  
*Default: Open*

**Note** – Guest networks are limited to Open, WPA-PSK Mixed and WPA2-PSK encryption modes. See section “15.5.2 - WPA-PSK Mixed and WPA2-PSK Modes” on page 40 for encryption setup instructions.



- **Broadcast SSID** – Selecting this option will allow the guest network SSID to appear in ‘Network Lists’ on wireless devices for user login. If not selected, the user will have to know the SSID and enter it manually to access the network.  
*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*



## 15.7 - Configuring the WAP as a Repeater

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 to get a wire to a WAP location than to use repeater mode.

### Special Setup Requirements

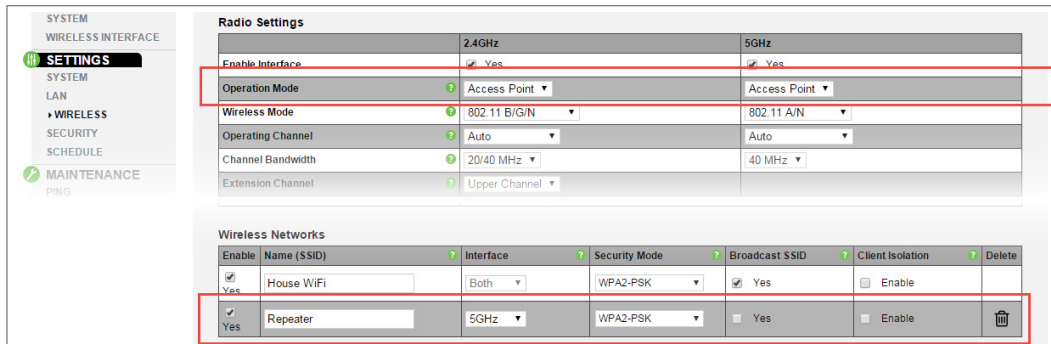
- At least one WAP with a wired LAN connection
- Additional WAP(s) with local power but no LAN connection (must be in range of the wired WAP)
- SSID configuration on each WAP

### Installation Notes

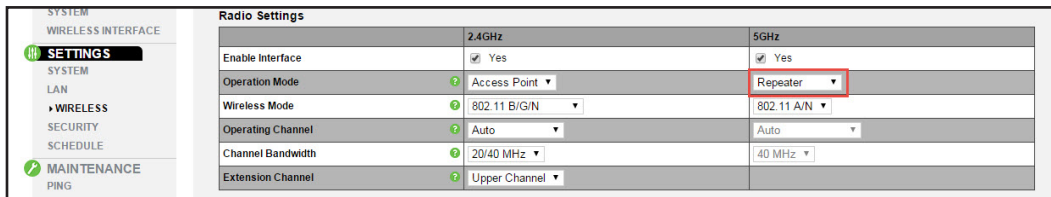
- **Do Fast Roaming and Repeater mode work together?**  
Not for the radio being used as a repeater. Fast Roaming is not required for repeater mode.
- **Can repeater WAPs be used as a wireless bridge? (LAN port to switch or client device)**  
Yes. Connect an Ethernet patch cable from the Ethernet port on the repeater WAP to the client device LAN port.
- **Can multiple unwired repeater WAPs connect to one wired WAP?**  
Yes.
- **If a 300 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 100 and 300 series WAPs work together using Repeater mode?**  
Yes.

### 15.7.1 - Repeater Mode Setup 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.



2. 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).



3. 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.

4. Click Apply and then Apply Changes to enable the new settings.
5. After setup, connect to each SSID on each WAP and confirm that your client device operates as expected.



## 16 - 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.

### 16.1 - User Accounts

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

Figure 36. User Accounts

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

**Add** **Edit**

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. OPTIONS: admin, 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** arrow in the left column of a user account and click **Edit** to modify the account.

#### Configuration Instructions –

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



## 16.2 - Access Control

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

Figure 37. 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: Enable*



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

### Configuration Instructions –

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



## 16.3 - Email Alert

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

Figure 38. 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 <input type="text"/>
Security Mode	None <input type="button" value="Send Test Mail"/>

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.





Figure 39. Common Email Client Ports

Email Client	Ports(TLS)	Ports(SSL)
Gmail	587	465
Outlook	25 or 587	-
Microsoft Exchange	25	465
Yahoo	-	465
Office 365	587	-

### Configuration Instructions -




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



## 16.4 - 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 40. 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: Disable*
- **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 “9.2 - Configured System Name Access” on page 16).  
*Default: Enable*



**Caution** – If VLANs are enabled, this setting will automatically become disabled. In order for VLANs to work correctly, it must remain disabled and will require you to use the local IP address of the WAP in order to gain access to the GUI.

### Configuration Instructions –

1. Click **Settings, Security**.
2. Specify the device discovery settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.



## 17 - Schedule

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

### 17.1 - 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 41. 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 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. Click **Settings, Schedule**.
2. Enable Auto Reboot.
3. Set the desired days and time for reboots to occur.
4. Click **Save**, then **Apply Changes** to enable the new settings.



## 17.2 - 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 42. 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	30 second(s) (10..60)
Timeout Attempts Before Reboot	10 time-out(s) (3..10)
Ping Delay After Auto Reboot	15 minute(s) (5..30)
Reboot Attempts	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.

## 17.3 - 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 43. 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 –

 **Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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;)

### 17.3.1 - 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 44. 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 45. Wi-Fi Scheduler Setup Complete

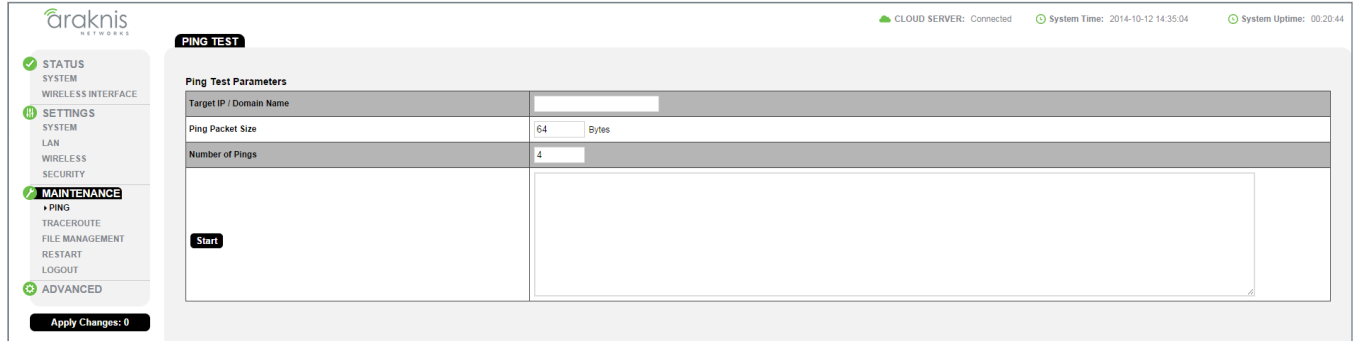
Wi-Fi Scheduler			
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable <small>NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Wi-Fi Scheduler.</small>		
Wireless Radio	2.4GHz ▾		
SSID Selection	Market 2 ▾		
Schedule Templates	Available 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



## 18 - Ping Test

The Ping Test screen can be used to determine if a particular IP address can be reached across an IP network.

Figure 46. 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.

### Configuration Instructions –

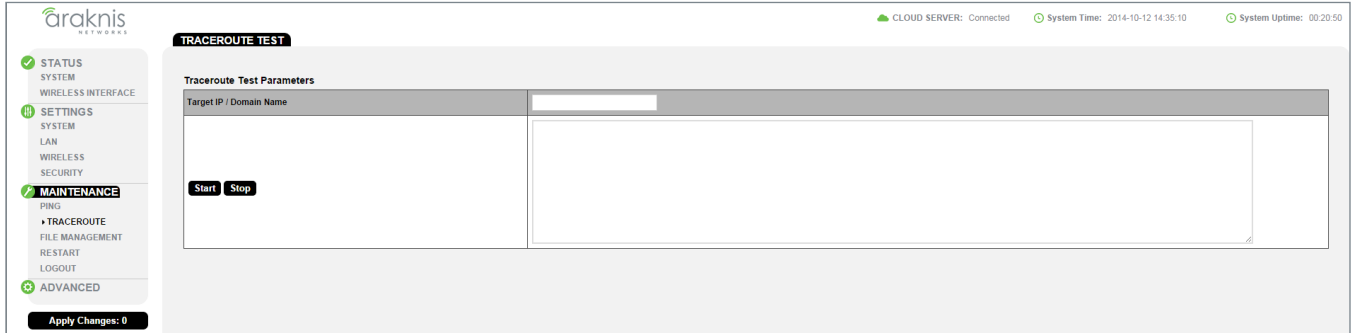
1. Click **Maintenance, Ping**.
2. Specify the ping test settings.
3. Click **Start**.



## 19 - Traceroute Test

The Traceroute Test screen can be used to display the route and delays for data packets to/from a destination on an IP network.

Figure 47. 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.

### Configuration Instructions –

1. Click **Maintenance, Traceroute**.
2. Specify the traceroute test settings.
3. Click **Start**.
4. Click **Stop** to end the test.



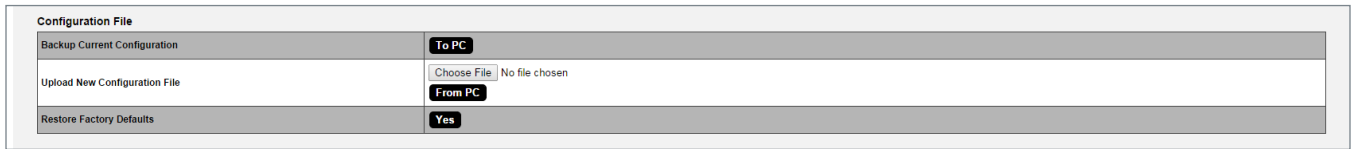
## 20 - File Management

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

### 20.1 - Configuration File

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

Figure 48. Configuration File



Path - Maintenance, File Management, Configuration File

#### 20.1.1 - Backup Current Configuration

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

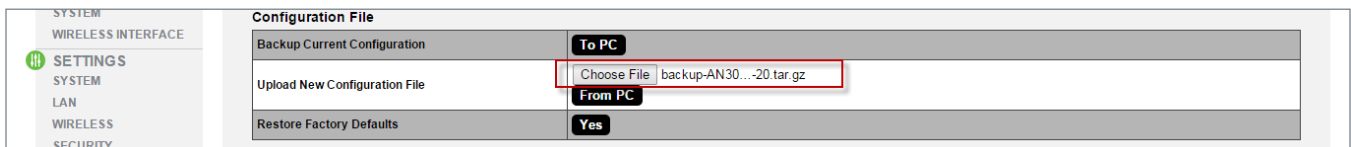
1. Click the To PC button and select a location to save the file.
2. Name the file and save it to your computer.

#### 20.1.2 - 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 in Figure 49. Uploading a New Configuration File, below.
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.

Figure 49. Uploading a New Configuration File



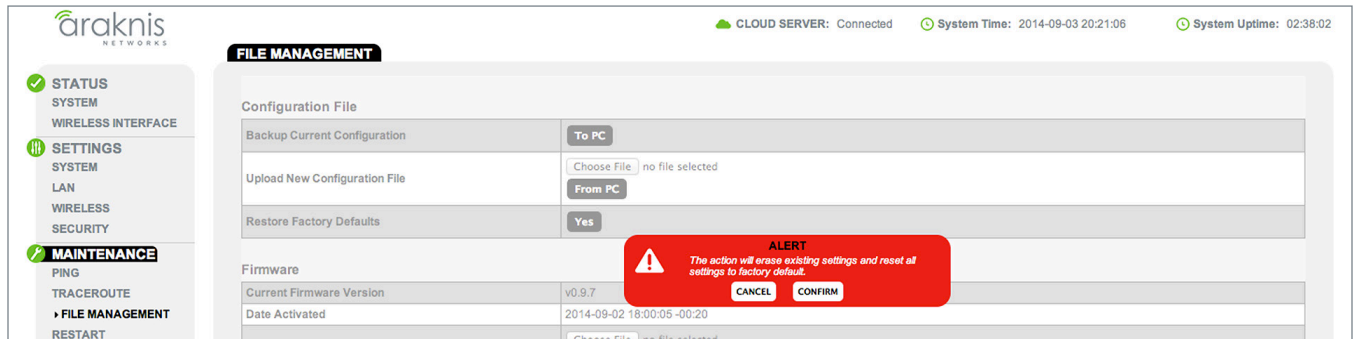


### 20.1.3 - Restore Factory Defaults

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 “9.1 - EZ Access Method (Default)” on page 15.

Figure 50. 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.

### 20.1.4 - 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.

## 20.1.5 - Firmware

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

Figure 51. Firmware

Firmware	
Current Firmware Version	v0.9.2
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.

### Configuration Instructions –

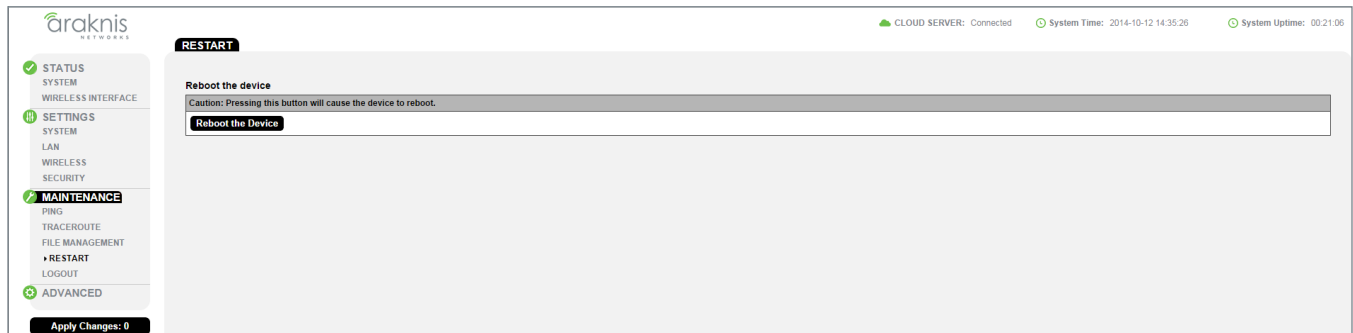
1. Click the **Browse** button to navigate to where the firmware file is saved.
2. Select the file and then press Enter/Return on the computer keyboard or click **Open** on the Upload menu. (The firmware file name should appear next to the Upload New Firmware File **Browse** button.)
3. Click **Upload**. 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.



## 21 - Restart

Reboot the access point.

Figure 52. Restart



Path – Maintenance, Restart

### Configuration Instructions –

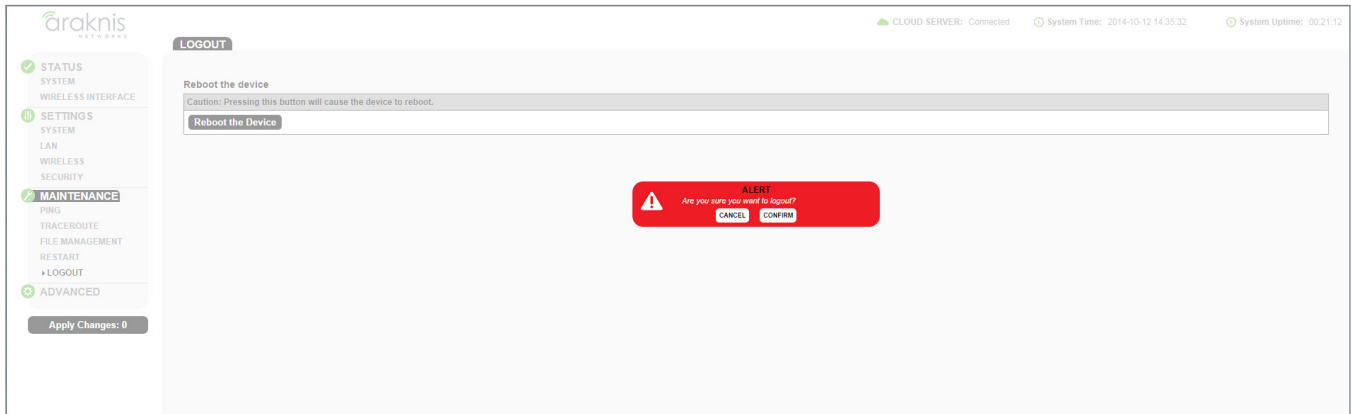
1. Click the **Reboot the Device** button. The message, “This will reboot the device and may take a few seconds...” will appear.
2. Click **OK** to reboot (or **Cancel** to return to the Restart Screen).
3. Wait while the access point reboots. When the device has rebooted, the login screen will appear.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



## 22 - 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 53.** Logout Alert



**Path** – Maintenance, Logout

### Configuration Instructions -

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.

## 23 - Advanced Menu

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

### 23.1 - Advanced Wireless Settings

The Advanced Wireless Settings screen allows configuration of radio settings for unit of measure, data rate, power and RTS/CTS Threshold as well as a client limit by band, (2.4GHz/5GHz).

#### 23.1.1 - Radio Settings

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

Figure 54. Radio Settings

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

Path – Advanced, Wireless Settings, Radio Settings

#### Parameters –

- 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. A higher gain will improve performance but can also 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.  
*Default: Full 100% -29dBm.*
- 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 –

- Click **Advanced, Wireless Settings**.
- Specify the radio settings.
- Click **Save**, then **Apply Changes** to enable the new settings.



## 23.1.2 - Client Limit

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

Figure 55. Client Limit Settings

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

Path – Advanced, Wireless Settings, Client Limit

### Parameters –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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. (For AN-300, the maximum number of clients is for each radio interface.) RANGE: 1-127.  
*Default: 127.*



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

### Configuration Instructions –

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



## 23.2 - Wireless MAC Filter Settings

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

### 23.2.1 - MAC Filter Settings

The MAC Filter Settings screen enables/disables Wireless MAC Filtering.

Figure 56. MAC Filter Settings

MAC Filter Settings	
Enable MAC Filter	<input type="checkbox"/> Yes
Filter Mode	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

Path – Advanced, MAC Filter, MAC Filter Settings

#### Parameters –

- **Enable MAC Filter** – Select Yes to enable MAC Filtering.  
*Default: Not Selected.*
- **Filter Mode** – Select Allow to permit wireless clients access to the wireless network as defined by wireless client MAC address. Select Deny to prevent wireless clients from accessing the wireless network as defined by wireless client MAC address. OPTIONS: Allow, Deny.  
*Default: Allow.*

#### Configuration Instructions –

1. Click **Advanced, MAC Filter**.
2. Specify the wireless MAC filter settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.

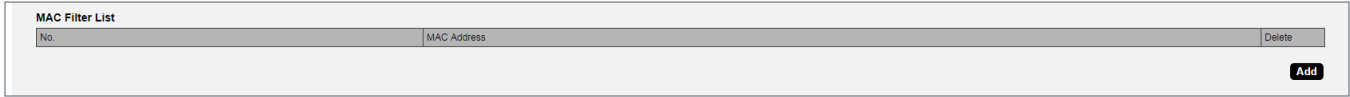




## 23.2.2 - MAC Filter List

The Wireless MAC Filter List screen can be used to add/delete wireless clients to be filtered by MAC address.

**Figure 57.** MAC Filter List



**Path** – Advanced, MAC Filter, MAC Filter List

### Parameters –

- **No.** – The client number for a device being filtered by MAC address.  
*Default: Not available if MAC Filtering is disabled; client number is in the list if MAC Filtering is enabled.*
- **MAC address** – The MAC address of a client being filtered by MAC address, if MAC address filtering is enabled.  
*Default: Blank.*
- **Add** – Click to add a new client to be filtered by MAC address.
- **Delete** – Click to delete an existing client.

### Configuration Instructions –

1. Click **Advanced, MAC Filter**.
2. Specify the MAC filter settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.



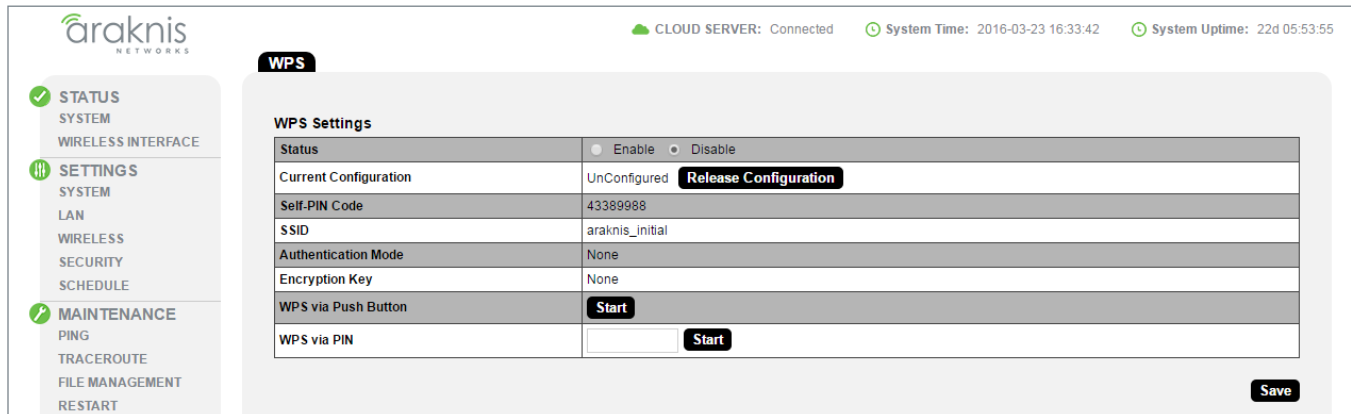
## 23.3 - WPS Settings

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.

Figure 58. WPS Settings Menu



Path – Advanced, WPS

### Parameters –

- **Status** – Enable or disable WPS.  
*Default: Disabled*
- **Current Configuration** – Lists whether the WPS feature is configured or unconfigured.
  - **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.
- **Encryption Key** – Displays encryption key for the SSID.
- **WPS via Push Button** – Click to connect a device using WPS Push Button. See section “23.3.1 - Connecting a Device Using WPS via Push Button” on page 67 for instructions.
- **WPS via PIN** – Used to connect a device using WPS via PIN. See section “23.3.2 - Connecting a Device Using WPS via PIN” on page 68 for instructions.



### 23.3.1 - 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 local interface as an administrator and navigate to Advanced, WPS. Enable WPS if it is disabled (remember to complete the Apply Settings process).

The screenshot shows the 'WPS Settings' configuration page. It features a table with the following rows and content:

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	AtilI4said
WPS via Push Button	<b>Start</b>
WPS via PIN	<input type="text"/> <b>Start</b>

A 'Save' button is located at the bottom right of the form.

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 WiFi operation. WPS-connected devices will appear in the Wireless Interface Status page Connected Clients list.



## 23.3.2 - 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 local interface as an administrator and navigate to Advanced, WPS. Enable WPS if it is disabled (remember to complete the Apply Settings process).

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	Atill4said
WPS via Push Button	<b>Start</b>
WPS via PIN	<input type="text"/> <b>Start</b>

**Save**

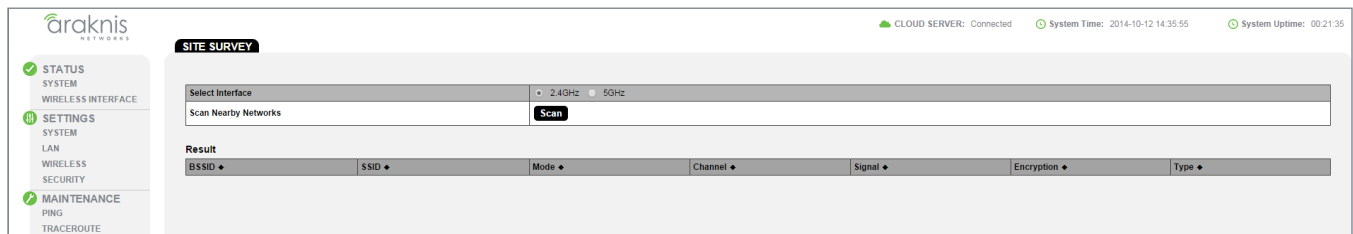
4. In the WAP interface, enter the WPS PIN from the client device in the WPS via PIN field, then click Start.
5. The device will connect. Test connectivity to the device to ensure WiFi operation. WPS-connected devices will appear in the Wireless Interface Status page Connected Clients list.



## 23.4 - 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 59. Site Survey



Path – Advanced, Site Survey

### Parameters –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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 i.e. AP, bridge, etc.
  - **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.

### Configuration Instructions –

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

## 23.5 - 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 60. 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.  
*Default: -75*
- **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.

### 23.5.1 - 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.

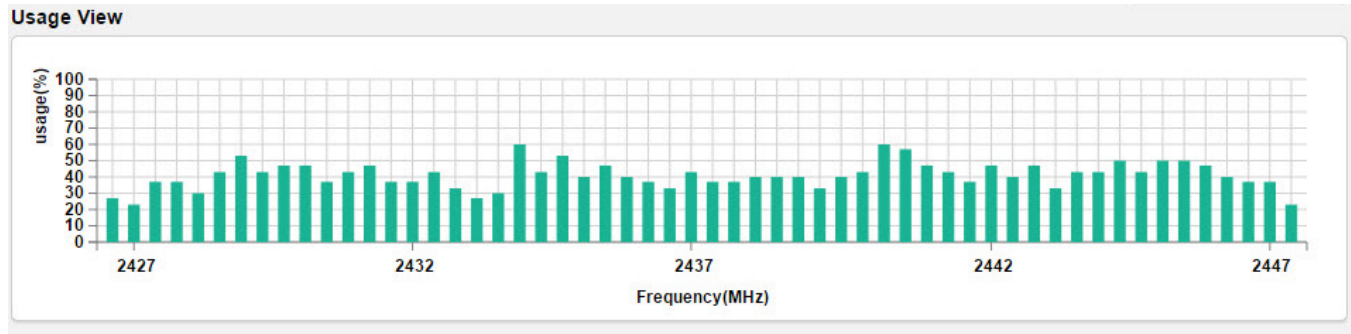
### 23.5.2 - Running a Scan

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.

### 23.5.3 - Understanding Spectrum Analyzer Results

#### Usage View

Figure 61. Spectrum Analyzer Usage View

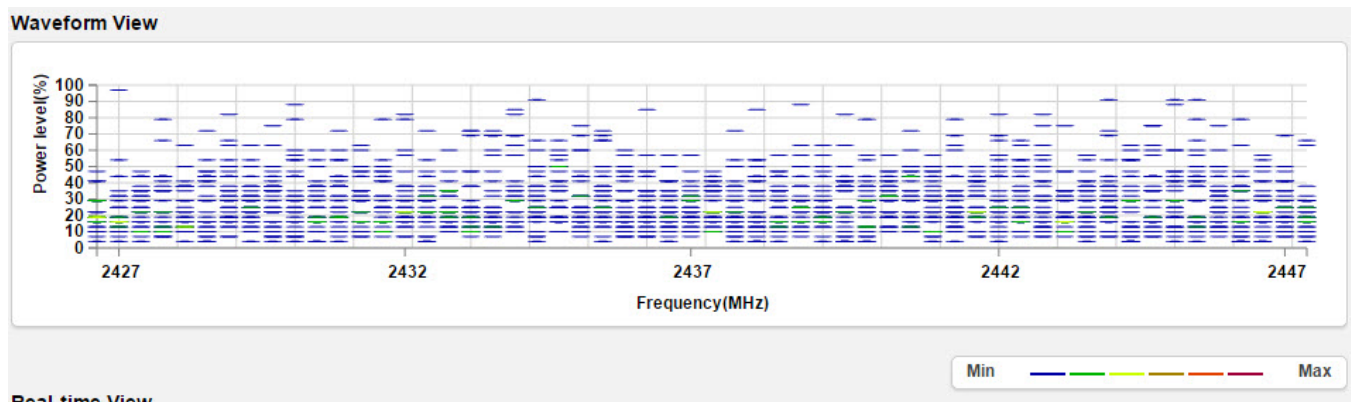


The Usage View displays approximate bandwidth use around the scanned channel. Higher values indicate higher use. Ideally, the channel selected for use will display little to no usage.

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 62. Spectrum Analyzer Waveform View



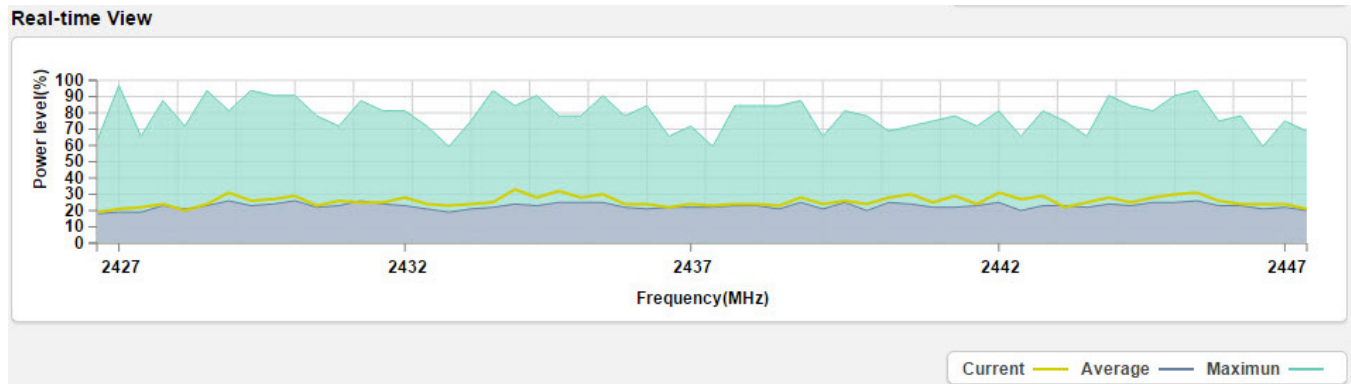
The Waveform view shows the aggregate energy recorded at each scanned frequency. Marks on the graph represent the power level at which signals are being recorded, and the color of the mark roughly estimates how much data is flowing at that level.

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



## Real-time View

Figure 63. 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.

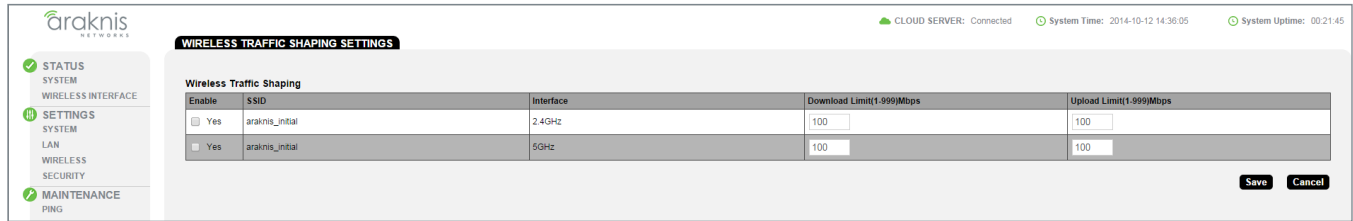




## 23.6 - Wireless Traffic Shaping Settings

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

Figure 64. Wireless Traffic Shaping Settings



Path – Advanced, Traffic Shaping

Parameters –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **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. RANGE: 1-999Mbps.  
*Default: 100Mbps.*
- **Upload Limit** – Enter a value to regulate upload speed. RANGE: 1-999Mbps.  
*Default: 100Mbps.*

Configuration Instructions –

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



## 23.7 - 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.

Figure 65. SNMP Settings

**araknis NETWORKS**

STATUS SYSTEM WIRELESS INTERFACE  
SETTINGS SYSTEM LAN WIRELESS SECURITY  
MAINTENANCE PING TRACEROUTE FILE MANAGEMENT RESTART LOGOUT  
ADVANCED WIRELESS SETTINGS MAC FILTER SITE SURVEY TRAFFIC SHAPING  
SNMP SPANNING TREE VLANS

Apply Changes: 0

CLOUD SERVER: Connected System Time: 2014-10-12 14:36:19 System Uptime: 00:21:59

### SNMP SETTINGS

#### SNMPv2 Settings

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

#### SNMPv3 Settings

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

Save Cancel

Path – Advanced, SNMP

## 23.7.1 - SNMPv2 Settings

This screen allows configuration of SNMPv2 Settings.

Figure 66. SNMPv2 Settings

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

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

## 23.7.2 - SNMPv3 Settings

This screen allows configuration of SNMPv3 Settings.

Figure 67. SNMPv3 Settings

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

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

## 23.8 - 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 68. Spanning Tree 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)

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 –

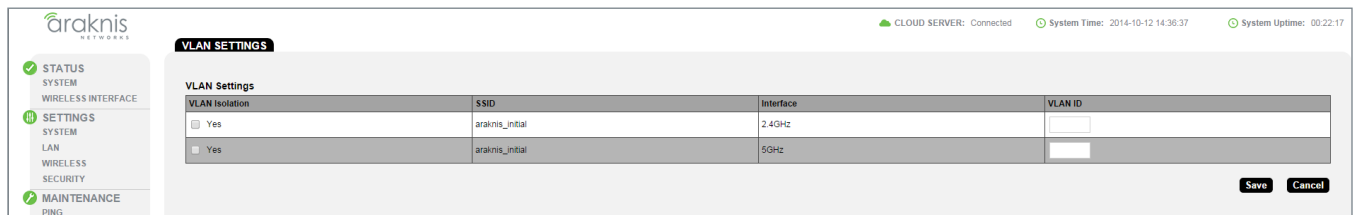
1. Click **Advanced, Spanning Tree**.
2. Specify the Spanning Tree settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.



## 23.9 - 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 69. VLAN Settings



Path – Advanced, VLANS

### Parameters –



**Note** – The AN-100 will indicate settings and information for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

- **VLAN Isolation** – Select Yes to assign a VLAN ID.  
*Default: Not selected.*
- **SSID** – Indicates the network name of the VLAN being tagged. Any Wireless VLANs that need to be tagged should be added in the Wireless Settings page under Wireless Networks. If a Wireless VLAN 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. Click **Advanced, VLANS**.
2. Specify the VLAN settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.

## 24 - Appendix

### 24.1 - 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 NOTE: Band Steering is not supported in repeater mode.

Fast Roaming  ON 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"/> Yes	Employee WiFi	Both	WPA2-PSK	<input checked="" type="checkbox"/> Yes	<input type="checkbox"/> Enable	
<input checked="" type="checkbox"/> Yes	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.

**WLAN SETTINGS**

**VLAN Settings**

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

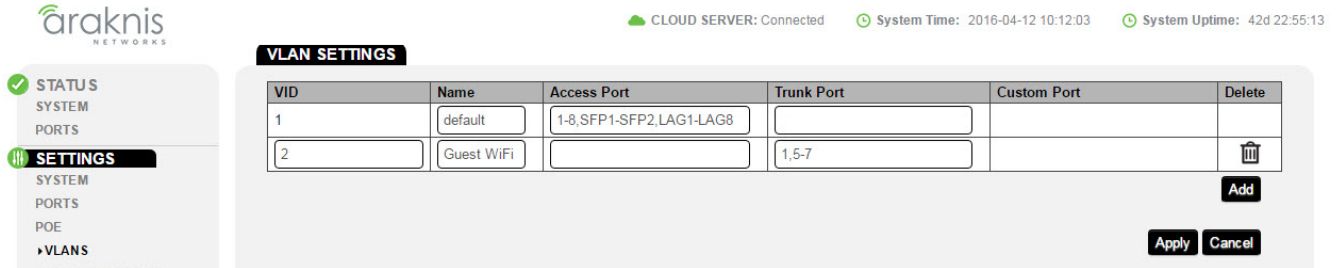
**Save** **Cancel**

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).



*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 dropdowns.
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.

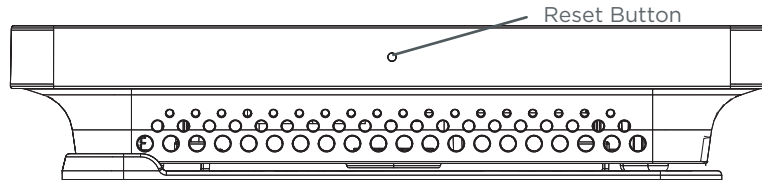


## 25 - Troubleshooting

### 25.1 - Hardware Reset Procedure

If restoring factory defaults does not restore proper functionality to the AN-100/300, a hardware reset may be performed to reload the original base configuration file (saved in the access point's memory).

Figure 70. Reset Button



#### 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



## 26 - Software Defaults

### 26.1 - Basic Menus

Item	Sub-Item	Content	AN-100 Default	AN-300 Default	Comment
SYSTEM	System Information	System Name	an100	an300	
		Operation Mode	Access Point		
		Admin Username	araknis	araknis	
		System LED	ON	ON	ON/OFF
		Management VLAN	Untagged	Untagged	
	Wi-Fi Scheduler	Status	Disable	Disable	
	Time Zone	Time Zone	UTC-05:00 Eastern Time	UTC-05:00 Eastern Time	
LAN	IP Settings	DHCP	Enable	Enable	
	Interface Settings	Speed	Auto	Auto	
		Duplex	Auto		
WIRELESS	Radio Settings	Enable Interface	Yes	Yes	
		Wireless Mode	802.11 B/G/N	802.11 B/G/N	2.4GHz
				802.11 A/N	5.0GHz
		Operating Channel	Auto	Auto	
		Channel Bandwidth	20 MHz	20 MHz	
			40 MHz	40 MHz	
	Extension Channel	Upper Channel	(Upper Channel/ N/A)		
	Wireless Networks	Enable	Yes	Yes	
		Name (SSID)	araknis_initial	araknis_initial	
		Interface	2.4GHz	Both	
		Security Mode	Open	Open	
					Yes
		Broadcast SSID	Yes	Yes	
		Channel Isolation	Disable	Disable	
Guest Network		Enable	Disable	Yes	
SECURITY	User Accounts	Username	araknis	araknis	
		Privilege Level	admin	admin	
		Access Control	HTTP Port	80	80
		Web Access	Enable	Enable	
		Telnet	Enable	Enable	
		SSH	Disable	Disable	
	Email Alert	Status	Disable	Disable	
	Device Discovery	Bonjour	Disable	Disable	
		UPnP	Disable	Disable	



## 26.2 - Advanced Menus

Item	Sub-Item	Content	AN-100 Default	AN-300 Default	Comment	
WIRELESS SETTINGS	Radio Settings	Transmit Power Unit	dBm	dBm	dBm/mW	
		Data Rate	Auto	Auto		
		Transmit Power	Full 100%	Full 100%-29dBm		
		RTS/CTS Threshold (Range:1-2346)	2346	2346		
		Client Limit	Enable	No	No	
		Max Client No.	127	127		
MAC FILTER	MAC Filter Settings	Enable MAC Filter	No	No		
TRAFFIC SHAPING	Wireless Traffic Shaping	Enable	Disable	Disable		
SNMP	SNMPv2 Settings	Status	Enable	Enable		
		Port	161	161		
		Community Name (Read Only)	public	public		
		Community Name (Read Write)	private	private		
		Port	162	162	Trap Destination	
		IP Address			Trap Destination	
		Community Name	public	public	Trap Destination	
	SNMPv3 Settings	Status	Enable	Enable		
		Username	admin	admin	(1-31 Characters)	
		Authorized Protocol	MD5	MD5		
		Authorized Key	12345678	12345678		
		Privacy Protocol	DES	DES		
		Privacy Key	12345678	12345678		
		Engine ID				
SPANNING TREE	Spanning Tree Protocol (STP)	Status	Disable	Disable		
		Hello Time	2	2	seconds (1-10)	
		Max Age	20	20	seconds (6-40)	
		Forward Delay	4	4	seconds (4-30)	
		Priority	32768	32768	(0-65535)	
VLANS	VLAN Settings	VLAN Isolation	No	No		



## 27 - Table of Figures

Figure 1.	Package Contents	6
Figure 2.	Residential Access Point Location	8
Figure 3.	Small Commercial Access Point Location	8
Figure 4.	EIA/TIA 568B Termination Pattern	9
Figure 5.	Network Wiring Diagram	10
Figure 6.	Junction Box Mounting	11
Figure 7.	Drywall Mounting	12
Figure 8.	Ceiling Tile Mounting	12
Figure 9.	Status LED Location	13
Figure 10.	Default SSID	15
Figure 11.	EZ Setup Login Screen	15
Figure 12.	System Name Access	16
Figure 13.	Fing IP Scanner Example	17
Figure 14.	Web Interface Layout	21
Figure 15.	Applying Changes	22
Figure 16.	System Information Table	23
Figure 17.	Wireless Information	24
Figure 18.	LAN Information and System Log	25
Figure 19.	Radio Status	26
Figure 20.	Utilization of SSID Status	27
Figure 21.	Wireless Network Status	27
Figure 22.	Connected Client Status	28
Figure 23.	System Information	29
Figure 24.	Date and Time Settings	30
Figure 25.	Time Zone	31
Figure 26.	IP Settings	32
Figure 27.	Interface Settings	33
Figure 28.	Radio Settings	34
Figure 29.	Utilization of SSID Status	35
Figure 30.	Global Wireless Settings	35
Figure 31.	Wireless Networks	38
Figure 32.	Wireless Security - WEP Mode	39
Figure 33.	Wireless Security - WPA-PSK and WPA2-PSK Modes	40
Figure 34.	Wireless Security - WPA-PSK and WPA2-PSK Modes	41
Figure 35.	Guest Network	42
Figure 36.	User Accounts	46
Figure 37.	Access Control	47
Figure 38.	Email Alert Setup Example	48
Figure 39.	Common Email Client Ports	49



Figure 40.	Device Discovery	50
Figure 41.	Auto Reboot Settings	51
Figure 42.	Gateway Connection Monitor Settings	52
Figure 43.	Wi-Fi Scheduler	53
Figure 44.	Wi-Fi Scheduler Menu	54
Figure 45.	Wi-Fi Scheduler Setup Complete	54
Figure 46.	Ping Test	55
Figure 47.	Traceroute Test	56
Figure 48.	Configuration File	57
Figure 49.	Uploading a New Configuration File	57
Figure 50.	Restore Factory Defaults	58
Figure 51.	Firmware	59
Figure 52.	Restart	60
Figure 53.	Logout Alert	61
Figure 54.	Radio Settings	62
Figure 55.	Client Limit Settings	63
Figure 56.	MAC Filter Settings	64
Figure 57.	MAC Filter List	65
Figure 58.	WPS Settings Menu	66
Figure 59.	Site Survey	69
Figure 60.	Spectrum Analyzer Settings	70
Figure 61.	Spectrum Analyzer Usage View	71
Figure 62.	Spectrum Analyzer Waveform View	71
Figure 63.	Spectrum Analyzer Real-time View	72
Figure 64.	Wireless Traffic Shaping Settings	73
Figure 65.	SNMP Settings	74
Figure 66.	SNMPv2 Settings	75
Figure 67.	SNMPv3 Settings	76
Figure 68.	Spanning Tree Settings	77
Figure 69.	VLAN Settings	78
Figure 70.	Reset Button	82



## 28 - Specifications

### 100/300 Series

Description	AN-100-AP-I-N	AN-300-AP-I-N
<b>Interfaces</b>		
RJ45 10/100/1000Base-T	1	
PoE 802.3at/af compliant	Yes	
Wireless Interface	802.11 b/g/n	802.11 a/b/g/n
Embedded Antennas	Yes	
<b>Performance</b>		
Antenna Type	Omni-directional	
Transmit Power	See MCS table	
Receiver Sensitivity	See MCS table	
802.11n	2x2:2 MIMO	
PHY Data Rate	Up to 300 Mbps	Up to 300 Mbps in both frequency bands
Operating Frequencies	2.4GHz	2.4GHz & 5GHz
Channel Bonding	Yes (20MHz and 40MHz)	
Memory	64MB	128MB
Flash Memory	16MB	16MB
<b>Wireless Features</b>		
Auto Channel Selection	Yes	
Operation Modes	Access Point	
Multiple SSIDs	Yes -up to 8	
Wireless Security	WPA2-PSK (AES + TKIP), WPA-Enterprise	
MAC Address Filtering	Yes	
Hide SSID	Yes	
Guest Network	Yes	
<b>L2 features</b>		
VLANs	Yes - 802.1Q	
QoS	Yes - WME 802.11e	
RJ45 Auto-sensing	Yes	
RJ45 Auto-negotiation	Yes	
Spanning Tree Protocol	Yes, 802.1d	



Description	AN-100-AP-I-N	AN-300-AP-I-N
<b>Management</b>		
Web Management		Yes
Telnet		Yes
SNMP v1, v2c, v3		Yes
DHCP client		Yes
System Log		Yes
Bonjour		Yes
Araknis EZ Access		Yes
UPnP		Yes
Remote Config File Download/Upload		Yes
OvrC Cloud Services		Yes
Wi-Fi Scheduler		Yes
Site Survey		Yes
LED Control		Yes
Auto Reboot		Yes
<b>Environmental &amp; Physical</b>		
Dimensions (W-H-D)	6.9 x 6.9 x 1.3	
External Power Supply	12V 1A DC	12V 2A DC
Temperature Range	Operating: 32° to 122°F( 0 to 50°C) Storage: -4F° to 140°F(-20°C to 60°C)	
Humidity	Operating: 90% or less Storage: 90% or less	
Certifications	CE, FCC, IC, Wi-Fi®	





### MCS Table (RF Performance)

Channel	Data Rate	Transmit Power (combined, dBm)	Receive Sensitivity (combined, dBm)
AN-100-AP-I-N			
802.11b @ 2.4 GHz	1 Mbps	29	≤ -93
	11 Mbps	29	≤ -90
802.11g @ 2.4 GHz	6 Mbps	28	≤ -89
	54 Mbps	25	≤ -71
802.11n HT20 @ 2.4 GHz	MCS 0/8	27	≤ -87
	MCS 7/15	24	≤ -69
802.11n HT40 @ 2.4GHz	MCS 0/8	27	≤ -87
	MCS 7/15	24	≤ -69
AN-300-AP-I-N			
802.11a @ 5GHz	6 Mbps	26	≤ 90
	54 Mbps	23	≤ -72
802.11b @ 2.4 GHz	1 Mbps	29	≤ -99
	11 Mbps	29	≤ -93
802.11g @ 2.4 GHz	6 Mbps	29	≤ -96
	54 Mbps	23	≤ -82
802.11n HT20 @ 2.4 GHz	MCS 0/8	29	≤ -97
	MCS 7/15	23	≤ -78
802.11n HT40 @ 2.4GHz	MCS 0/8	29	≤ -86
	MCS 7/15	23	≤ -69
802.11n HT20 @ 5GHz	MCS 0/8	26	≤ -89
	MCS 7/15	23	≤ -70
802.11n HT40 @ 5GHz	MCS 0/8	26	≤ -87
	MCS 7/15	23	≤ -68



## CE Warning

This is a product with CE certification. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

## AN-100-AP-I-N FCC Statement

### Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

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

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

### Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

### Industry Canada statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

### Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

## Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

## Europe - EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1**  
Safety of Information Technology Equipment
- **EN50385**  
Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- **EN 300 328**  
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 489-1**  
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17**  
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

# CE 0560

Česky [Czech]	Araknis Networks tímto prohlašuje, že tento wireless access point je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede Araknis Networks erklærer herved, at følgende udstyr wireless access point overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt Araknis Networks, dass sich das Gerät wireless access point in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab Araknis Networks seadme wireless access point vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Araknis Networks , declares that this wireless access point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/ EC.



Español [Spanish]	Por medio de la presente Araknis Networks declara que el wireless access point cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Araknis Networks ΔΗΛΩΝΕΙ ΟΤΙ wireless access point ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente Araknis Networks déclare que l'appareil wireless access point est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente Araknis Networks dichiara che questo wireless access point è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo Araknis Networks deklarē, ka wireless access point atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo Araknis Networks deklaruoja, kad šis wireless access point atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart Araknis Networks dat het toestel wireless access point in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, Araknis Networks, jiddikjara li dan wireless access point jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, Araknis Networks nyilatkozom, hogy a wireless access point megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym Araknis Networks oświadcza, że wireless access point jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	Araknis Networks declara que este wireless access point está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	Araknis Networks izjavlja, da je ta wireless access point v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	Araknis Networks týmto vyhlasuje, že wireless access point spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	Araknis Networks vakuuttaa täten että wireless access point tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar Araknis Networks att denna wireless access point står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.



## AN-300-AP-I-N FCC Statement

### Federal Communication Commission Interference Statement

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

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

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

### IMPORTANT NOTE:

#### FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 21cm between the radiator & your body.

#### Industry Canada Statement:

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

#### Caution:

- (i) The device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;
- (ii) high-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.



## Avertissement:

- (i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;
- (ii) De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

## FOR MOBILE DEVICE USAGE

### Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 21cm between the radiator & your body.

### Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 21cm de distance entre la source de rayonnement et votre corps.

## Europe - EU Declaration of Conformity

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC. The following test methods have been applied in order to prove presumption of conformity with the essential requirements of the R&TTE Directive 1999/5/EC:

- **EN60950-1**  
Safety of Information Technology Equipment
- **EN50385**  
Generic standard to demonstrate the compliance of electronic and electrical apparatus with the basic restrictions related to human exposure to electromagnetic fields (0 Hz - 300 GHz)
- **EN 300 328**  
Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive
- **EN 301 893**  
Broadband Radio Access Networks (BRAN); 5 GHz high performance RLAN; Harmonized EN covering essential requirements of article 3.2 of the R&TTE Directive
- **EN 301 489-1**  
Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements
- **EN 301 489-17**  
Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 17: Specific conditions for 2,4 GHz wideband transmission systems and 5 GHz high performance RLAN equipment

This device is a 5GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

CE 0560

Česky [Czech]	Araknis Networks tímto prohlašuje, že tento wireless access point je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.
Dansk [Danish]	Undertegnede Araknis Networks erklærer herved, at følgende udstyr wireless access point overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt Araknis Networks, dass sich das Gerät wireless access point in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab Araknis Networks seadme wireless access point vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, Araknis Networks, declares that this wireless access point is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]	Por medio de la presente Araknis Networks declara que el wireless access point cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ Araknis Networks ΔΗΛΩΝΕΙ ΟΤΙ wireless access point ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente Araknis Networks déclare que l'appareil wireless access point est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente Araknis Networks dichiara che questo wireless access point è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo Araknis Networks deklarē, ka wireless access point atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo Araknis Networks deklaruoja, kad šis wireless access point atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart Araknis Networks dat het toestel wireless access point in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.



Malti [Maltese]	Hawnhekk, Araknis Networks, jiddikjara li dan wireless access point jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, Araknis Networks nyilatkozom, hogy a wireless access point megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.
Polski [Polish]	Niniejszym Araknis Networks oświadcza, że wireless access point jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	Araknis Networks declara que este wireless access point está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	Araknis Networks izjavlja, da je ta wireless access point v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	Araknis Networks týmto vyhlasuje, že wireless access point spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	Araknis Networks vakuuttaa täten että wireless access point tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar Araknis Networks att denna wireless access point står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.





## 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).

## Contacting Technical Support

P: (866) 838-5052

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



© 2016 Araknis Networks®

160412-1255