

WIRELESS ACCESS POINT PRODUCT MANUAL



Models: AN-100-AP-I-N AN-300-AP-I-N AN-500-AP-I-AC AN-700-AP-I-AC

# 1 - About this Manual

This manual was created to provide a reference for installers and end users of Araknis Networks<sup>™</sup> 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:

i	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	
3 -	Hardware Overview	
	3.1 - Тор	
	3.2 - Bottom	
	3.3 - Side	
4 -	Mounting Location - General Guidelines	
5 -	Wiring Requirements	9
	5.1 - Network Cable Requirements	
	5.2 - PoE Requirements	
	5.3 - Power Requirements for Non-PoE Application	.9
	5.4 - Wiring Instructions	9
	5.4.1 - Wiring Diagram	
6 -	Mounting the Access Point	11
	6.1 - Table Top/Shelf	11
	6.2 - Junction Box Mounting	11
	6.2.1 - Instructions	11
	6.3 - Wall or Ceiling Drywall Mounting Instructions	12
	6.4 - Ceiling Tile Mounting Instructions	
7 -	Power-On and Operation	13
	7.1 - Status LED Operation	13
8 -	Introduction to Network Setup	14
9 -	Accessing the Web Interface	
	9.1 - EZ Access Method (Default)	15
	9.2 - Configured System Name Access	
	9.3 - DHCP/Static IP Address Method	
	9.3.1 - Finding the IP Address of the Access Point	
	9.3.2 - Default IP Address Access	18
10 -	· Web Interface Overview	21
	10.1 - Applying Changes in the Web Interface	22
11 -	Status Menu	23
	11.1 - System Status	23
	11.1.1 - System Information	
	11.1.2 - Wireless Information	
	11.1.3 - LAN Information	
	11.1.4 - System Log	
	11.1.4.1 - Using the System Log	27

11.2 - Wireless interface	28
11.2.1 - Radio Status	
11.2.2 - Utilization of SSID	
11.2.3 - Wireless Network	30
11.2.4 - Connected Clients	
12 - Settings Menu	
12.1 - System Settings	
12.1.1 - System Information	33
12.1.2 - Date and Time Settings	
12.1.3 - Time Zone	35
12.2 - LAN Settings	
12.2.1 - IP Settings	37
12.2.2 - Interface Settings	
12.3 - Wireless Settings	
12.3.1 - Radio Settings	_40
12.3.2 - Utilization of SSID	41
12.3.3 - Wireless Networks	
12.3.4 - Wireless Security Menu	
12.3.4.1 - WPA-PSK Mixed and WPA2-PSK Modes	43
12.3.4.2 - WPA and WPA2 Modes	44
12.3.5 - Guest Network	45
12.4 - Security Settings	47
12.4.1 - User Accounts	48
12.4.2 - Access Control	
12.4.3 - Email Alert	
12.4.4 - Device Discovery	
12.5 - Schedule	
12.5.1 - Auto Reboot Settings	
12.5.2 - Auto Ping Gateway Settings	
12.5.3 - Wi-Fi Scheduler	
13 - Maintenance	
13.1 - Ping Test	
13.2 - Traceroute Test	
13.3 - File Management	
13.3.1 - Configuration File	
13.3.1.1 - Backup Current Configuration	61
13.3.1.2 - Upload New Configuration File	
13.3.1.3 - Restore Factory Defaults	
13.3.1.4 - Hardware Factory Default	
13.3.1.5 - Firmware	
13.4 - Restart	
13.5 - Logout	

14 - Advanced Menu	
14.1 - Advanced Wireless Settings	
14.1.1 - Radio Settings	
14.1.2 - Client Limit	
14.2 - Wireless MAC Filter Settings	
14.2.1 - MAC Filter Settings	69
14.2.2 - MAC Filter List	70
14.3 - WPS Settings	
14.3.1 - Configuring WPS Connections	71
14.4 - Site Survey	
14.4.1 - Select Interface	
14.4.2 - Result	
14.5 - Spectrum Analyzer	
14.6 - Wireless Traffic Shaping Settings	
14.7 - SNMP Settings	
14.7.1 - SNMPv2 Settings	
14.7.2 - SNMPv3 Settings	
14.8 - Spanning Tree Settings	
14.9 - VLAN Settings	
14.10 - Rogue AP Detection	
15 - Troubleshooting	
15.1 - Hardware Reset Procedure	
16 - Software Defaults	
16.1 - Basic Menus	
16.2 - Advanced Menus	
17 - Table of Figures	
18 - Specifications	
19 - CE Warning	
20 - AN-100-AP-I-N FCC Statement	
21 - AN-300-AP-I-N FCC Statement	
22 - AN-500/700-AP-I-N FCC Statement	
23 - 2-Year Limited Warranty	
24 - Contacting Technical Support	



# 2 - Welcome to Araknis Networks™

Thank you for choosing an Araknis<sup>™</sup> 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	AN-500-AP-I-N	AN-700-AP-I-N
2.4GHz Radio	Yes	Yes		Yes
5GHz Radio	No	Yes		Yes
Concurrent Dual-band	No	Yes		Yes
Gigabit Ethernet	No	Yes		Yes
PoE Standard	802.3af	802.3af/at		802.3af/at
WiFi Standard	802.11 b/g/n	802.11 a/b/g/n		802.11 a/b/g/n
OvrC Enabled	Yes	Yes		Yes

# 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

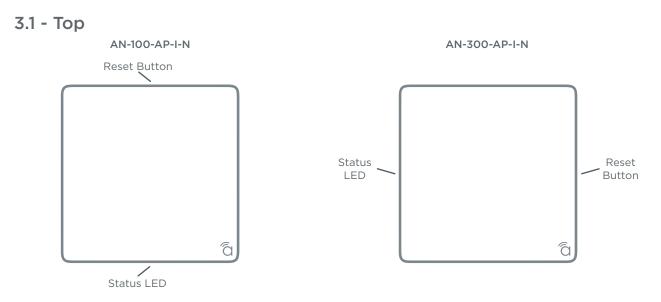
CEEL U

Drywall Mounting Hardware

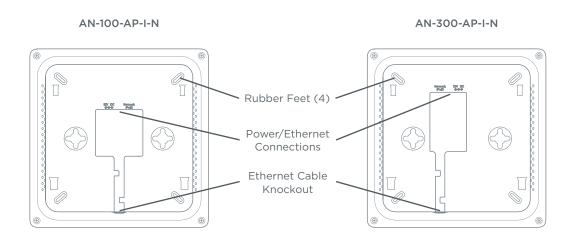


# 3 - Hardware Overview

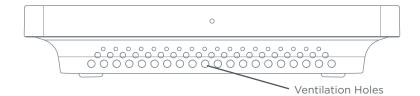
Use these images to familiarize yourself with the physical layout of your access point.



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.

*i* **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

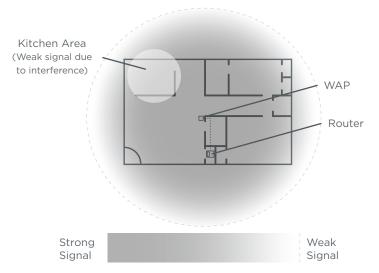
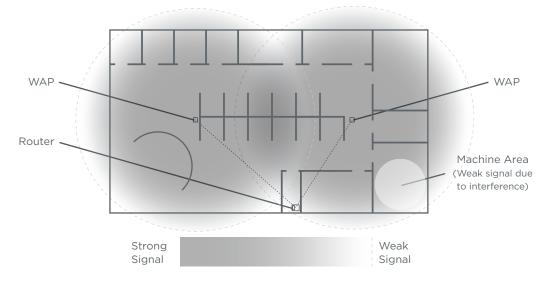


Figure 3. Small Commercial Access Point Location





# 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.

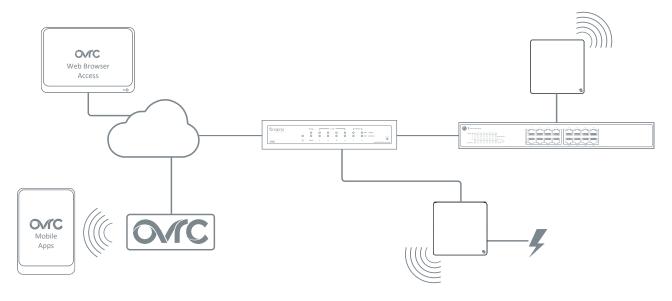
- 1. For PoE installations, install a network cable from the PoE device to the access point and terminate both ends to the same pattern. The DC power supply is not needed.
- 2. For non-PoE installations, locate an outlet for the power supply.

*i* **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

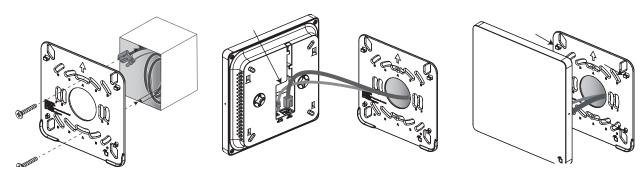
- Place the mounting bracket over the junction box and attach it loosely with 2 screws. (two 6-32 x 1" screws are included) Use the hole pattern on the bracket that best matches the box pattern. See Figure 5A.
- 2. Level or align the bracket with nearby objects for uniformity and tighten the screws enough 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 5B.
- 4. Snap the access point onto the bracket. See Figure 5C.

#### Figure 6. Junction Box Mounting

Figure 6A

Figure 6B

Figure 6C

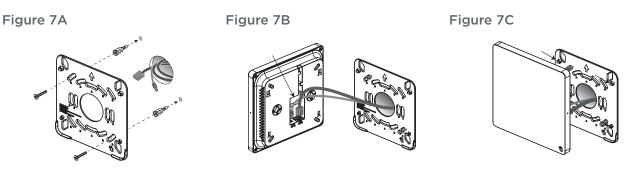




# 6.3 - Wall or Ceiling Drywall Mounting Instructions

- 1. Place the bracket over the desired mounting location with the arrow on the bracket pointing up for wall mounting. See Figure 6A.
- 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 6B.
- 5. Snap the access point onto the bracket. See Figure 6C.

### Figure 7. Drywall Mounting



## 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.

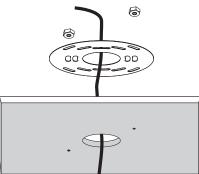
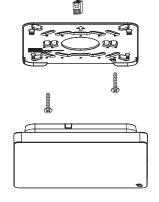


Figure 8. Ceiling Tile Mounting





# 7 - Power-On and Operation

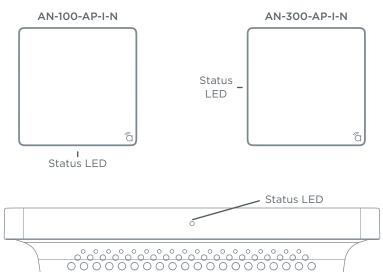
Once the access point is powered, the status LED can be used to determine proper operation.

*i* **Pro Tip –** Check the wireless network connection status in your PC to see if the default SSID "araknis\_initial" is being broadcast. If the SSID is being broadcast, 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)
  - 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

[≡]



PC set to DHCP

WAP set to DHCP by default

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

http://config.an300.wap/ ×		
← → 🗙 🖍 🗋 config.an300.w	ap/	4 🙆 =
Accessing Device	Authentication Required × The server http://10.102.151.11:80 requires a username and password. The server says: The server says: Managed. User Name: Password: Log In Cancel	



## 9.2 - Configured System Name Access

- Note "Araknis EZ Access" on page 52 must be enabled for this access method to work. The setting is enabled by default.
- 1. See section "12.1 System Settings" on page 32 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

http://config.an300.wap/ ×		
← - × ♠ 🗋 config.an300.w	ap/	4 🙆 🗄
Accessing Device	Authentication Required × The server http://10.102.151.11:80 requires a username and password. The server says: The server says: Managed. User Name: Password: Log In Cancel	



[≡]

# 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.

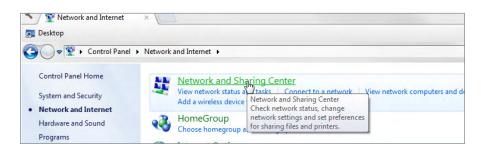
1. Connect your PC to the WAP using a network patch cable.



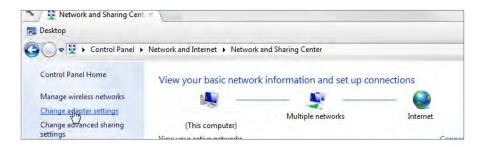
2. On your PC, open the Control Panel and left-click Network and Internet.

Scontrol Panel ×		
Desktop		
OOV Control Panel >		
	Adjust your computer's settings	View by: Category
	System and Security Review your computer's status Back up your computer Find and fix problems           Network and Internet View network statut Chose homegroup, Network and Internet Hardware and View devices and prise Add a device Adjust commonly used mobility settings	User Accounts Change account type Appearance and Personalization Change destop background Adjust screen resolution Clock, Language, and Region Change keyboards or other input methods Ease of Access Let Windows suggest settings Optimize visual display
	Programs	

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.

-	😰 🕨 Control Panel 🕨 Network an	nd Internet 🔸 Network Connecti	ons 🕨			
)rganize •	<ul> <li>Disable this network device</li> </ul>	Diagnose this connection	Rename this connection	Change settir	ngs of this connection	
8	Bluetooth Network Connection 2 Vol connected Bluetooth Device (Personal Area Wireless Network Connection 5 Vol connected Wicrosoft Virtual WiFi Miniport A	fotiss1 Disconnected PPPoP WAN Adapter		Local Area Conne Network cable Intel(R) 82579L	<ul> <li>Disable</li> <li>Status</li> <li>Diagnose</li> <li>Bridge Connections</li> <li>Create Shortcut</li> <li>Delete</li> </ul>	VPN C

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

Connect using: Pheal® L2572LM Gigabit Network Connection Configure This connection uses the following team. If the Gare for Monroek Networks If the Gare for Monroek Networks If the and Pheter Shearing for Monroek Networks If the stand Pheter Shearing for Monroek Network Shearing for Monroek Networks If the stand Pheter Shearing for Monroek Network Shearing for Monroek Networks If the stand Pheter Shearing for Monroek Network	letworking Sharing		
Configure_ This connection uses the following items.	Connect using:		
This connection uses the following terms.	2 Intel(R) 82579LN	I Gigabit Network Conv	nection
Clert for Moroach Networks     Clert for Moroach Networks     Stera of Prese Sharing for Moroach Networks     Linker Sharing for Moroach Networks     Linker Sharing for Moroach Networks     Linke Layer Topology Decovery Nagoer 10 Driver			Configure
	This connection uses th	he following items:	(
	Client for More	pooft Networks	
Main         Fermet Protocol Vesson 6 (CD-VRI-V6)           Main         And Main         Main           Main         And Main         Main           Main         Lark Layer Topology Dacovery Mapper ID Driver         Main           Main         Lark Layer Topology Dacovery Responder         Main           Describtion         Main         Describtion           Describtion         Main         Main           Toponsation         Control         Main           Main         Describtion         Main           Toponsation         Describtion         Main	Cos Packet S	cheduler	
Mill Lineard Protocol Network 11/07/07/09           Mill Homen Protocol Network 11/07/07/09           Mill Homen Protocol Network Processor           Mill Homen Protocol Network Protocol Networ	File and Printe	r Sharing for Microsoft	Networks
Note Lark Layer Topology Discovery Magner I/O Driver         Image I/O Driver           Note Lark Layer Topology Discovery Responder         Image I/O Driver           Instal         Discovery Responder           Describtion         Image I/O Driver           Toponsation Control Peticocity Texant Peticocity         Image I/O Driver           Toponsation Control Peticocity Texant Peticocity         Image I/O Driver	🗹 斗 Internet Protoc	col Version 6 (TCP/IPv	6)
Link Layer Topology Discovery Responder      Instal     Line Layer Topology Discovery Responder      Description     Toromssion Control Peticoch Vennet Pictocch     Toromssion Control Peticoch Vennet Pictocch     The defaat	The second secon	And Magnines & (TJT PUID)	11
Instal Universal Properties Description Transmission Control Protocol/Veternet Protocol. The default wide area network protocol Veternet Protocol. The default			
Description Transmission Control Protocol/Internet Piotocol. The default wide area network protocol that provides communication	🗹 🔺 Link-Layer Top	pology Discovery Maps	per I/O Driver
Description Transmission Control Protocol/Internet Piotocol. The default wide area network protocol that provides communication	🗹 🔺 Link-Layer Top	pology Discovery Maps	per I/O Driver
Transmission Control Protocol/Internet Piotocol. The default wide area network protocol that provides communication	Link-Layer Top     Link-Layer Top	pology Discovery Map; pology Discovery Resp	per I/O Driver
wide area network protocol that provides communication	Link-Layer Top     Link-Layer Top	pology Discovery Map; pology Discovery Resp	per I/O Driver
	A Link-Layer Top     A Link-Layer Top     A Link-Layer Top     Install.	pology Discovery Map; pology Discovery Resp	per I/O Driver
across diverse recommendation records.	Link-Layer Top     Link-Layer Top     Link-Layer Top     Install     Description     Transmission Control	pology Discovery Mapp pology Discovery Resp Uninstall Protocol/Internet Prot	Properties
	Link-Layer Top     Link-Layer Top     Link-Layer Top     Install     Description     Transmission Control wide area network p	pology Discovery Mapp pology Discovery Resp Uninstall Protocol/Internet Piot retocol that provides or	Properties
	Link-Layer Top     Link-Layer Top     Link-Layer Top     Install     Description     Transmission Control wide area network p	pology Discovery Mapp pology Discovery Resp Uninstall Protocol/Internet Piot retocol that provides or	Properties
	Link-Layer Top     Link-Layer Top     Link-Layer Top     Install     Description     Transmission Control wide area network p	pology Discovery Mapp pology Discovery Resp Uninstall Protocol/Internet Piot retocol that provides or	Properties Properties cool. The default communication

- 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





- 8. Left-click OK to close Internet Protocol Version 4 (TCP/IPv4) Properties, then left-click OK to close Wireless Network Connection Properties.
  - Network Connections Desktop Internet Protocol Version 4 (TCP/IPv4) Properties 2 - 8 ..... General Local Area Con You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Networking Shar Connect using: Obtain an IP address automatically 🙎 Intel(R) 82 Use the following IP address: 192 . 168 . 20 . 2 IP address: Subnet mask: 255 . 255 . 255 . 0 Clert f Clert Default gateway: Obtain DNS server address automatically • Use the following DNS server addresses: Preferred DNS server: Ň Alternate DNS server: listal. Validate settings upon exit Advanced... Transmissi wide area Cancel
- 9. Open a web browser and navigate to *http://192.168.20.253/*. Log in using the default credentials:
  - Username: *araknis*
  - Password: araknis

○ 192.168.20.253 ×	
← → X 前 □ 192.168.20.	253
Accessing Device	Authentication Required × The server http://192.168.20.253:80 requires a username and password. The server says: The server says: Managed. User Name: srakniz Password: ******
	Log In Cancel

# **10 - Web Interface Overview**

Figure 14. Web Interface Layout

SYSTEM						
VIRELESS INTERFACE	System Information					
and a second second second	System Name		smith100			
SETTINGS	Service Tag					
SYSTEM	Firmware Version		1.1.00			
AN	Management VLAN ID		Untagged			
SECURITY	Wireless Information		2.4GHz		5GHz	
MAINTENANCE	MAC Address		1 TO A THE REAL PROPERTY OF		0.000	
PING			88:DC:96:1D:33:69		88:DC:96:1D:	33.6A
RACEROUTE	Number of Networks	0			1	
TLE MANAGEMENT	Number of Connected Clients		2		0	
RESTART	Operation Mode		Access Point		Access Point	
OG OUT	TX		2394778880 Bytes		353714816 By	
ADVANCED	RX		971170176 Bytes		151871360 By	rtes
	LAN Information					
Apply Changes: 0	Speed	1Gbps	1	IP Address		192.168.1.20
	Duplex	Full		Subnet Mask		255.255.255.0
	MAC Address	88:DC:9	96:1D:33:68	Default Gateway		192.168.1.1
	TX	101481	9328 Bytes	Primary DNS		192.168.1.1
	RX		072 Bytes	Secondary DNS		8.8.8.8

#### • 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. Left-click **Apply** to make the changes or **Revert** to cancel the changes.

STATUS SYSTEM	IP Settings			
WIRELESS INTERFACE	IP Address	192.168.1.20		
SETTINGS SYSTEM	Subnet Mask	255.255.255.0		
+ LAN	Default Gateway	192.168.1.1		
WIRELESS	Primary DNS	192.168.1.1		
MAINTENANCE	Secondary DNS	8.8.8.8		
PING	DHCP	Enable		
TRACEROUTE FILE MANAGEMENT	line of the second s			
RESTART	Interface Settings Speed	Auto		
ADVANCED	Duplex	Full *		
Apply Changes: 7	• C100	I SERVEP: Connected	045-01-72-72-50-00	Save C
	CLOUR APPLY CHANGES Unsaved	SERVER: Connected O System Time: 2	015-01-22 23:50:00	Save C
Caraknis Status System Wireless Nterface	APPLY CHANGES	SERVER: Connected O System Time: 2	015-01-22 23:50:00	
	APPLY CHANGES Unsaved Unsaved changes list wireless.wi_index0.ssid wireless.wifi0.mianlist wireless.wifi0.mist=1 wireless.wifi0.midx1.msid wireless.wifi0.midx1.ssid	<pre>wAN-300-AP-I-N_1 -0,1 -0,1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1</pre>	015-01-22 23:50:00	
STATUS SYSTEM WIRELESS INTERFACE (1) SECTINGS SYSTEM LAN WIRELESS	APPLY CHANGES Unsaved Unsaved changes list wireless.wfii.network wireless.wfii0.entoork wireless.wfii0.entoork wireless.wfii0.entoork	<pre>wAN-300-AP-I-N_1 -0,1 -0,1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1 -1</pre>	015-01-22 23:50:00	

#### Figure 15. Applying Changes

# 11 - Status Menu

## 11.1 - 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 figures displayed use AN-300-AP-I-N screenshots. AN-100 interfaces will indicate settings and information only for the 2.4GHz channel. The AN-300 will indicate settings and information for the 2.4GHz and 5GHz channels.

Figure 16. System Status Screen

SYSTEM	System Information					
VIRELESS INTERFACE	System Name	smith 100				
ETTINGS	Service Tag					
YSTEM	Firmware Version	1.1.00				
AN	Management VLAN ID	Untagged				
VIRELESS ECURITY ICHEDULE	Wireless Information					
		2.4GHz		5GHz		
	MAC Address	88:DC:96:1D:33:69		88:DC:96:1D:3	33:6A	
RACEROUTE	Number of Networks	0 1		1		
ILE MANAGEMENT	Number of Connected Clients	2		0		
RESTART	Operation Mode	Access Point		Access Point	1	
OG OUT	ТХ	2394778880 Bytes		353714816 By	/tes	
DVANCED	RX	971170176 Bytes		151871360 By	rtes	
Apply Changes: 0	Speed Duplex	1Gbps Full	IP Address Subnet Mask		192.168.1.20 255.255.255.0	
	MAC Address	88:DC:96:1D:33:68	Default Gateway Primary DN S		192.168.1.1 192.168.1.1	
	TX	1014819328 Bytes				
	RX	201073072 Bytes	Secondary DNS		8.8.8.8	
	Sep 8 19:14:37 AN300 daem Sep 8 18:14:58 AN300 daem Sep 8 18:14:58 AN300 daem Sep 8 18:14:58 AN300 user Sep 8 18:14:58 AN300 user	non.info hostapd: ath0: STA 80: non.info hostapd: ath0: STA 9c: non.info hostapd: ath0: STA 9c: warn kernel: [ieee80211_ioct] warn kernel: Node Added (NC=	b7:0d:64:0b:2d WPA: group k b7:0d:64:0b:2d WPA: pairwis _setmlme] non sta mode, ski 2)	ey handshake c e key handshak p to set bssid	ompleted (RSN) e completed (RSN)	
	Sep 8 18:14:46 AN300 daem Sep 8 18:14:45 AN300 user Sep 8 18:14:45 AN300 daem Sep 8 18:14:45 AN300 daem	r.warn kernel: Node deleted (NC non.info hostapd: ath50: STA 34 non.info hostapd: ath0: STA 80 .warn kernel: Node deleted (NC	02:86;bb:32:fd IEEE 802.11: = 0) :02:86:bb:32:fd IEEE 802.11 d2:1d:13:12:b6 WPA: group k	deauthenticat : disassociate		

Path - Status, System



### 11.1.1 - System Information

Displays current information about the WAP's system settings.

#### Figure 17. System Information Table

System Information	
System Name	smith100
Service Tag	
Firmware Version	1.1.00
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.



## 11.1.2 - Wireless Information

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

#### Figure 18. Wireless Information

Wireless Information		
	2.4GHz	5GHz
MAC Address	88:DC:96:1D:33:69	88:DC:96:1D:33:6A
Number of Networks 3	1	1
Number of Connected Clients	2	0
Operation Mode	Access Point	Access Point
тх	2394778880 Bytes	353714816 Bytes
RX	971170176 Bytes	151871360 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 that the device is set up as a Wi-Fi access point.
- **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.



## 11.1.3 - LAN Information

Displays current LAN connection parameters.

Figure	19.	LAN	Information
--------	-----	-----	-------------

Speed	1Gbps	IP Address	192.168.1.20
Duplex	Full	Subnet Mask	255.255.255.0
MAC Address	88:DC:96:1D:33:68	Default Gateway	192.168.1.1
ТХ	1014819328 Bytes	Primary DNS	192.168.1.1
RX	201073072 Bytes	Secondary DNS	8.8.8.8

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 acces 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 AN-100/300.
- Secondary DNS Indicates the secondary DNS for the AN-100/300.



### 11.1.4 - System Log

Records all activity within the access point. The table refreshes to show the most recent activity when the System Status Page is opened.

Figure 20. System Log

Sep	8	19:14:37	AN300	daemon.info hostapd: ath0: STA 80:d2:1d:13:12:b6 WPA: group key handshake completed (RSN)	-
Sep	8	19:14:37	AN300	daemon.info hostapd: ath0: STA 9c:b7:0d:64:0b:2d WPA: group key handshake completed (RSN)	
Sep	8	18:14:58	AN300	daemon.info hostapd: ath0: STA 9c:b7:0d:64:0b:2d WPA: pairwise key handshake completed (RSN)	_
Sep	8	18:14:58	AN300	user.warn kernel: [ieee80211_ioctl_setmlme] non sta mode, skip to set bssid	
Sep	8	18:14:58	AN300	user.warn kernel: Node Added (NC = 2)	
Sep	8	18:14:58	AN300	daemon.info hostapd: ath0: STA 9c:b7:0d:64:0b:2d IEEE 802.11: associated	
Sep	8	18:14:46	AN300	daemon.info hostapd: ath0: STA 34:02:86:bb:32:fd IEEE 802.11: deauthenticated due to local deauth request	
Sep	8	18:14:45	AN300	user.warn kernel: Node deleted (NC = 0)	
Sep	8	18:14:45	AN300	daemon.info hostapd: ath50: STA 34:02:86:bb:32:fd IEEE 802.11: disassociated	
Sep	8	18:14:37	AN300	daemon.info hostapd: ath0: STA 80:d2:1d:13:12:b6 WPA: group key handshake completed (RSN)	
Sep	8	17:51:11	AN300	user.warn kernel: Node deleted (NC = 1)	-

Path - Status, System, System Log

#### Parameters -

• **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.

#### 11.1.4.1 - Using the System Log

- 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.



## 11.2 - Wireless interface

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

Figure 21	. Wireless	Interface	Status
-----------	------------	-----------	--------

STATUS SYSTEM	Radio Status								
WIRELESS INTERFACE					2.4GHz		5GHz		
SETTINGS	Interface Status				Enabled		Enabled		
SYSTEM	Operation Mode				Access Point		Access Point		
LAN WIRELESS	Wireless Mode			0	802.11 B/G/N 802.11 A/N		802,11 A/N		
SECURITY	Channel Bandwidth			9	20MHz 40MHz		40MHz		
SCHEDULE	Channel Selection			0	Auto		Auto		
	Operating Channel				Channel 1		Channel 48		
MAINTENANCE	Channel Frequency			0	2.412 GHz		5.24 GHz		
TRACEROUTE	TX				2803286016 Bytes		431986592 Bytes		
FILE MANAGEMENT	RX				1097777792 Bytes		159262528 Bytes		1
RESTART LOG OUT	Utilization of SSID								
ADVANCED					2.4GHz		5GHz		
	SSID's Used	_			1		1		
Apply Changes: 0	SSID's Available				7		7		
	Wireless Network								
	Wireless Network(SSID) 🔺	Ena	abled Inte	rface	Security 7	VLAN ID	MAC Address	Broadcast SSID *	Client Isolation
	AN-100-AP-I-N_1	Yes	3 2,40	ЗHz	WPA2/PSK AES		88:DC:96:1D:33:69	Yes	No
	AN-100-AP-I-N_1	Yes	s 5GH	Hz	WPA2/PSK AES		88:DC:96:1D:33:6A	Yes	No
	Connected Clients								Refresh
	Wireless Network(SSID) +		Device Name +		MAC Address +	TX(KBytes) +	RX(KBytes) +	RSSI(dbm)	Release
	AN-100-AP-I-N_1		Chromecast		80:D2:1D:13:12:B6	38954	3285	-45	Yes
		161	WhisonantE65	20	9C:B7:0D:64:0B:2D				Yes

Path - Status, Wireless interface



## 11.2.1 - Radio Status

Provides a detailed look at radio settings and performance.

Linura	22	Dadia	Status
rigure	<b>∠</b> ∠.	Raulo	Status

		2.4GHz	5GHz
Interface Status		Enabled	Enabled
Operation Mode		Access Point	Access Point
Wireless Mode	0	802.11 B/G/N	802.11 A/N
Channel Bandwidth	9	20MHz	40MHz
Channel Selection	0	Auto	Auto
Operating Channel	9	Channel 1	Channel 48
Channel Frequency	0	2.412 GHz	5.24 GHz
TX		2803286016 Bytes	431986592 Bytes
RX		1097777792 Bytes	159262528 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.



### 11.2.2 - Utilization of SSID

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

#### Figure 23. Utilization of SSID Status

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

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

### 11.2.3 - Wireless Network

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

#### Figure 24. Wireless Network Status

Wireless Network(SSID) 🔺	Enabled	Interface	Security ?	VLAN ID	MAC Address	Broadcast SSID	Client Isolation
AN-100-AP-I-N 1	Yes	2.4GHz	WPA2/PSK AES		88:DC:96:1D:33:69	Yes	No

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.

### 11.2.4 - 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 25. Connected Client Status

Wireless Network(SSID) +		Device Name ◆	MAC Address 🔶	TX(KBytes) ◆	RX(KBytes) +	RSSI(dbm)	Release
AN-100-AP-I-N_1		Chromecast	80:D2:1D:13:12:B6	38954	3285	-45	Yes
	1	WhisonantE6520	9C:B7:0D:64:0B:2D				Yes

Path - Status, Wireless interface, Connected Clients

#### Parameters -

- 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.

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

# 12 - Settings Menu

## 12.1 - System Settings

The System Settings screen allows configuration of basic system settings.

### Figure 26. System Settings

araknis	SYSTEM SETTINGS	CLOUD SERVER: Connected 🕜 System Time: 2015-09-09 08:20:47. 📀 System Uptime: 14d 16:07:20						
STATUS SYSTEM	System Information							
WIRELESS INTERFACE	System Name	smith100						
	Admin Username	admin						
LAN	Admin Current Password	0						
WIRELESS SECURITY	Admin New Password							
SCHEDULE	Confirm Admin New Password							
MAINTENANCE	System LED 0	• ON @ OFF						
PING TRACEROUTE	Management VLAN	Untagged Tagged 4096						
FILE MANAGEMENT	Country	United States						
RESTART LOG OUT	Date and Time Settings							
ADVANCED	Manually Set Date and Time							
	Date: 2015 / 09 / 09							
Apply Changes: 0	Time: 08 : 20 (24-Hour)							
	Synchronize with PC							
	Automatically Get Date and Time							
	NTP Server: time.nist.gov V							
	Time Zone	Time Zone						
	Time Zone: UTC-05:00 Eastern Time (US & Car	nada) 🔹						
	Enable Daylight Saving							
	Start: March ▼ 2nd ▼ Sun ▼ 02:00 ▼							
	End : November ▼ 1st ▼ Sun ▼ 02:00 ▼							
		Save Cancel						

Path - Settings, System

## 12.1.1 - System Information

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

Figure	27.	System	Information
--------	-----	--------	-------------

System Name	smith100
Admin Username	admin
Admin Current Password	0
Admin New Password	0
Confirm Admin New Password	
System LED	😢 🖲 ON 🍥 OFF
Management VLAN	Untagged 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. Can be used for system name access. See section "9.2 Configured System Name Access" on page 16.
- 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. If Management VLAN=10, your computer must also be on VLAN 10. 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 "13.3.1.4 - Hardware Factory Default" on page 62).
- **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 click Apply Changes to enable the new settings.



### 12.1.2 - Date and Time Settings

The Date and Time menu allows configuration of the 'real world' time setting and how it is kept correct for all access point functions.

#### Figure 28. Date and Time Settings

Manually S	Set Date and	me	
Date: 2015	/ 09	/ 09	
Time: 08	: 20	(24-Hour)	
Synchronize	with PC		
Automatica	ally Get Date	nd Time	

#### 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 click Apply Changes to enable the new settings.



### 12.1.3 - Time Zone

The menu allows configuration of time zone settings.

#### Figure 29. Time Zone

Time Zone: UTC	-05;(	00 Eas	tern T	ime	(US &	Canada)					
Enable Daylig	ht S	aving						-			
Start : March	۲	2nd	• Su	n •	02:00	•					
End : November	۲	1st	v Su	1 .	02:00	•					

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 dropdowns.
  - End Select the month, date, day and time Daylight Saving Time ends from the dropdowns.

#### **Configuration Instructions -**

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



## 12.2 - LAN Settings

The LAN Settings screen allows configuration of the access point LAN connection to the network router. In default mode, the IP Settings screen will show the DHCP IP address and default subnet mask. A static IP address, subnet mask, default gateway and DNS settings can be configured by disabling DHCP. LAN speed can also be configured in the Interface Settings menu.

Figure	30.	LAN	Settings
--------	-----	-----	----------

araknis	LAN SETTINGS	CLOUD SERVER: Connected O System Time: 2015-09-09 08:32:23 O System Uptime: 14d 16:191
STATUS SYSTEM	IP Settings	
WIRELESS INTERFACE	IP Address	192.168.1.20
SETTINGS SYSTEM	Subnet Mask	255.255.255.0
+ LAN	Default Gateway	192.168.1.1
WIRELESS SECURITY	Primary DNS	192.168.1.1
SCHEDULE	Secondary DNS	8.8.8
MAINTENANCE	DHCP	0 Enable
TRACEROUTE FILE MANAGEMENT	Interface Settings	
	Speed	Auto T
RESTART		

Path - Settings, LAN



### 12.2.1 - 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 31. IP Settings	Figure	31.	IΡ	Settings
------------------------	--------	-----	----	----------

IP Settings		
IP Address	192.168.1.20	
Subnet Mask	255.255.255.0	
Default Gateway	192.168.1.1	
Primary DNS	192.168.1.1	
Secondary DNS	8.8.8.8	
DHCP	🔞 🗐 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 AN-100/300. A static IP address is recommended.

**Warning -** Be sure to 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 AN-100/300. 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 AN-100/300. This will typically be the network router IP address.
- Secondary DNS With DHCP disabled, enter the secondary DNS for the AN-100/300. This will 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 click Apply Changes to enable the new settings.

### 12.2.2 - Interface Settings

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

### Figure 32. Interface Settings

Speed	1	Auto 🔹	
Duplex	0	Full 💌	

### 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

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



# 12.3 - Wireless Settings

The Wireless Settings screen allows configuration of the access point's wireless settings and connections including 2.4GHz and 5GHz Radio settings, setup and configuration of wireless networks (SSID's) and all required wireless modes, channels, security settings and, guest network configuration.

	idio s	Settings						_			
RELESSINTERFACE				2.4GHz				5GHz			
ETTINGS Er	hable I	Interface		Yes				Y Y	es		
	peratio	on Mode		Access Point	•			Acce	ss Point 🔹	h	
INCLES 5	ireles	s Mode	0	802.11 B/G/N	•			802.1	1 A/N 🔻		
CURITY OF	peratir	ng Channel	6	Auto				Auto	· ·		
AINTENANCE	hanne	I Bandwidth	0	20 MHz 🔻	-		÷ 1	40 M	Hz ▼		
NG	ctensi	on Channel	9	Upper Channel 🔻							
ACEROUTE		A Second									
LE WANAGEWENT	ilizati	ion of SSID	_	0.400	_						_
ESTART DG OUT SS	SID's (	lised		2.4GHz				5GHz			
	SSID's Available			7				7			
					_						_
Apply Changes: 0	-	s Networks			_			_	_		
	-	Name (SSID)	2	Interface ?	Securit	ty Mode 👘 🤌	Band Steering	\$	Broadcast \$SID	Client Isolation	? Del
2 Ve		AN-100-AP-I-N_1		Both •	WPA2	-PSK 🔹	Yes		Yes	Enable	
Yes											
and the second se	2012	Network									A
Er	nable	Network Name (SSID)		Interface		Security Mode	3	Broa	idcast SSID	Client Isolation	A
and the second se	nable	C.P. Concerna.	1	Interface 2.4GHz		Security Mode	2	Broa		Client Isolation	A
Er	nable es	Name (SSID)	1					8			
Er Ye	nable es es	Name (SSID) Araknis-2.4_GuestNetwork	1	2.4GHz		Open	•	8	Yes	🕑 Enable	A
Fi Ye Wi	nable es es anual	Name (SSID) Araknis-2.4_GuestNetwork Araknis-5.0_GuestNetwork	1	2.4GHz		Open	•	8	Yes	🕑 Enable	A
Fi Ye Mi Gr	nable es es anual	Name (SSID) Araknis-2 4_GuestNetwork Araknis-5.0_GuestNetwork IP Settings y IP Address		2.4GHz 5GHz		Open	•	8	Yes	🕑 Enable	A
Fi Ye Ye Si	nable es es anual ateway ubnet l	Name (SSID) Araknis-2 4_GuestNetwork Araknis-5.0_GuestNetwork IP Settings y IP Address		2.4GHz 5GHz 192.168.200.1		Open	•	8	Yes	🕑 Enable	
Fi Yee Gi Su	nable es es anual ateway ubnet l	Name (SSID) Araknis-2 4_GuestNetwork Araknis-5.0_GuestNetwork IP Settings y IP Address Mask		2.4GHz 5GHz 192.168.200.1		Open	•	8	Yes	🕑 Enable	
Fi Ye Mi Gi St	nable es es anual atewa ubnet l utoma tarting	Name (SSID) Araknis-2 4_GuestNetwork Araknis-5.0_GuestNetwork IP Settings y IP Address Mask tic DHCP Server Settings		2.4GHz 5GHz 192.168.200.1 255.255.255.0		Open	•	8	Yes	🕑 Enable	

Figure 33. Wireless Settings (AN-300-AP-I-N interface shown)

Path - Settings, Wireless



# 12.3.1 - 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 34. Radio Settings

		2.4GHz	5GHz
Enable Interface		🕑 Yes	Ves Ves
Operation Mode		Access Point T	Access Point
Wireless Mode	0	802.11 B/G/N 🔹	802.11 A/N 🔻
Operating Channel	9	Auto 🔹	Auto
Channel Bandwidth	0	20 MHz 🔻	40 MHz 🔻
Extension Channel	9	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.*
- 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.* 
  - *i* **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 ultimate 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.
  - *i* **Pro Tip –** The access point features a Site Survey tool that shows all 2.4GHz/5GHz networks and settings. Use the tool to scan the wireless neighborhood and find the channel with the least amount of interference and the extension channel with less traffic from other wireless devices.



### **Configuration Instructions -**

- 1. Click Settings, Wireless.
- 2. Specify the radio settings.
- 3. Click **Save**, then click **Apply Changes** to enable the new settings.

## 12.3.2 - Utilization of SSID

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

#### Figure 35. Utilization of SSID Status

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

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



# 12.3.3 - 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 36. Wireless Networks

Enable	Name (SSID)	lnterface	Security Mode	Band Steering	Broadcast SSID	Client Isolation	Delete
₩ Yes	AN-100-AP-I-N_1	Both 🔻	WPA2-PSK V	Yes	Yes	📄 Enable	1

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 ("Figure 37. Wireless Security – WPA-PSK and WPA2-PSK Modes" on page 43).
- **Band Steering –** (AN-300-AP-I-N only) Band steering uses both signal quality and throughput relative to the client device to determine whether the client should communicate on the 2.4- or 5GHz band. This optimizes signal strength to the device. *Default: Disabled (Unchecked)*
- **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.



## 12.3.4 - Wireless Security Menu

The Wireless Security menu opens during the setup of an existing or new wireless network.

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

Figure 37. Wireless Security - WPA-PSK and WPA2-PSK Modes

Wireless Security		
Name (SSID)		"WAP2"
Security Mode	0	WPA2-PSK •
Encryption	0	AES •
Passphrase	0	
Group Key Update Interval	0	3600

Path - Settings, Wireless, Wireless Networks, Security Mode

### Parameters -

- Name (SSID) The name of the network being configured.
- **Security Mode** Select a mode from the drop-down. Use the same mode as the network router and other APs on the network. Selecting a non-PSK mode will cause the menu options to change.
- 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.

### 12.3.4.2 - WPA and WPA2 Modes

Wireless Security	
Name (SSID)	"araknis_initial"
Security Mode 0	WPA2 \$
Encryption 0	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	
	600

Figure 38. Wireless Security – WPA-PSK and WPA2-PSK Modes

- Name (SSID) The name of the network being configured.
- **Security Mode –** Select a mode from the drop-down. Use the same mode as the network router and other APs on the network. Selecting a PSK mode will cause the menu options to change.
- 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.



# 12.3.5 - Guest Network

Use the Guest Network menu to configure guest networks. These optional networks are useful for allowing access to temporary users and controlling what parts of the network they can access.

#### Figure 39. Guest Network

Enable	Name (SSID)	Interface	Security Mode	Broadcast SSID	Client Isolation
Yes	Araknis-2.4_GuestNetwork	2.4GHz	Орел 🔻	Ves	🕑 Enable
Yes	Araknis-5.0_GuestNetwork	5GHz	Open 🔹	Ves	🥜 Enable
Manual	IP Settings				
Gatewa	y IP Address	192.168.200.1			
Subnet	Mask	255.255.255.0			
Automa	tic DHCP Server Settings				
Starting	IP Address	192.168.200.100			
Ending	P Address	192,168.200.200			
WINS S	erver IP	0.0.0.0			

Path - Settings, Wireless, Guest 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.

- Enable Select to create a guest network. This will allow guests to log in to the wireless system without having to compromise network security by giving guests the password to the home network. There are separate 2.4GHz and 5GHz Guest Networks. 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. *Default: Not Selected.*
- Name (SSID) Enter an SSID for the guest network. Default: Araknis-2.4\_GuestNetwork; Araknis-5.0\_GuestNetwork
- Edit Click the Edit button to open the Guest Network Security Setup Window.

Note - Guest networks are limited to Open, WPA-PSK Mixed and WPA2-PSK encryption modes. See section "12.3.4.1 - WPA-PSK Mixed and WPA2-PSK Modes" on page 43 for encryption setup instructions.

Security Mode – This indicates the Security Mode and Encryption selected in the Edit Mode, previous.

Default: None

• **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: Un-selected.

 Channel Isolation – Select to prevent communication between wireless clients on different SSID's of the guest network.

Default: Selected.

- Manual IP Settings Use the access point's defaults or manually enter IP address settings.
  - Gateway IP Address Enter the access point's Guest Network Gateway IP address. *Default: 192.168.200.1*
  - **Subnet Mask** Enter the subnet mask for the access point's Guest Network Gateway. *Default: 255.255.255.0*
- Automatic DHCP Server Settings
  - **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*



# 12.4 - 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.

### Figure 40. Security Settings

	SECURITY SETTINGS					
STATUS SYSTEM	User Accounts					
WIRELESS INTERFACE	Select Username	Privileg	e Level	Password	Confirm Password	Delet
SYSTEM	admin	admin		*****	****	创
LAN WIRELESS • SECURITY SCHEDULE	Access Control					Add Edit
MAINTENANCE	HTTP Port	80				
PING TRACEROUTE FILE MANAGEMENT RESTART	Web Access	0 E	nable 🔻			
	Teinet	0 D	sable 🔻			
	SSH	<b>0</b> D	sable 🔻			
LOG OUT	Email Alert					
ADVANCED	Status		Enable			
Apply Changes: 0	From					
	To					
	Subject					
	Email Account					
	Username					
	Password					
	SMTP Server	Po	rt:			
	Security Mode	S	SL/TLS •			Send Test Mail
	Device Discovery					
	Bonjour	0 S	sable 🔻			
	UPnP	<b>e</b> D	isable 🔻			
	Araknis EZ Access	e E	nable 🔻			

Path - Settings, Security



### 12.4.1 - User Accounts

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

#### Figure 41. User Accounts

ccounts				
Username 📀	Privilege Level	Password 📀	Confirm Password	Delete
admin	admin	***	***	匬
			Add	Edit
	Username ?	Username C Privilege Level C	Username   Privilege Level  Password	Username         Privilege Level         Password         Confirm Password           admin         admin         *******         *******

### Path - Settings, Security, User Accounts

### Parameters -

- **Select -** Select to allow editing of the selected table entry. *Default: Not selected*
- Username Click the Edit button to access the settings on a selected User Account. Enter a new username for logging into the access point. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces. Default: araknis (Blank when adding a new account)
- **Privilege Level** Indicates the level of device management for the logged in user. 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.

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



# 12.4.2 - Access Control

The Access Control menu allows configuration of how the access point can be accessed.

### Figure 42. Access Control

Access Control			
HTTP Port	8	80	
Web Access	0	Enable 🔻	
Telnet	6	Disable 🔻	
SSH	0	Disable 🔻	

Path - Settings, Security, Access Control

### Parameters -

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

*i* **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

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

# 12.4.3 - Email Alert

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

Email Alert		
Status	Enable	
From		
То		
Subject		
Email Account		
Username		
Password		6.4
SMTP Server	Port	
Security Mode	SSL/TLS	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 44. 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	-

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



# 12.4.4 - 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 45. Device Discovery

Bonjour	6	Disable 💌	
UPnP	0	Disable 🔻	
Araknis EZ Access	8	Enable •	

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.

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



# 12.5 - Schedule

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

Figure -	46.	Schedule	Settings	Menu
----------	-----	----------	----------	------

STATUS SYSTEM	Auto Reboot Settings					
WIRELESS INTERFACE	Status	Enable • D NOTE Please assure	Disable a that the Time Zone Settings is synted i	Min your local time when en	abing the Auto Record Settings.	
SETTINGS SYSTEM	Date		ay Monday Tuesday W	CONTRACTOR OF A DATE	THE REPORT OF THE PARTY OF THE	
LAN WIRELESS	Time	Time 0 0 (24-Hour)				
SECURITY • SCHEDULE	Auto Ping Gateway Settings					
MAINTENANCE	Status	Enable • Disable NOTE Please asswe that the Time Zoné Settings is synced with your local time when enabling the Aud Ping Baseway Settings.				
PING	Gateway IP Address	Get Current Gateway IP				
TRACEROUTE FILE MANAGEMENT	Timeout Before Reboot	30 second(s	i) (1060)	-		
RESTART	Continuous Ping Timeouts	10 time-outs (310)				
ADVANCED	Ping Delay After Auto Reboot	15 minute(s) (530)				
ADVANCED	Reboot Attempts	5 reboots (	010, 0=Infinite reboots)			
	Status	Enable • NOTE: Please assu	Disable re that the Time Zone Settings a syncad	with your local time when e	nabing the W-F. Scheduler	
	Wireless Radio	2.4GHz 🔻				
	SSID Selection	AN-100-AP-I-N_				
	Schedule Templates	Choose a templa		1		
		Day	Availability	Duration		
		Sunday	available •	00 : 00		
		Monday	available •	00 ; 00		
	Schedule Table	Tuesday	available •	00 : 00		
		Wednesday	available 🔹	00 : 00		
		Thursday	available 🔻	00 : 00	~ 24 : 00	
		Friday	available •	00 ; 00	~ 24 ;00	
		Saturday	available 🔻	00 : 00	~ 24 :00	

Path - Settings, Schedule



# 12.5.1 - 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 47. Auto Reboot Settings

Auto Reboot Settings	
Status	Enable      Disable     NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Auto Reboot Settings.
Date	Every: Sunday Monday Tuesday Wednesday Thursday Friday 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)

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



# 12.5.2 - Auto Ping Gateway Settings

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 48. Auto Reboot Settings

Auto Ping Gateway Settings					
Status	Enable Disable				
Gateway IP Address	NOTE:	NOTE: Please assure that the Time Zone Settings is synced with your local time when enabling the Auto Ping Gateway Settings.  Get Current Gateway IP			
Timeout Before Reboot	30	second(s) (10.60)			
Continuous Ping Timeouts	10	time-outs (310)			
Ping Delay After Auto Reboot	15	minute(s) (530)			
Reboot Attempts	5	reboots (010, 0=Infinite reboots)			

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)

*i* **Pro Tip -** Set the WAP to reboot when there are few or no users connected. This will ensure that users have the best experience when connected to the WAP.

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





# 12.5.3 - 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 49. Wi-Fi Scheduler

Status	Endote + Distance (1979) Malan Analy from The London gradients on factors from the Analysis (1975) Secure				
Wireless Radio	.2.4GHz •	2.4042 *			
SSID Selection	araknis_initial •	araknja jelital •			
Schedule Templates	Choose a template	Choose a temptate •			
	Day	Availability	Duration		
	Sunday	available 🔻	00 00 - 24 00		
	Monday	availably	00 - 00 - 24 00		
	Tuesday	avadable 🔹	00 00 - 24 ::00		
Schedule Table	Wednesday	avarlable 💌	00 24 20		
	Thursday	available	00 00 ~ 24 00		
	Friday	available	00 24 00		
	Saturday	availably 🔹	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;)



# **Configuration Instructions -**

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	50	Wi-Fi	Scheduler	Menu
I I gai c	~~.	***	Schedaler	1 10110

Wi-Fi Scheduler					
Status	Enable Disable (07E Please searce instrine Time Zone George is syncelliwin your cost line when anothing the WHP Gineoular				
Wireless Radio	2.4GHz ¥				
SSID Selection	Market 2 V				
Schedule Templates	Available 8-17 dail	y 🔻			
	Day	Availability	Duration		
	Sunday	available •	08 00 ~ 17 00		
	Monday	available 🔹	08 00 ~ 17 00		
Schedule Table	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 dropdown 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.

Wi-Fi Scheduler					
Status	Enable Disable (4015) Please assure that the Time Done Bettings is synced with your cost time when encoung the WAPI Surequier				
Wireless Radio	2.4GHz 🔻	2.4GHz V			
SSID Selection	Market 2 💌	Market 2 🔹			
Schedule Templates	Available 8-17 daily				
	Day	Availability	Duration		
	Sunday	unavailable 🔻	08 : 00	~ 18	: 00
	Monday	available 🔻	08 00	~ 18	00
	Tuesday	available 🔻	08 : 00	~ 18	: 00
Schedule Table	Wednesday	available 🔻	08 00	~ 18	00
	Thursday	available 🔻	08 : 00	~ 18	: 00
	Friday	available 🔹	08 00	~ 18	00
	Saturday	available 🔻	10 00	~ 17	: 00

Figure 51. Wi-Fi Scheduler Setup Complete

# 13 - Maintenance

# 13.1 - Ping Test

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

Figure 52. Ping Test

PING TEST				System Uppmer datative
Ping Test Parameters				
Target IP / Domain Name				
Ping Packet Size	64 Bytes			
Number of Pings	4			
Start				
	Ping Test Parameters Target IP: Domain Name Ping Packet Size Number of Pings	Ping Test Parameters       Target IP / Domain Name       Ping Packet Size       E4       Bytes       Number of Pings	First Parameters       Target IP / Domain Name       Ping Packet Size       Number of Pings       4	Ping Test Parameters       Target IP / Donain Name       Ping Packet Size       Rember of Pings

### 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.

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

# 13.2 - 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 53. Traceroute Test

araknis	TRACEROUTE TEST	CECUD XERVER: Connected	System Time: 2014-10-12 ha 35 (0)	<ul> <li>System Uptime: 0027130</li> </ul>
STATUS SYSTEM WIRELESS INTERFACE	Traceroute Test Parameters Target IP / Domain Name	 		
SETTINGS SYTEM LAR WIRLLSS SECURITY MIRLLSS SECURITY PING • TRACEROUTE FILE MANAGEMENT	Start Stop			
RESTART LOGOUT O ADVANCED Apply Changes: 0				

### 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.

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



# 13.3 - File Management

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

### Figure 54. File Management

araknis	FILE MANAGEMENT	A CLOUD SERVICE: Conversion 🔯 System Tenne: 2014-10-12 14:36-20. 🔘 System Uprene: 3012-10
STATUS SYSTEM	Configuration File	
WIRELESSINTERFACE SETTINGS	Backup Current Configuration	To PC
SYSTEM LAN	Upload New Configuration File	Choose File No file chosen From PC
WHRELESS SECURITY	Restore Factory Defaults	
PENG	Firmware	
TRACEROUTE	Current Firmware Version	10.8.9.2
+ FILE MANAGEMENT	Date Activated	2014-10-03 02:41:07-00:40
RESTART	Upload New Firmware	Choose File No file chosen Upload
ADVANCED		

Path - Maintenance, File Management



# 13.3.1 - Configuration File

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

### Figure 55. Configuration File

Configuration File		
Backup Current Configuration	To PC	
Upload New Configuration File	Choose File No file chosen	
	From PC	
Restore Factory Defaults	Yes	

Path – Maintenance, File Management, Configuration File

### 13.3.1.1 - 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.

### 13.3.1.2 - 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 56. 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 56. Uploading a New Configuration File

SYSTEM	Configuration File			
WIRELESS INTERFACE	Backup Current Configuration	To PC		
SETTINGS     SYSTEM     LAN	Upload New Configuration File	Choose File backup-AN3020 tar.gz		
WIRELESS	Restore Factory Defaults	Yes		
SECURITY	<u></u>			



# 13.3.1.3 - 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 57. Restore Factory Defaults

araknis	FILE MANAGEMENT	CLOUD SERVER: Connected O System Time: 2014-09-03 20:21:06 O System Uptime: 02:38:02
STATUS SYSTEM	Configuration File	
	Backup Current Configuration	To PC
SYSTEM LAN	Upload New Configuration File	Choose File no file selected From PC
WIRELESS SECURITY	Restore Factory Defaults	Yes
	Firmware	ALERT     The action of acting settings and reset at     settings to factory default.
TRACEROUTE	Current Firmware Version	V0.9.7 CANCEL CONFIRM
FILE MANAGEMENT	Date Activated	2014-09-02 18:00:05 -00:20
RESTART		Choose File, no file selected

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.

### 13.3.1.4 - Hardware Factory Default

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).

- 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.



### 13.3.1.5 - Firmware

Use the Firmware menu to upload new firmware to the AN-100/300.

### Figure 58. Firmware

v0.9.9.2	
2014-10-03 02/41 07 -00/40	
Choose File No file chosen Upload	
	2014-10-03 00 at 07 -00:40 Choose File No file phosen

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.

- 1. Click the **Browse** button to navigate to where the firmware file is saved.
- 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.



# 13.4 - Restart

Reboot the access point.

### Figure 59. Restart

araknis	to the st	CECKID SERVER: Connected	) System Time: 2014-10-12-14-36-26	G System Uptime: 00/21/76
(),	RESTART			
STATUS SYSTEM	Reboot the device			
WIRELESS INTERFACE	Caution: Pressing this button will cause the device to reboot.			
SETTINGS SYSTEM	Reboat the Device			
LAN				
WIRELUSS-				
SECURITY				
MAINTENANCE				
PING TRACEROUTE				
FILE MANAGEMENT				
+ RESTART				
LOGOUT				
O ADVANCED				
Apply Changes: 0				

Path - Maintenance, Restart

- 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.



# 13.5 - 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 60. Logout Alert

<i>araknis</i>	LOGOUT	CLOUD SERVER: Connected	System Time: 2014-10-12 14:35:32	System Uptime: 00.21:12
STATUS SYSTEM WERLESS INTERFACE SETTINGS SYSTEM LAN WIRLESS NECURITY MAINTERANCE PAGE TRACERCOUTE FILE MAIAGEMENT RESTART + LOGOUT ADVANCED ADVANCED	Reboot the device Caution: Prensing this button will cause the device to reboot. Reboot the Device	ALERT or proceeding languad? CANCES CONTRA		

### Path - Maintenance, Logout

- 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.



# 14 - Advanced Menu

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

# 14.1 - 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).



ADVANCED WIRELESS SETTINGS				
Radio Settings				
Transmit Power Unit	• ciām mili			
Data Rate	Auto 🔻			
Transmit Power	Euli 100%-29 dBm			
RTS/CTS Threshold (Range:1-2346)	<b>2</b> 346			
Client Limit				
1.20	2.4GHz	5GHz		
Enable	10 Yes	U Yes		
Max Client No.	9 127	127		
				Savo Cancal
	Transmit Power Unit Data Rate Transmit Power RTS:CTS Threshold (Range:1-2346) Client Limit Enable	Transmit Power Unit     • dammm/       Data Rate     Ø       Transmit Power     Full 100%-29 dBm •       RTSICTS Threshold (Renge:1-2549)     Ø       Zala6     Client Limit       Enable     240kg	Transmit Power Unit     • Gim _ mit/       Data Rate     Auto       Transmit Power     Full 100%-29 dBm       RTSCTS Threshold (Ranger: 12346)     2346	Transmit Power Unit         • 68m mmt           Data Rate         Auto         •           Transmit Power         Full 100%-29 dBm         •           RTSCTS Tirreshold (Range:1-2346)         2346         •           Client Limit         •         56m c           Finable         11 Yes         56m c

Path - Advanced, Wireless Settings



# 14.1.1 - Radio Settings

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

### Figure 62. Radio Settings

Radio Settings		
Transmit Power Unit	• dām mW	
Data Rate	Auto •	
Transmit Power	7 Full 100%-29 dBm •	
RTSICTS Threshold (Range:1-2346)	0 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

- 1. Click Advanced, Wireless Settings.
- 2. Specify the radio settings.
- 3. Click Save, then click Apply Changes to enable the new settings.



# 14.1.2 - Client Limit

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

### Figure 63. Client Limit Settings

	2.40Hz	5GH2	
Enable	Tes .	🙂 Yes	
Max Client No.		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.

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

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



# 14.2 - 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.



WIRELESS MAC FILTER SETTINGS				System Uptime: 002128
MAC Filter Settings				
Enable MAC Filter	Yes			
Filter Mode	e Allow Deny			
MAC Filter List				
No.	MAC Address			Delete
				Add
				Save Cancel
				save
	Enable MAC Filter Filter Mode MAC Filter List	MAC Filter Settings Enable MAC Filter Filter Mode Anow Deny MAC Filter List	WRIELESS MAC FILTER-SISTEMOS MAC Filter Settings Enable MAC Filter Filter Mode  Allow Deny MAC Filter List	MAC Filter Settings Exable MAC Filter Filter Mode Filter List MAC Filter List

Path - Advanced, MAC Filter

# 14.2.1 - MAC Filter Settings

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

### Figure 65. MAC Filter Settings

MAC Filter Settings				
line:				
- Allow Deny				
	Albu 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.*

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



# 14.2.2 - MAC Filter List

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

#### Figure 66. 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.

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



# 14.3 - WPS Settings

WPS (Wi-Fi Protected Setup) allows setup of WPS-equipped Wi-Fi devices...



araknis,		CLOUD SERVER: Connected	System Time: 2015-09-09 12:44:43	System Uptime: 14d 20:312		
STATUS SYSTEM	WPS WPS Settings					
WIRELESS INTERFACE	Status	Enable • Disable				
SETTINGS SYSTEM LAN WIRELESS SECURITY SCHEDULE	Current Configuration	Configured Release Configuration				
	Self-PIN Code	33562162				
	SSID	AN-100-AP-I-N_1				
	Authentication Mode	WPA2/PSK AES				
	Encryption Key	ragetim101				
MAINTENANCE	WPS via Push Button	Start				
PING	WPS via PIN	Start				
TRACEROUTE FILE MANAGEMENT RESTART				Save		

### Path - Advanced, WPS

### Parameters -

- **Status –** Enable or disable WPS. *Default: Disabled*
- Current Configuration Lists whether the WPS feature is configured or unconfigured.
  - **Release Configuration** Press to release the current configuration settings. All devices connected using the configuration will lose Wi-Fi access.
- Self-PIN Code- The Default: Blank.
- SSID The Default: Blank.
- Authentication Mode The Default: Blank.
- Encryption Key The Default: Blank.
- WPS via Push Button The Default: Blank.
- WPS via PIN The Default: Blank.

# 14.3.1 - Configuring WPS Connections

••••



# 14.4 - 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.



araknis	SITE SURVEY			CLOUD SERVER: Converses () System Time: 2014-10-12 14-25-35 () System Uprime: 00.21			
STATUS SYSTEM WIRELESS INTERPACE	Select Interface		• 2.4GHz 5GHz	_	_		
SETTINGS SYSTEM LAN	Scan Nearby Networks		Scan				
	Result						
WIRELESS SECURITY	BSSID +	SSID +	Mode +	Channel +	Signal +	Encryption +	Type •
MAINTENANCE PING TRACEROUTE							

Path - Advanced, Site Survey

### 14.4.1 - Select Interface

The Site Survey Select Interface screen can be used to select the frequency (2.4GHz/5GHz) to be scanned.

Figure 69. Site Survey Settings - Select Interface



Path - Advanced, Site Survey, Select Interface

### 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.

- 1. Click Advanced, Site Survey.
- 2. Specify the site survey settings.
- 3. Click Scan.

## 14.4.2 - Result

The Site Survey Result shows detected 2.4GHz/5GHz wireless networks, their modes, channels, security settings, signal strengths, encryptions, and type based upon the frequency selected for scanning.

Figure 70. Site Survey Settings - shown with scan results



Path - Advanced, Site Survey, Result

### Parameters -

- **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 AN-100/300.
- Encryption Indicates the security mode encryption of a detected device.
- **Type –** Indicates the wireless mode of the detected device.



# 14.5 - Spectrum Analyzer

### Figure 71. Spectrum Analyzer Menu

araknis	SPECTRUM ANALYZER	CLOUD SERVER: Connected OSystem Time: 2015-09-09 12:45:37 OSystem Uptime: 14d 20:32:16
STATUS SYSTEM		
WIRELESS INTERFACE	Select Interface	2.4GHz 5GHz
	Scan Bandwidth	20MHz
SYSTEM	Scan Channel	Channel 1 (2412 MHz)
LAN	RSSI Filter	0 (-40~30)
WIRELESS	Scan Action	Start
SECURITY SCHEDULE		

Path - Advanced, Site Survey, Result

#### Parameters -

- Select Interface 2.4 or 5 Ghz antenna.
- Scan Bandwidth -
- Scan Channel -
- RSSI Filter -
- Scan Action -

## 14.6 - Wireless Traffic Shaping Settings

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

### Figure 72. Wireless Traffic Shaping Settings

araknis		S TRAFFIC SHAPING SETTINGS		CLOUD SERVER: Connector		System Uptime: 00:21
STATUS SYSTEM	Wireless 1	Traffic Shaping				
WIRELESS IN TERMACE.	Enable	SSID	Interface	Download Limit(1-999)Mbps	Upload Limit(1-999)Mbps	
SETTINGS SYSTEM	E Yes	araknis_initial	2.4GHz	100	100	
LAN WIRELESS	- Yes	arakmet_initial	5042	100	100	
SECURITY			and the second			Save Cancel
MAINTENANCE PING						

## 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.

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



## 14.7 - 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 73. SNMP Settings

SNMPv2 Settings								
Status	Enable Disable							
Contact								
Location		1.1						
Port	161							
Community Name (Read Only)	public							
Community Name (Read Write)	private							
Trap Destination	1.000							
Port	162							
IP Address								
Community Name	public							
SNMPv3 Settings								
Status	Enable Disable	·						
Username	admin	(1-31 Characters)						
Authorized Protocol	MD5 •							
Authorized Key	12345678	(8-32 Characters)						
Privacy Protocol	DES •	the second s						
Privacy Key	12345678	(8-32 Characters)						
Engine ID								
					Save Cancel			

Path - Advanced, SNMP



## 14.7.1 - SNMPv2 Settings

This screen allows configuration of SNMPv2 Settings.

### Figure 74. SNMP Settings

SNMPv2 Settings	
Status	Exist     Exist
Contact	
Location	
Port	161
Community Name (Read Only)	public
Community Name (Read Write)	private
Trap Destination	
Port	162
IP Address	
Community Name	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.

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



## 14.7.2 - SNMPv3 Settings

This screen allows configuration of SNMPv3 Settings.

#### Figure 75. SNMP Settings

Status	Erapia Deabe		
Username	admin	(1-31 Characters)	
Authorized Protocol	MD5 ·		
Authorized Key	12345678	(8-32 Characters)	
Privacy Protocol	DES •		
Privacy Key	12345678	(8-32 Crossectors)	
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

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



## 14.8 - 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 76. Spanning Tree Settings

araknis				CECHID SERVER: Connected	System Time: 2014-10-12 14:36:26	G System Uptime: 00.22.78
++ /+++++	SPANNING TREE SETTINGS					
STATUS SYSTEM	Spanning Tree Protocol (STP) Settings					
WIRELESSINTERFACE	Status	Enaple • Dinab	le .			
SETTINGS SYSTEM	Hello Time	2	seconds (1+10)			
LAN	Max Age	20	seconda (6-40)			
WHILLISS SECURITY	Forward Delay	-4	seconds (4-30)			
MAINTENANCE	Priority	32768	(0-66536)			
TRACEROUTE FILE MANAGEMENT RESTART LOGOUT						Save Cancel
O ADVANCED WIRELESS SETTINGS						

## 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
  - Derault. 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.*

- 1. Click Advanced, Spanning Tree.
- 2. Specify the spanning tree settings.
- 3. Click Save.



## 14.9 - 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 77. VLAN Settings

araknis	VLAN SETTINGS		a crow	SERVER: Connected () System Time: 2014-10-12 14 36 37 () System Uptime: 00 22 1
STATUS SYSTEM	VLAN Settings			
WIRELESSINTERFACE	VLAN Isolation	SSID	Interface	VLAN ID
SETTINGS SYSTEM	E Yes	arainis_ințal	2 4GHz	
LAN WIRELESS	_ Yes	araknis_kristai	SCH2	
SECURITY MAINTENANCE PING TRACERCOUTE FILE MANAGEMENT RESTART				Save Cancel

## 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.
- Interface Indicates the 2.4GHz or 5GHz Interface for a given network.
- VLAN ID Enter a value for the VLAN ID. RANGE: 1-4094. Default: Blank

- 1. Click Advanced, VLANS.
- 2. Specify the vlan settings.
- 3. Click Save.



# 14.10 - Rogue AP Detection

#### Figure 78. VLAN Settings

araknis	VLAN SETTINGS		- cto	UD SERVER: Connected (), System Time: 2014-10-12-14-36-37	System Uptime: 00/2217
STATUS SYSTEM	VLAN Settings				
WIRELESSINTERFACE	VLAN isolation	SSID	Interface	YLAN ID	2
B SETTINGS SYSTEM	E Yes	araknis_initai	2 4GHz		
LAN WIRELESS	· Yes	araknig_kntal	\$GH2		2
SECURITY MAINTENANCE PING TRACEROUTE FILE MANAGEMENT RESTART					Save Cancel

Path - Advanced, VLANS

Parameters -

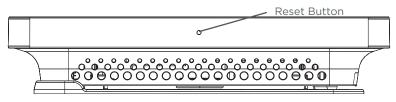
- Select Interface .
- Detect Rogue AP -
- Detect -
- Configure Trust AP List -
- Trust APs -

# 15 - Troubleshooting

## 15.1 - 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 79. Reset Button



- 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

# 16 - Software Defaults

## 16.1 - 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	

# 16.2 - Advanced Menus

ltem	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	

# 17 - Table of Figures

ପି

Figure 1.	Package Contents	
Figure 2.	Residential Access Point Location	
Figure 3.	Small Commercial Access Point Location	
Figure 4.	EIA/TIA 568B Termination Pattern	9
Figure 5.	Network Wiring Diagram	
Figure 6.	Junction Box Mounting	11
Figure 7.	Drywall Mounting	
Figure 8.	Ceiling Tile Mounting	
Figure 9.	Status LED Location	13
Figure 10.	Default SSID	
Figure 11.	EZ Setup Login Screen	
Figure 12.	System Name Access	
Figure 13.	Fing IP Scanner Example	
Figure 14.	Web Interface Layout	21
Figure 15.	Applying Changes	22
Figure 16.	System Status Screen	
Figure 17.	System Information Table	
Figure 18.	Wireless Information	25
Figure 19.	LAN Information	
Figure 20.	System Log	27
Figure 21.	Wireless Interface Status	28
Figure 22.	Radio Status	29
Figure 23.	Utilization of SSID Status	
Figure 24.	Wireless Network Status	30
Figure 25.	Connected Client Status	
Figure 26.	System Settings	
Figure 27.	System Information	33
Figure 28.	Date and Time Settings	
Figure 29.	Time Zone	
Figure 30.	LAN Settings	36
Figure 31.	IP Settings	
Figure 32.	Interface Settings	38
Figure 33.	Wireless Settings (AN-300-AP-I-N interface shown)	39
Figure 34.	Radio Settings	
Figure 35.	Utilization of SSID Status	41
Figure 36.	Wireless Networks	10
Figure 37.	Wireless Security - WPA-PSK and WPA2-PSK Modes	
Figure 38.	Wireless Security - WPA-PSK and WPA2-PSK Modes	44
Figure 39.	Guest Network	



Figure 40.	Security Settings	
Figure 41.	User Accounts	
Figure 42.	Access Control	
Figure 43.	Email Alert Setup Example	
Figure 44.	Common Email Client Ports	
Figure 45.	Device Discovery	
Figure 46.	Schedule Settings Menu	
Figure 47.	Auto Reboot Settings	
Figure 48.	Auto Reboot Settings	
Figure 49.	Wi-Fi Scheduler	
Figure 50.	Wi-Fi Scheduler Menu	
Figure 51.	Wi-Fi Scheduler Setup Complete	
Figure 52.	Ping Test	
Figure 53.	Traceroute Test	
Figure 54.	File Management	60
Figure 55.	Configuration File	
Figure 56.	Uploading a New Configuration File	
Figure 57.	Restore Factory Defaults	
Figure 58.	Firmware	
Figure 59.	Restart	C 4
Figure 60.	Logout Alert	
Figure 61.	Advanced Wireless Settings	
Figure 62.	Radio Settings	
Figure 63.	Client Limit Settings	
Figure 64.	Wireless MAC Filter Settings	_69
Figure 65.	MAC Filter Settings	_69
Figure 66.	MAC Filter List	.70
Figure 67.	WPS Settings Menu	
Figure 68.	Site Survey Settings	
Figure 69.	Site Survey Settings - Select Interface	
Figure 70.	Site Survey Settings - shown with scan results	
Figure 71.	Spectrum Analyzer Menu	
Figure 72.	Wireless Traffic Shaping Settings	
Figure 73.	SNMP Settings	
Figure 74.	SNMP Settings	
Figure 75.	SNMP Settings	
Figure 76.	Spanning Tree Settings	
Figure 77.	VLAN Settings	
Figure 78.	VLAN Settings	
Figure 79.	Reset Button	

# 18 - Specifications

# 100/300 Series

Description	AN-100-AP-I-N	AN-300-AP-I-N
	Interfaces	
RJ45 10/100/1000Base-T	· · · · · · · · · · · · · · · · · · ·	1
PoE 802.3at/af compliant	Ye	es
Wireless Interface	802.11 b/g/n	802.11 a/b/g/n
Embedded Antennas	Ye	es
	Performance	
Antenna Type	Omni-di	rectional
Transmit Power	See MC	CS table
Receiver Sensitivity	See MC	CS table
802.11n	2x2:2	МІМО
PHY Data Rate	Up to 300 Mbps Up to 300 Mbps in bot frequency bands	
Operating Frequencies	2.4GHz	2.4GHz & 5GHz
Channel Bonding	Yes (20MHz	and 40MHz)
Memory	64MB	128MB
Flash Memory	16MB	16MB
	Wireless Features	
Auto Channel Selection	Ye	es
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	Ye	es
	L2 features	
VLANs	Yes - 802.1Q	
QoS	Yes - WME 802.11e	
RJ45 Auto-sensing	Yes	
RJ45 Auto-negotiation	Yes	
Spanning Tree Protocol	Yes, 8	302.1d

ପି

Description	AN-100-AP-I-N	AN-300-AP-I-N
	Management	
Web Management	Y	es
Telnet	Y	es
SNMP v1, v2c, v3	Y	es
DHCP client	Y	es
System Log	Y	es
Bonjour	Y	es
Araknis EZ Access	Y	es
UPnP	Y	es
Remote Config File Download/Upload	Y	es
OvrC Cloud Services	Y	es
Wi-Fi Scheduler	Y	es
Site Survey	Yes	
LED Control	Yes	
Auto Reboot	Y	es
	Environmental & Physical	
Dimensions (W-H-D)	6.9 x 6	5.9 x 1.3
External Power Supply	12V 1A DC	12V 2A DC
Temperature Range	Operating: 32º to 122ºF( 0 to 50ºC) Storage: -4Fº to 140ºF(-20ºC to 60ºC)	
Humidity	Operating: 90% or less Storage: 90% or less	
Certifications	CE, FCC,	IC, Wi-Fi®



## MCS Table (RF Performance)

Channel Bonding	Data Range	Transmit Power (combined, dBm)	Receive Sensitivity (combined, dBm)	
	AN-100-AP-I-N			
802.11b @ 2.4 GHz	1 Mbps	29	<u>≤</u> -93	
602.11b @ 2.4 GHz	11 Mbps	29	<u>&lt;</u> -90	
802.11g @ 2.4 GHz	6 Mbps	28	<u>≤</u> -89	
	54 Mbps	25	<u>&lt;</u> -71	
802.11n HT20 @ 2.4 GHz	MCS 0/8	27	<u>≤</u> -87	
802.111 H120 @ 2.4 GH2	MCS 7/15	24	<u>≤</u> -69	
	MCS 0/8	27	<u>≤</u> -87	
802.11n HT40 @ 2.4GHz	MCS 7/15	24	<u>≤</u> -69	
	A٨	I-300-AP-I-N		
	6 Mbps	26	<u>≤</u> 90	
802.11a @ 5GHz	54 Mbps	23	<u>≤</u> -72	
20211h @ 2.4 CH-	1 Mbps	29	<u>≤</u> -99	
802.11b @ 2.4 GHz	11 Mbps	29	<u>≤</u> -93	
802.11g @ 2.4 GHz	6 Mbps	29	<u>≤</u> -96	
802.11g @ 2.4 GHz	54 Mbps	23	<u>≤</u> -82	
802.11n HT20 @ 2.4 GHz	MCS 0/8	29	<u>≤</u> -97	
802.111 H120 @ 2.4 GH2	MCS 7/15	23	<u>≤</u> -78	
	MCS 0/8	29	<u>≤</u> -86	
802.11n HT40 @ 2.4GHz	MCS 7/15	23	<u>&lt;</u> -69	
	MCS 0/8	26	<u>&lt;</u> -89	
802.11n HT20 @ 5GHz	MCS 7/15	23	<u>≤</u> -70	
	MCS 0/8	26	<u>≤</u> -87	
802.11n HT40 @ 5GHz	MCS 7/15	23	<u>≤</u> -68	



# 500/700 Series

Description	AN-500-AP-I-AC	AN-700-AP-I-AC
	Interfaces	
RJ45 10/100/1000Base-T	· · · · · ·	1
PoE 802.3at/af compliant	Ye	es
Wireless Interface	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac
Embedded Antennas	Ye	es
	Performance	
Antenna Type	Omni-di	rectional
Transmit Power	See MC	CS table
Receiver Sensitivity	See MC	S table
802.11n	2x2:2 MIMO	3x3:3 MIMO
PHY Data Rate	Up to 300Mbps @ 2.4GHz Up to 867Mbps @ 5GHz	Up to 450Mbps @ 2.4GHz Up to 1300Mbps @ 5GHz
Operating Frequencies	2.4GHz	& 5GHz
Channel Bonding	Yes (20MHz, 40N	1Hz, and 80MHz)
Max TX Power	28dBm @ 2.4GHz 26dBm @ 5GHz	
Memory	64MB	128MB
Flash Memory	16MB	16MB
	Wireless Features	
Auto Channel Selection	Ye	es
Operation Modes	Access Point, Repeater	
Multiple SSIDs	Yes -up to 8 per radio	
Wireless Security	WPA2-PSK (AES + T	KIP), WPA-Enterprise
MAC Address Filtering	Yes	
Hide SSID	Yes	
Guest Network	Yes	
	L2 features	20210
VLANs	Yes - 8	
QoS	Yes - WME 802.11e	
RJ45 Auto-sensing	Yes	
RJ45 Auto-negotiation	Yes	
Spanning Tree Protocol	Yes, 802.1d	

ପି

Description	AN-500-AP-I-AC	AN-700-AP-I-AC
	Management	
Web Management	Yes	5
Telnet	Yes	5
SNMP v1, v2c, v3	Yes	5
DHCP client	Yes	5
System Log	Yes	5
Bonjour	Yes	6
Araknis EZ Access	Yes	5
UPnP	Yes	5
Remote Config File Download/Upload	Yes	5
OvrC Cloud Services	Yes	
Wi-Fi Scheduler	Yes	
Site Survey	Yes	
LED Control	Yes	
Auto Reboot	Yes	
	Environmental & Physical	
Dimensions (W-H-D)	6.9" x 6.9" x 1.3"	6.9" x 6.9" x 1.6"
External Power Supply	12V 2A	DC
Temperature Range	Operating: 32º to 12 Storage: -4Fº to 1409	
Humidity	Operating: 90% or less Storage: 90% or less	
Certifications	CE, FCC, IC	C, Wi-Fi®



## MCS Table (RF Performance)

Channel Bonding	Data Range	Transmit Power (combined, dBm)	Receive Sensitivity (combined, dBm)	
	AN-500-AP-I-AC			
802.11b @ 2.4 GHz	1 Mbps	29	<u>&lt;</u> -93	
002.110 @ 2.4 0112	11 Mbps	29	<u>&lt;</u> -90	
802.11g @ 2.4 GHz	6 Mbps	28	<u>≤</u> -89	
002.11g @ 2.4 0112	54 Mbps	25	<u>≤</u> -71	
802.11n HT20 @ 2.4 GHz	MCS 0/8	27	<u>≤</u> -87	
802.111 H120 @ 2.4 GH2	MCS 7/15	24	<u>≤</u> -69	
	MCS 0/8	27	<u>≤</u> -87	
802.11n HT40 @ 2.4GHz	MCS 7/15	24	<u>≤</u> -69	
	AN	-700-AP-I-AC		
	6 Mbps	26	<u>≤</u> 90	
802.11a @ 5GHz	54 Mbps	23	<u>≤</u> -72	
20211h @ 2.4 CU-	1 Mbps	29	<u>≤</u> -99	
802.11b @ 2.4 GHz	11 Mbps	29	<u>≤</u> -93	
20211 <del>2</del> @ 2.4 CU	6 Mbps	29	<u>≤</u> -96	
802.11g @ 2.4 GHz	54 Mbps	23	<u>≤</u> -82	
	MCS 0/8	29	<u>≤</u> -97	
802.11n HT20 @ 2.4 GHz	MCS 7/15	23	<u>≤</u> -78	
	MCS 0/8	29	<u>≤</u> -86	
802.11n HT40 @ 2.4GHz	MCS 7/15	23	<u>≤</u> -69	
	MCS 0/8	26	<u>≤</u> -89	
802.11n HT20 @ 5GHz	MCS 7/15	23	<u>≤</u> -70	
	MCS 0/8	26	<u>≤</u> -87	
802.11n HT40 @ 5GHz	MCS 7/15	23	<u>≤</u> -68	

^^TBD^^

# **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

# €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.

# 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.

# €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 $\Delta$ ΗΛΩΝΕΙ ΟΤΙ wireless access point ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ $\Delta$ ΙΑΤΑΞΕΙΣ 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.

# AN-500/700-AP-I-AC 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 22cm 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 22cm 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

# CE

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]	ME THN ΠΑΡΟΥΣΑ Araknis Networks $\Delta$ ΗΛΩΝΕΙ ΟΤΙ wireless access point ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ $\Delta$ ΙΑΤΑΞΕΙΣ 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<sup>®</sup> 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



© 2016 Araknis Networks\* 160225-1513