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™ products. It provides all known information regarding the installation, setup, use, and maintenance of the product. The symbols below are used to identify important information:

Pro Tip – Pro tips are included in sections of the manual to add information that provides extra value, utility, or ease-of-use for the installer or end user of the product. Pro tips may also link to extra information that will provide a better understanding of application, technology or use of the product or feature in question. These items are not required, but have been added for your convenience.

Note – Notes emphasize information important to the installation, setup, or use of the product that is not essential to follow for safety of the equipment or user. Notes may be located before or in the midst of the section to which they apply, depending on the type of information. These items usually contain essential information, like the size or dimension of a separate part required, or a critical step in the process, that, if missed, would cause the installer or end user extra work to overcome.

Caution – The caution symbol is used to indicate information vital to the safety of the equipment in use with the product, or the product itself. Cautions are always provided before the information they relate to. Not following a caution will almost always result in permanent damage to equipment that is not covered by warranty.

Warning – Warnings indicate information vital to the safety of the installer or end user of the product. Warnings are always provided before the information they relate to. Not following a warning may result in permanent damage to equipment and serious injury or death of the installer or end user.
# Table of Contents

1 - About this Manual ................................................................. 2

2 - Welcome to Araknis Networks™ .............................................. 6
   2.1 - Features ........................................................................... 6
   2.2 - Package Contents ............................................................ 6

3 - Hardware Overview .............................................................. 7
   3.1 - Top .................................................................................. 7
   3.2 - Bottom ............................................................................ 7
   3.3 - Side ................................................................................ 7

4 - Mounting Location - General Guidelines ................................. 8

5 - Wiring Requirements ............................................................. 9
   5.1 - Network Cable Requirements ........................................... 9
   5.2 - PoE Requirements ............................................................ 9
   5.3 - Power Requirements for Non-PoE Application .................. 9
   5.4 - Wiring Instructions .......................................................... 9
         Wiring Diagram ............................................................... 10

6 - Mounting the Access Point .................................................... 11
   6.1 - Table Top/Shelf .............................................................. 11
   6.2 - Junction Box Mounting Instructions .................................. 11
   6.3 - Wall or Ceiling Drywall Mounting Instructions ................. 12
   6.4 - Ceiling Tile Mounting Instructions .................................. 12

7 - Power-On and Operation ......................................................... 13
   7.1 - Status LED Operation ...................................................... 13

8 - Introduction to Network Setup ................................................ 14

9 - Accessing the Web Interface .................................................. 14
   9.1 - EZ Access Method (Default) .............................................. 15
   9.2 - Configured System Name Access ..................................... 16
   9.3 - DHCP/Static IP Address Method ...................................... 17
         Finding the IP Address of the Access Point ......................... 17
         Default IP Address Access .................................................. 18

10 - Web Interface Overview ........................................................ 21
    10.1 - Applying Changes in the Web Interface ......................... 22

11 - System Status ....................................................................... 23
    11.1 - System Information ..................................................... 23
    11.2 - Wireless Information ................................................... 24
    11.3 - LAN Information ........................................................ 25
    11.4 - System Log ................................................................ 25

12 - Wireless interface Status ...................................................... 26
    12.1 - Radio Status ............................................................... 26
    12.2 - Utilization of SSID ....................................................... 27
         Wireless Network ............................................................ 27
## 22 - Logout

## 23 - Advanced Menu

### 23.1 - Advanced Wireless Settings
- Radio Settings
- Client Limit

### 23.2 - Wireless MAC Filter Settings
- MAC Filter Settings
- MAC Filter List

### 23.3 - WPS Settings
- Connecting a Device Using WPS via Push Button
- Connecting a Device Using WPS via PIN

### 23.4 - Site Survey

### 23.5 - Spectrum Analyzer
- Configuring Scan Settings
- Running a Scan
- Understanding Spectrum Analyzer Results

### 23.6 - Wireless Traffic Shaping Settings

### 23.7 - SNMP Settings
- SNMPv2 Settings
- SNMPv3 Settings

### 23.8 - Spanning Tree Settings

### 23.9 - VLAN Settings

## 24 - Appendix

### 24.1 - Configuring Guest Networks with Fast Roaming

## 25 - Troubleshooting

### 25.1 - Hardware Reset Procedure

## 26 - Table of Figures

## 27 - Specifications

## 28 - CE Warning

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

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

## 31 - 2-Year Limited Warranty

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

2.1 - Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>AN-100-AP-I-N</th>
<th>AN-300-AP-I-N</th>
<th>AN-500-AP-I-N</th>
<th>AN-700-AP-I-N</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.4GHz Radio</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5GHz Radio</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Concurrent Dual-band</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Gigabit Ethernet</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PoE Standard</td>
<td>802.3af</td>
<td>802.3af/at</td>
<td>802.3af/at</td>
<td>802.3af/at</td>
</tr>
<tr>
<td>WiFi Standard</td>
<td>802.11 b/g/n</td>
<td>802.11 a/b/g/n</td>
<td>802.11 a/b/g/n/ac</td>
<td>802.11 a/b/g/n/ac</td>
</tr>
<tr>
<td>OvrC Enabled</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Antennas</td>
<td>2x2:2</td>
<td>2x2:2</td>
<td>2x2:2</td>
<td>3x3:3</td>
</tr>
</tbody>
</table>

2.2 - Package Contents
*Not Pictured: Wall Mount Template

Figure 1. Package Contents

- WAP
- Mounting Bracket
- Tile Ceiling Backing Plate
- Quick Start Guide
- LAN Cable
- Tile Ceiling Mounting Hardware
- Drywall Mounting Hardware
3 - Hardware Overview
Use these images to familiarize yourself with the physical layout of your access point.

3.1 - Top

3.2 - Bottom

3.3 - Side
4 - Mounting Location - General Guidelines

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

---

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

---

Figure 2. Residential Access Point Location

Figure 3. Small Commercial Access Point Location
5 - Wiring Requirements

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

5.1 - Network Cable Requirements

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

**Figure 4. EIA/TIA 568B Termination Pattern**

<table>
<thead>
<tr>
<th>Pin 1</th>
<th>White/Orange</th>
<th>Pin 5</th>
<th>White/Blue</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pin 2</td>
<td>Orange</td>
<td>Pin 6</td>
<td>Green</td>
</tr>
<tr>
<td>Pin 3</td>
<td>White/Green</td>
<td>Pin 7</td>
<td>White/Brown</td>
</tr>
<tr>
<td>Pin 4</td>
<td>Blue</td>
<td>Pin 8</td>
<td>Brown</td>
</tr>
</tbody>
</table>

(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 (100 Series: 0.3A; 300/500/700 Series: 0.6A)
- **DC Input** – 12V DC 1A (100 Series); 2A (300/500/700 Series).

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 within reach of the mounting location.
5.4.1 - Wiring Diagram

Figure 5. Network Wiring Diagram
6 - Mounting the Access Point

6.1 - Table Top/Shelf
The access point comes with rubber feet installed for placement on flat surfaces. The mounting bracket is not required for this application.

6.2 - Junction Box Mounting
The mounting bracket is compatible with most common junction box and plaster ring dimensions, including common ceiling box sizes:

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

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

Figure 6. Junction Box Mounting

Figure 6A  Figure 6B  Figure 6C
6.3 - Wall or Ceiling Drywall Mounting Instructions
1. Place the bracket over the desired mounting location with the arrow on the bracket pointing up for wall mounting. See Figure 7A, below.

2. Mark the “C” or “D” slots on the mounting surface, then remove the bracket and thread one of the included drywall anchors into the center of each mark using a Phillips screwdriver.

3. Level or align the bracket with nearby objects and fasten it to the anchors using the two included anchor screws. Tighten the screws enough to secure the bracket. Avoid over-tightening and warping the bracket.

4. Connect the wiring to the access point and push any extra wiring back into the opening. See Figure 7B, below.

5. Snap the access point onto the bracket. See Figure 7C, below.

Figure 7. Drywall Mounting

6.4 - Ceiling Tile Mounting Instructions
1. Place the bracket over the desired mounting location and align it with nearby objects for uniformity.

2. Mark the “C” or “D” slots on the ceiling tile (and the center hole if needed for wiring).

3. Cut the opening with a keyhole saw. Use a drill to make clean holes for the mounting screws.

4. Place the ceiling backing plate and nuts on top of the tile as shown and fasten the mounting bracket to the tile using the included screws.

5. Connect the wiring to the access point and push any extra wiring back into the opening.

6. Snap the access point onto the bracket.

Figure 8. Ceiling Tile Mounting
7 - Power-On and Operation

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

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

7.1 - Status LED Operation

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

Figure 9. Status LED Location

- Blue LED:
  - Blinking: Device is not working correctly. Refer to the Troubleshooting section.
  - Solid: Device is operating correctly.
8 - Introduction to Network Setup
The access point setup menu is used to make network configuration changes. This section explains how to access and use the menu.

**Warning** - All Araknis access points will transmit the same SSID, "araknis_initial" by default. If multiple access points are being installed in the same network, power on and complete network setup for one device at a time to avoid confusion about which access point you are connected to. Always change the SSID during initial setup.

9 - Accessing the Web Interface
There are several ways to access the web interface of the access point:

- **EZ Access Method** – Default method used for initial setup. Connect your computer to the access point using Wi-Fi.

- **Configured System Name Access** – Enter the device name instead of the IP address to access the web interface.

- **DHCP/Static IP Address Method** – Can be used any time. Connect your computer to the network wired or wirelessly and enter the IP address issued to the access point by the network, or the default IP address, (192.168.20.253).

- **OvrC Method** – OvrC gives you remote device management, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required. To add this device to your OvrC account:
  1. Connect the WAP to the Internet
  2. Log Into OvrC (www.ovrc.com)
  3. Add the Device (MAC address and Service Tag numbers needed for authentication)
9.1 - EZ Access Method (Default)
When the WAP is powered on for the first time, it transmits the default, unsecured SSID, “araknis_initial”. Connect and access the web interface without any cable connections or network card setting changes.

Note – Make sure the WAP is connected to a network with a functioning DHCP server. After the WAP is powered on, startup usually takes two to four minutes to complete. Wait for the Status LED to turn solid before beginning setup.

Figure 10. Default SSID

On your wireless network-enabled computer:
1. Disconnect any network cables from your computer.
2. Make sure the wireless network card is set to obtain an IP address automatically (DHCP mode).
3. Connect your computer to the wireless network named “araknis_initial”.
4. Open a web browser and enter the configuration address for your device:
   - AN-100-AP-I-N enter: http://config.an-100-ap-i-n.wap/
   - AN-300-AP-I-N enter: http://config.an-300-ap-i-n.wap/
   - AN-500-AP-I-AC enter: http://config.an-500-ap-i-ac.wap/
   - AN-700-AP-I-AC enter: http://config.an-700-ap-i-ac.wap/
5. Enter the default login credentials:
   - Username: araknis
   - Password: araknis

Figure 11. EZ Setup Login Screen
9.2 - Configured System Name Access

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

1. See section “13 - System Settings” on page 29 to set the system name.

2. Apply the settings. After configuration, the WAP web interface may be accessed using the system name.

3. Open a web browser and enter the configuration address for your WAP in this format (Example System Name = smith100):
   - Enter into address bar: http://config.smith100.wap/

4. Enter the login credentials. (Default: araknis/araknis)

Figure 12. System Name Access
9.3 - DHCP/Static IP Address Method

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

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

9.3.1 - Finding the IP Address of the Access Point

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

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

   Figure 13. Fing IP Scanner Example

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

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

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

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

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

4. In the left bar, left-click **Change adapter settings**.
5. Right-click the icon for the wired network connection and left-click **Properties**.

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

7. In the General tab, left-click **Use the following IP address**: and enter the IP address and subnet mask.
   - IP Address: **192.168.20.2**
   - Subnet Mask: **255.255.255.0**
8. Left-click OK to close **Internet Protocol Version 4 (TCP/IPv4) Properties**, then left-click OK to close **Wireless Network Connection Properties**.

   - Username: **araknis**
   - Password: **araknis**
10 - Web Interface Overview

Figure 14. Web Interface Layout

- **A - Main Navigation Menu**
  Use the submenus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the access point. Click **Apply Changes** to review and apply changes made in menus.

- **B - Main Window**
  The main window displays the currently selected submenu.

- **C - Top Bar**
  The top bar displays the current connection status to the OvrC server, the current internally-set system time, and the current system uptime in DAYS:HOURS:MINUTES.
10.1 - Applying Changes in the Web Interface

1. After making changes to settings on a menu page, left-click the **Save** button on the menu to hold the new settings in the Apply Changes field.

2. After all desired changes have been made, left-click **Apply Changes** to review the new settings.

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

Figure 15. Applying Changes
11 - System Status

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

Note – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

11.1 - System Information
Displays current information about the WAP’s system settings.

Figure 16. System Information Table

<table>
<thead>
<tr>
<th>System Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>an300</td>
</tr>
<tr>
<td>Service Tag</td>
<td>ST100616510841A</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>1.1.04</td>
</tr>
<tr>
<td>Management VLAN ID</td>
<td>Untagged</td>
</tr>
</tbody>
</table>

Path – Status, System, System Information

Parameters –

- **System Name** – Name assigned to the system. Used for configured name access.
- **Service Tag** – Internal tracking number used to track every product sold by Araknis Networks.
- **Firmware Version** – Current version of firmware running on the access point.
- **Management VLAN ID** – VLAN that must be used to access the web interface.
11.2 - Wireless Information
Displays current information about the wireless radio channel(s) in use.

Figure 17. Wireless Information

<table>
<thead>
<tr>
<th>Wireless Information</th>
<th>2.4GHz</th>
<th>5GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Networks</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Number of Connected Clients</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Operation Mode</td>
<td>Access Point</td>
<td>Access Point</td>
</tr>
<tr>
<td>TX</td>
<td>0 Bytes</td>
<td>0 Bytes</td>
</tr>
<tr>
<td>RX</td>
<td>0 Bytes</td>
<td>0 Bytes</td>
</tr>
</tbody>
</table>

Path – Status, System, Wireless Information

Parameters –

Note – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

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

Path – Status, System, LAN Information

Parameters –
- **Speed** – Indicates negotiated LAN speed between the access point and the wired network.
- **Duplex** – Indicates the negotiated duplex setting between the access point and the wired network.
- **MAC address** – The MAC address assigned to the access point network connection. This address may also be found on the access point’s service tag.
- **TX** – Amount of data, in bytes, transmitted over the wired network connection.
- **RX** – Amount of data, in bytes, received from the wired network connection.
- **IP Address** – Access point IP address issued by the network router.
- **Subnet Mask** – Access point subnet mask.
- **Default Gateway** – Network router IP address.
- **Primary DNS** – Indicates the primary DNS for the device.
- **Secondary DNS** – Indicates the secondary DNS for the device.

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

Path – Status, System, System Log

Parameters –
- **Save Log** – Click to view the log as a text file or save the log for future reference.
- **Clear Log** – Click to permanently delete to contents of the System Log.
12 - Wireless interface Status
Provides a detailed look at wireless settings and performance for radio status and settings, wireless network configuration and connected client status.

12.1 - Radio Status
Provides a detailed look at radio settings and performance.

Figure 19. Radio Status

Path – Status, Wireless interface, Radio Status

Parameters –

- **Interface Status** – Indicates whether the wireless antenna is enabled or disabled.
- **Operation Mode** – Indicates whether the antenna is operating in Access Point or Repeater mode.
- **Wireless Mode** – Indicates whether the antenna is operating in 802.11b/g/n, 802.11a/n, or 802.11ac/n mode.
- **Channel Bandwidth** – Indicates whether the channel is operating at 20MHz, 40MHz, or 80 Mhz. (80 MHz 500/700 only)
- **Channel Selection** – Indicates the current channel setting.
- **Operating Channel** – Indicates the current operating channel.
- **Channel Frequency** – Indicates the frequency of the operating channel.
- **TX** – Amount of data transmitted in bytes.
- **RX** – Amount of data received in bytes.

Note – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.
12.2 - Utilization of SSID
Details the use and availability of SSID’s configured in the WAP.

Figure 20. Utilization of SSID Status

<table>
<thead>
<tr>
<th>Utilization of SSID</th>
<th>2.4GHz</th>
<th>5GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID's Used</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SSID's Available</td>
<td>7</td>
<td>5</td>
</tr>
</tbody>
</table>

Path – Status, Wireless interface, Wireless Network

Parameters –

Note - The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series 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 available for use.

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

Figure 21. Wireless Network Status

<table>
<thead>
<tr>
<th>Wireless Network (SSID)</th>
<th>Enabled</th>
<th>Interface</th>
<th>Security</th>
<th>VLAN ID</th>
<th>MAC Address</th>
<th>Broadcast SSID</th>
<th>Client Isolation</th>
</tr>
</thead>
</table>

Path – Status, Wireless interface, Wireless Network

Parameters –

Note - The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

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

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

Figure 22. Connected Client Status

<table>
<thead>
<tr>
<th>Status</th>
<th>Wireless Network (SSID)</th>
<th>Device Name</th>
<th>MAC Address</th>
<th>TX (KBytes)</th>
<th>RX (KBytes)</th>
<th>RSSI (dBm)</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>android-15586e2764ee0010</td>
<td>58:5F:34:F0:67:08</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Path – Status, Wireless interface, Connected Clients

Parameters –

• **Status** – Indicates whether the client is currently connected. Green indicates that the client is connected to the SSID.

• **Wireless Network (SSID)** – Indicates the SSID being used by a connected wireless client.

• **Interface** – Indicates the channel frequency of a connected wireless client.

• **MAC address** – Indicates the MAC address of a connected wireless client.

• **TX (KBytes)** – Amount of data, in kilobytes, transmitted to a connected wireless client.

• **RX (KBytes)** – Amount of data, in kilobytes, received from a connected wireless client.

• **RSSI (dBm)** – Indicates the wireless signal strength between the access point and the connected client. The color of the table field indicates signal quality: green=strong, yellow=medium, and red=weak.

• **Release** – Click the Yes button to drop a client from the network.

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

13.1 - System Information

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

![System Information Screen](image)

**Figure 23. System Information**

**Path** – Settings, System, System Information

**Parameters** –

- **System Name** – Enter a meaningful name such as *SmithHome* or *SmithBasement*. Limited to 32 characters, including spaces.

- **Admin Username** – Enter a username for logging into the access point. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.
  
  *Default: araknis*

- **Admin Current Password** – Enter the current login password when changing the password.
  
  *Default: araknis*

- **Admin New Password** – Enter a new login password. Use letters, numbers, or punctuation. Limited to 32 characters, including spaces.

- **Confirm Admin New Password** – Confirm a new login password (enter same password as above).

- **System LED** – Turn the Status LED ON or OFF.
  
  *Default: ON*

- **Management VLAN** – The VLAN ID from where the WAP web interface must be accessed.
  
  *Default: Untagged*

  **Caution** – Changing the management VLAN may cause a loss of access to the web interface. Move the computer to the new management VLAN or reset the WAP to regain connectivity (see section “20.1.4 - Hardware Factory Default” on page 58).

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

**Configuration Instructions** –

1. Click **Settings, System**.

2. Specify the system information settings.

3. Click **Save**, then **Apply Changes** to enable the new settings.
13.2 - Date and Time Settings
Allows configuration of the ‘real world’ time setting and how it is kept set correctly for all access point functions.

Figure 24. Date and Time Settings

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.

Configuration Instructions –
1. Click **Settings, System**.
2. Specify the date and time settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
13.3 - Time Zone
Allows configuration of time zone settings.

Figure 25. Time Zone

Path – Settings, System, Time Zone

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

Configuration Instructions –
1. Click **Settings, System**.
2. Specify the time zone and DST settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
14 - LAN Settings

14.1 - IP Settings

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

Figure 26. IP Settings

<table>
<thead>
<tr>
<th>IP Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.20.253</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>192.168.20.253</td>
</tr>
<tr>
<td>Primary DNS</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>Secondary DNS</td>
<td>8.8.8.8</td>
</tr>
<tr>
<td>DHCP</td>
<td></td>
</tr>
</tbody>
</table>

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

Path – Settings, LAN, IP Settings

Parameters –

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

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

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

• Subnet Mask – Enter the subnet mask for the device.
  Default: 255.255.255.0

• Default Gateway – With DHCP disabled, enter the default gateway for the access point (network router IP address).

• Primary DNS – With DHCP disabled, enter the primary DNS for the device. This is typically the network router IP address.

• Secondary DNS – With DHCP disabled, enter the secondary DNS for the device. This is typically be the network router IP address.

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

• DHCP – Allows the access point to receive a DHCP IP address from the network router if DHCP is enabled. Un-check the box to configure a static IP address (recommended).
  Default: Enabled
Configuration Instructions –
1. Click Settings, LAN.
2. Specify the IP settings.
3. Click Save, then Apply Changes to enable the new settings.

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

Figure 27. Interface Settings

Path – Settings, LAN, Interface Settings

Parameters –
- **Speed** – Select LAN speed from Auto, 1Gbps (300/500/700 Series only), 100Mbps, 10Mbps, Disable (turns the LAN Port OFF)
  
  Default: Auto

- **Duplex** – (10/100Mbps modes only) Select the duplex setting between the access point and the network router from Half or Full.
  
  Default: Full

Configuration Instructions –
1. Click Settings, LAN.
2. Specify the interface settings.
3. Click Save, then Apply Changes to enable the new settings.
15 - Wireless Settings

15.1 - Radio Settings

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

Path – Settings, Wireless, Radio Settings

Parameters –

Note – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

- Enable Interface – Enable or disable the radio interface.
  Default: Yes.

- Operation Mode – Set the radio to Access Point or Repeater mode. See “15.7 - Configuring the WAP as a Repeater” on page 44 for Repeater mode setup instructions.
  Default: Access Point

- Wireless Mode – Select the wireless mode for the radio.
  Default: 2.4GHz - 802.11b/g/n; 5GHz - 802.11a/n (300), 802.11ac/n (500/700).

- Operating Channel – Select the desired Wi-Fi channel. Use a different channel than other WAPs on the network. On the 2.4GHz radio, there are only three non-overlapping channels: 1, 6 and 11. Select a channel as far away from close-numbered channels as possible.
  Default: Auto.

  Pro Tip – In a multi-WAP environment, put adjacent WAPs on channels as far apart as possible. A spectrum analyzer tool (such as Metageek’s Chanalyzer Pro) is recommended for providing insight into the network setup.

- Channel Bandwidth – Select the desired channel bandwidth. Smaller values allow greater range and larger values provide greater throughput. The combination setting allows the WAP to decide.
  Default: 2.4GHz - 20MHz; 5GHz - 40MHz (300), 80Mhz (500/700)

- Extension Channel – Specify whether the channel extends above or below the normal 20MHz range. Only applies when the Channel Bandwidth is set higher than 20MHz.
  Default: 2.4GHz - Upper Channel; 5GHz - Lower Channel.
15.2 - Utilization of SSID
Details the use and availability of SSID’s configured in the WAP.

Figure 29. Utilization of SSID Status

<table>
<thead>
<tr>
<th>Utilization of SSID</th>
<th>2.4GHz</th>
<th>5GHz</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID’s Used</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>SSID’s Available</td>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Path – Settings, Wireless, Utilization of SSID

Parameters –

- **Note** – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

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

15.3 - Global Wireless Settings
Configure Band Steering and Fast Roaming.

Figure 30. Global Wireless Settings

Path – Settings, Wireless, Global Wireless Settings

Parameters –

- **Band Steering** – (300/500/700 Series only) This feature pushes clients to the 5 GHz radio if a client is compatible. We recommend enabling this feature for the best performance. Click the button to toggle between on and off.

- **Fast Roaming** – This feature allows clients to seamlessly switch between multiple WAPs transmitting the same SSID based on which WAP will provide the best signal at any time. See section “15.3.1.1 - Fast Roaming Setup Instructions” on page 37 for setup requirements and instructions.
15.3.1 - Fast Roaming Mode
This powerful feature, known in Araknis products as Fast Roaming, is essential for building reliable WiFi networks with multiple access points. After a client joins a WiFi network, they don’t always stay close to the WAP they originally connected to.

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

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

Installation Notes
• WEP security mode does NOT work with Fast Roaming. Configure SSIDs using other encryption modes.
• How do I configure the locations of WAPs for the best performance?
Use a site analyzer tool to determine ideal WAP locations. For the best performance, use more WAPs closer together and reduce the transmit power some to avoid interference (Advanced Wireless Settings).
• Does it matter what operating channel is used?
If you aren’t using Auto Operating Channel selection, use a different wireless radio channel in each WAP to lower the amount of interference each device encounters.
• Do fast roaming and band steering work together?
Yes, configure each one based on individual needs. Remember, some devices may not be compatible with these features.
• How do I set up Guest Networks with Fast Roaming enabled?
The guest network feature is not ideal for use with Fast Roaming since each WAP creates a new DHCP server for clients connected to that SSID. Instead, create a separate VLAN and assign SSIDs for guest use. See section “24.1 - Configuring Guest Networks with Fast Roaming” on page 79 for setup instructions.
• Is this a proprietary technology for Araknis Networks?
No. Fast Roaming utilizes the standard IEEE 802.11r and 802.11k to negotiate handoff with the client. Only clients that support 802.11r/k are able to perform best in this environment.
• Do any other WAP brands that support Handoff work with Araknis Fast Roaming?
We don’t guarantee compatibility with any other brands, but will list them if we find any that are.
• Does any equipment NOT work with Fast Roaming/Handoff?
• Gen 1 Apple iOS products won’t work. Most newer iOS devices work correctly.
• Check the product page support tab at www.snapav.com for recent updates on compatibility issues.
15.3.1.1 - Fast Roaming Setup Instructions

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

<table>
<thead>
<tr>
<th>Wireless Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>Yes</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Global Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Band Steering</td>
</tr>
<tr>
<td>On</td>
</tr>
</tbody>
</table>

3. Click Save and then Apply Changes to enable the new settings.

4. Repeat steps 1-3 in the remaining WAPs.

5. After setup, test the new settings using several client devices. You should see the client device listed in each WAP’s Connected Clients table (Path: Status, Wireless Interface).

15.3.1.2 - Fast Roaming Troubleshooting

- If certain devices don’t work once Fast Roaming is enabled, try turning Fast Roaming off and checking for connection again. The device might be incompatible with Fast Roaming.
15.4 - Wireless Networks
The Wireless Networks menu allows configuration of access point wireless networks (SSID’s), security settings, band steering and channel isolation.

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

Figure 31. Wireless Networks

Path – Settings, Wireless, Wireless Settings, Wireless Networks

Parameters –

Note – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

- Enable – Select Yes to turn a wireless network ON.
  Default: Yes (Checked)
- Name (SSID) – Enter the network name for the network being configured.
  Default: araknis_initial; (Blank when adding a new network).
  Note – Be sure to change the SSID. The default settings are not secure.
- Interface – Select 2.4GHz/5GHz or Both Channel Frequency.
  Default: Both, (2.4GHz when adding a network).
- Security Mode – Configure the security mode for each wireless network. Select a security mode from the drop-down to open the Wireless Security Setup Window. See section “15.5 - Wireless Security Setup (SSID Encryption)” on page 39 for wireless security setup instructions.
  Default: Open
- Broadcast SSID – Select whether or not to publicly display the SSID to nearby Wi-Fi devices.
  Default: Yes
- Channel Isolation – Select to prevent communication between wireless clients on different SSID’s.
  Default: Not selected.
- Add – Click to add a wireless network.
- Delete – Click to delete a wireless network.
15.5 - Wireless Security Setup (SSID Encryption)
The Wireless Security menu opens during the setup of an existing or new wireless network. The options change with the encryption method, so each type of encryption is described in a separate section.

15.5.1 - WEP Mode

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

Figure 32. Wireless Security – WEP Mode

Path – Settings, Wireless, Wireless Networks, Security Mode

Parameters –
- **Name (SSID)** – The name of the network being configured.
- **Security Mode** – Select a different encryption mode from the drop-down.
- **Auth Type** – Select Open System or Shared Key mode from the drop-down:
- **Input Type** – Select Hex or ASCII from the drop-down.
- **Key Length** – Select 64 or 128 bit encryption from the drop-down.
- **Default Key** – Select which of the 4 keys is the default value.
- **Key (1-4)** – Enter up to 4 unique identification keys for WEP.
- **Save** – Click to save changes to the Wireless Security Settings for this network. The window will close.
- **Cancel** – Click to cancel changes to the Wireless Security Settings for this network. The window will close.
15.5.2 - WPA-PSK Mixed and WPA2-PSK Modes

Figure 33. Wireless Security – WPA-PSK and WPA2-PSK Modes

Path – Settings, Wireless, Wireless Networks, Security Mode

Parameters –

• **Name (SSID)** – The name of the network being configured.

• **Security Mode** – Select a different encryption mode from the drop-down.

• **Encryption** – WPA2-PSK: AES; WPA2-PSK Mixed: Both (TKIP+AES).

• **Passphrase** – Enter the appropriate passphrase for the wireless network being configured. If using the ASCII format, the password must be 8-63 characters in length. If using HEX, the password must be 64 HEX characters in length. 
  *Default: Blank*

• **Group Key Update Interval** – Enter a value to specify how often in seconds the Group key changes. RANGE: 30-3600 seconds. 
  *Default: 3600 (60 minutes)*

• **Save** – Click to save changes to the Wireless Security Settings for this network. The window will close.

• **Cancel** – Click to cancel changes to the Wireless Security Settings for this network. The window will close.
15.5.3 - WPA and WPA2 Modes

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

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

Pro Tip – For models with 2.4 and 5Ghz radios: With Band Steering enabled, the 2.4 and 5 Ghz networks automatically share SSID settings. If Band Steering is not enabled, provide guests with passwords to both the 2.4 and 5GHz network for seamless operation.

Pro Tip – Fast Roaming will not work for SSIDs created using the Guest Network feature. To create guest SSIDs with Fast Roaming, see section “24.1 - Configuring Guest Networks with Fast Roaming” on page 79.

Figure 35. Guest Network

Path – Settings, Wireless, Guest Network

Parameters –

- Enable – Check the box to enable a guest network.  
  Default: Disabled

- Name (SSID) – Enter an SSID for the guest network.  
  Default: Araknis-2.4_GuestNetwork; Araknis-5.0_GuestNetwork

- Interface – Displays the wireless radio used for the guest network (2.4 or 5.0 Ghz).

- Security Mode – Select a security mode for the SSID.  
  Default: Open

Note – Guest networks are limited to Open, WPA-PSK Mixed and WPA2-PSK encryption modes. See section “15.5.2 - WPA-PSK Mixed and WPA2-PSK Modes” on page 40 for encryption setup instructions.
• **Broadcast SSID** – Selecting this option will allow the guest network SSID to appear in ‘Network Lists’ on wireless devices for user login. If not selected, the user will have to know the SSID and enter it manually to access the network.
  
  *Default: Not selected*

• **Channel Isolation** – Select to prevent communication between wireless clients on different SSID’s of the guest network.
  
  *Default: Selected*

• **Manual IP Settings** – Settings for the guest network DHCP server. All guest clients are placed on a different subnet as configured in this area.
  
  • **Gateway IP Address** – Enter the Guest Network Gateway IP address.
    
    *Default: 192.168.200.1*

  • **Subnet Mask** – Enter the subnet mask for the Guest Network Gateway.
    
    *Default: 255.255.255.0*

• **Automatic DHCP Server Settings** – Configure the IP addresses issued to guest clients.
  
  • **Starting IP Address** – Enter the lowest address available for the Guest Network.
    
    *Default: 192.168.200.100*

  • **Ending IP Address** – Enter the highest address available for the Guest Network.
    
    *Default: 192.168.200.200*

  • **WINS Server IP** – Enter the IP address for the WINS Server for the Guest Network.
    
    *Default: 0.0.0.0*
15.7 - Configuring the WAP as a Repeater

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

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

**Pro Tip** – It is always better to get a wire to a WAP location than to use repeater mode.

Special Setup Requirements

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

Installation Notes

- **Do Fast Roaming and Repeater mode work together?**
  Not for the radio being used as a repeater. Fast Roaming is not required for repeater mode.

- **Can repeater WAPs be used as a wireless bridge? (LAN port to switch or client device)**
  Yes. Connect an Ethernet patch cable from the Ethernet port on the repeater WAP to the client device LAN port.

- **Can multiple unwired repeater WAPs connect to one wired WAP?**
  Yes.

- **If a 300/500/700 series WAP is configured using one radio in repeater mode, can I configure more SSIDs on the other radio?**
  Yes. All traffic will be sent to the wired LAN over the repeater antenna.

- **Can an all Araknis WAPs work together using Repeater mode?**
  Yes.
15.7.1 - Repeater Mode Setup Instructions

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

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

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

   - **Repeater SSID** – Enter an SSID name for the repeater WAP connection.
   - **Interface** – Displays the interface frequency set for repeater mode.
   - **Security** – Enter the security credentials for the SSID from the wired WAP in step 1.
   - **Target SSID** – Enter the SSID from the wired WAP configured in step 1.
   - **Preferred BSSID** – (Optional) enter the MAC address of the radio for the Target SSID. This is required if there are multiple WAPs transmitting the same SSID.

4. Click Apply and then Apply Changes to enable the new settings.

5. After setup, connect to each SSID on each WAP and confirm that your client device operates as expected.
16 - Security Settings
The Security Settings screen allows configuration of who can log into the access point interface and what level of privileges they have, how the device can be accessed, email notification of system status and warnings, and device discovery.

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

Figure 36. User Accounts

Path – Settings, Security, User Accounts

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

Configuration Instructions –
1. Click **Settings**, **Security**.
2. Specify the user account settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
16.2 - Access Control
Allows configuration of how the access point interface may be accessed.

Figure 37. Access Control

Path – Settings, Security, Access Control

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

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

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

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

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

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

Configuration Instructions –
1. Click **Settings, Security**.
2. Specify the access control settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
16.3 - Email Alert
The Email Alert menu allows configuration of the email notification system for status and warnings.

Figure 38. Email Alert Setup Example

Path – Settings, Security, Email Alerts

Parameters –

• **Status** – Select Enable to send email notifications in the event of certain abnormal conditions.  
  *Default: Not selected*

• **From** – Enter the email address of the sender.  
  *Default: Blank*

• **To** – Enter the email address of the recipient.  
  *Default: Blank*

• **Subject** – Information regarding the nature of the system condition.  
  *Default: [Email-Alert][araknis][88:DC:96:1D:33:6B][Configuration Changed]*

• **Email Account** –
  - **Username** – Enter the username for the email account (Outlook, Gmail, etc.) sending the alert.  
    *Default: Blank*
  - **Password** – Enter the password for the email account (Outlook, Gmail, etc.) sending the alert.  
    *Default: Blank*
  - **SMTP Server** – Enter the SMTP Server and Port Number of the email client sending emails.  
    *Default: SMTP Server Blank; Port: 25*
  - **Security Mode** – Select a security mode for sending Email Alerts. None, SSL/TLS, STARTTLS  
    *Default: None*
  - **Send Test Email** – Click the button to send a test email to confirm Email Alert settings.
Figure 39. Common Email Client Ports

<table>
<thead>
<tr>
<th>Email Client</th>
<th>Ports(TLS)</th>
<th>Ports(SSL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gmail</td>
<td>587</td>
<td>465</td>
</tr>
<tr>
<td>Outlook</td>
<td>25 or 587</td>
<td>-</td>
</tr>
<tr>
<td>Microsoft Exchange</td>
<td>25</td>
<td>465</td>
</tr>
<tr>
<td>Yahoo</td>
<td>-</td>
<td>465</td>
</tr>
<tr>
<td>Office 365</td>
<td>587</td>
<td>-</td>
</tr>
</tbody>
</table>

Configuration Instructions –
1. Click Settings, Security.
2. Specify the email alert settings.
3. Click Save, then Apply Changes to enable the new settings.
16.4 - Device Discovery
The Device Discovery menu allows configuration of how or if the access point can search for and connect to network devices via Bonjour and UPnP.

Figure 40. Device Discovery

Path – Settings, Security, Device Discovery

Parameters –
- **Bonjour** – Enable to allow the access point to search for and connect to network devices running Apple iOS and OS X. Bonjour can also be run on devices running a Microsoft OS.
  
  *Default: Disable*

- **UPnP** – Enable to allow the access point to search for and connect to network devices via UPnP Protocol (Universal Plug and Play).
  
  *Default: Disable*

- **Araknis EZ Access** – Use a URL to access the web interface (see section “9.2 - Configured System Name Access” on page 16).
  
  *Default: Enable*

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

Configuration Instructions –
1. Click **Settings, Security**.
2. Specify the device discovery settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
17 - Schedule
Use the schedule settings menu to configure automated features including auto reboot, auto ping, and Wi-Fi access schedules for different SSID’s.

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

Figure 41. Auto Reboot Settings

Path – Settings, Schedule, Auto Reboot Settings

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

Configuration Instructions –
1. Click Settings, Schedule.
2. Enable Auto Reboot.
3. Set the desired days and time for reboots to occur.
4. Click Save, then Apply Changes to enable the new settings.
17.2 - Gateway Connection Monitor

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

**Figure 42. Gateway Connection Monitor Settings**

<table>
<thead>
<tr>
<th><strong>Gateway Connection Monitor</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Status</strong></td>
</tr>
<tr>
<td><strong>Gateway IP Address</strong></td>
</tr>
<tr>
<td><strong>Delay Between Timeouts</strong></td>
</tr>
<tr>
<td><strong>Timeout Attempts Before Reboot</strong></td>
</tr>
<tr>
<td><strong>Ping Delay After Auto Reboot</strong></td>
</tr>
<tr>
<td><strong>Reboot Attempts</strong></td>
</tr>
</tbody>
</table>

**Path** – Settings, Schedule, Gateway Connection Monitor

**Parameters** –

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

**Configuration Instructions** –

1. Enable Gateway Connection Monitor.
2. Set the desired days and time for reboots to occur.
3. Click **Save**, then **Apply Changes** to enable the new settings.
17.3 - Wi-Fi Scheduler
The Wi-Fi Scheduler is used to configure when wireless networks are available for use. The scheduler is based on a 24-hour clock (00:00 = 12:00AM, the start of a given day).

Figure 43. Wi-Fi Scheduler

Path – Settings, System, Wi-Fi Scheduler

Parameters –

- **Status** – Enable or Disable the Wi-Fi Scheduler.
  
  *Default: Disable*

- **Wireless Radio** – Select 2.4GHz or 5GHz for the channel frequency to be scheduled.
  
  *Default: 2.4GHz.*

- **SSID Selection** – Select the SSID to be scheduled.

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

- **Note** – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.
17.3.1 - Configuring Wi-Fi Scheduler

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

Figure 44. Wi-Fi Scheduler Menu

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

Figure 45. Wi-Fi Scheduler Setup Complete
18 - Ping Test

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

Figure 46. Ping Test

Path – Maintenance, Ping

Parameters –

• **Target IP / Domain Name** – Enter the IP address of a device or web page to determine if it can be reached.

• **Ping Packet Size** – Enter the packet size of each ping. Maximum size: 65535. 
  *Default: 64 Bytes*

• **Number of Pings** – Enter the number of ping attempts. 
  *Default: 4*

• **Start** – Click the Start button to send the Ping. Ping Test results will be displayed in the text frame. 
  Ideal results: Same number of packets transmitted/received, 0% packet loss.

Configuration Instructions –

1. Click **Maintenance, Ping**.
2. Specify the ping test settings.
3. Click **Start**.
19 - Traceroute Test

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

Figure 47. Traceroute Test

**Path** – Maintenance, Traceroute

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

**Configuration Instructions** –
1. Click **Maintenance, Traceroute**.
2. Specify the traceroute test settings.
3. Click **Start**.
4. Click **Stop** to end the test.
20 - File Management
Use the File Management screen to back up or restore settings and apply firmware updates.

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

Figure 48. Configuration File

Path – Maintenance, File Management, Configuration File

20.1.1 - Backup Current Configuration
Save the access point’s current configuration settings to a “.tar” format compressed archive on your computer.

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

20.1.2 - Upload New Configuration File
Restore previously saved configuration settings to the access point to restore settings.

1. Click the Choose File button and select a configuration file (“.tar” file type) from the Open window.
2. The file name will appear to the right of the Choose File button as shown in Figure 49. Uploading a New Configuration File, below.
3. Click the From PC button to upload the configuration file. Wait while the Rebooting screen opens and loads the selected configuration. When the upload is finished, the Authentication Required (Log In) window will open.
4. Log in and confirm Configuration settings.

Figure 49. Uploading a New Configuration File
20.1.3 - Restore Factory Defaults

Use the File Management screen to restore default settings.

**Note** – When restoring factory defaults, the SSID, IP address, subnet mask, and gateway IP address will also be reset. Reconnect to the access point using the instructions beginning in section “9.1 - EZ Access Method (Default)” on page 15.

**Figure 50. Restore Factory Defaults**

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

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

**Configuration Instructions** –

1. Click the Yes button to restore the access point to factory default settings. The red ALERT message will appear.

2. Click Confirm to restore factory defaults. Wait while the rebooting screen is open and loading the selected configuration. When the configuration upload is finished, the login window will appear.

3. Enter the username and password. (araknis; araknis)

4. Confirm the new configuration settings.

20.1.4 - Hardware Factory Default

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

**Configuration Instructions** –

1. Using a paper clip or other small, blunt tool press the reset button located on the top of the access point for 30 seconds.

2. After two to four minutes, the WAP will reboot. Restart the setup process or upload a previously saved configuration.
20.1.5 - Firmware

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

Figure 51. Firmware

Path – Maintenance, File Management, Firmware

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

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

Figure 52. Restart

Path – Maintenance, Restart

Configuration Instructions –
1. Click the Reboot the Device button. The message, “This will reboot the device and may take a few seconds...” will appear.

2. Click OK to reboot (or Cancel to return to the Restart Screen).

3. Wait while the access point reboots. When the device has rebooted, the login screen will appear.

4. Enter the username and password.

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

Figure 53. Logout Alert

Path - Maintenance, Logout

Configuration Instructions –
1. From any screen, click **Logout** in the system menu. The Logout ALERT will appear on screen.

2. Click **Cancel** to return to the setup screen; click **Confirm** to log the current user out.
23 - Advanced Menu

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

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

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

Figure 54. Radio Settings

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

Configuration Instructions –
1. Click **Advanced, Wireless Settings**.
2. Specify the radio settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
23.1.2 - Client Limit
The Advanced Wireless Settings screen allows configuration of client limit by band, (2.4GHz/5GHz).

Figure 55. Client Limit Settings

Path – Advanced, Wireless Settings, Client Limit

Parameters –

- **Enable** – Select to enable Client Limit, by channel.
  
  Default: Not Selected.

- **Max Client No.** – Set the maximum number of clients that can be connected to a channel at a given time. (For 300/500/700, the maximum number of clients is set separately for each radio interface.) RANGE: 1-127.
  
  Default: 127.

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

Configuration Instructions –
1. Click **Advanced, Wireless Settings**.
2. Specify the client limit settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
23.2 - Wireless MAC Filter Settings
The Wireless MAC Filter determines if wireless clients (computers, tablets, smartphones) can access the wireless network as defined by client MAC address. Authorized clients can be configured and viewed in the MAC Filter List.

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

**Figure 56. MAC Filter Settings**

Path – Advanced, MAC Filter, MAC Filter Settings

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

Configuration Instructions –
1. Click **Advanced, MAC Filter**.
2. Specify the wireless MAC filter settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
23.2.2 - MAC Filter List
The Wireless MAC Filter List screen can be used to add/delete wireless clients to be filtered by MAC address.

Figure 57. MAC Filter List

Path – Advanced, MAC Filter, MAC Filter List

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

**Configuration Instructions** –
1. Click Advanced, MAC Filter.
2. Specify the MAC filter settings.
3. Click Save, then Apply Changes to enable the new settings.
23.3 - WPS Settings
WPS (Wi-Fi Protected Setup) allows setup of WPS-equipped Wi-Fi devices. Instead of sharing the SSID and security credentials with a client, WPS connected clients using a push button or PIN entry method.

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

Figure 58. WPS Settings Menu

Path – Advanced, WPS

Parameters –

• **Status** – Enable or disable WPS.
  
  *Default: Disabled*

• **Current Configuration** – Lists whether the WPS feature is configured or unconfigured.
  
  • **Release Configuration** – The primary SSID in the WAP will be reset to default if Release Configuration is clicked and then settings are applied.

• **Self-PIN Code** – The WPS pin generated by the WAP.

• **SSID** – Displays SSID used for WPS. Will always be the first SSID in the list on the Wireless Settings page; WPS cannot be used unless this SSID is enabled (checked).

• **Authentication Mode** – Displays authentication mode for the SSID.

• **Encryption Key** – Displays encryption key for the SSID.

• **WPS via Push Button** – Click to connect a device using WPS Push Button. See section “23.3.1 - Connecting a Device Using WPS via Push Button” on page 67 for instructions.

• **WPS via PIN** – Used to connect a device using WPS via PIN. See section “23.3.2 - Connecting a Device Using WPS via PIN” on page 68 for instructions.
23.3.1 - Connecting a Device Using WPS via Push Button

Specific Setup Requirements
• Client device equipped with WPS Push Button
• Administrator access to the WAP interface

Configuration Instructions –
1. Power on the WPS enabled client device to be connected.

2. Log into the WAP local interface as an administrator and navigate to Advanced, WPS. Enable WPS if it is disabled (remember to complete the Apply Settings process).

3. Press the WPS button on the client device, then click the WPS via Push Button Start button in the WAP interface.

4. The device will connect. Test connectivity to the device to ensure WiFi operation. WPS-connected devices will appear in the Wireless Interface Status page Connected Clients list.
23.3.2 - Connecting a Device Using WPS via PIN

Specific Setup Requirements
• Client device equipped with WPS via PIN
• Administrator access to the WAP interface

Configuration Instructions –
1. Power on the WPS enabled client device to be connected.
2. Find the WPS setup menu and record the device’s WPS PIN.
3. Log into the WAP local interface as an administrator and navigate to Advanced, WPS. Enable WPS if it is disabled (remember to complete the Apply Settings process).
4. In the WAP interface, enter the WPS PIN from the client device in the WPS via PIN field, then click Start.
5. The device will connect. Test connectivity to the device to ensure WiFi operation. WPS-connected devices will appear in the Wireless Interface Status page Connected Clients list.
23.4 - Site Survey

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

Figure 59. Site Survey

Path – Advanced, Site Survey

Parameters –

- **Note** – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

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

Configuration Instructions –

1. Click **Advanced, Site Survey**.
2. Specify which interface to scan.
3. Click **Start** to scan. Results will be displayed once the test is complete.
23.5 - Spectrum Analyzer
Analyze Wi-Fi channel interference at different frequencies and power levels. This information can help determine what channel settings to use for the best Wi-Fi performance.

Figure 60. Spectrum Analyzer Settings

Path – Advanced, Site Survey, Result

Parameters –
• **Select Interface** – 2.4 or 5 Ghz antenna.
• **Scan Bandwidth** – Based on the setting of the selected wireless antenna.
• **Scan Channel** – Based on the setting of the wireless antenna
• **RSSI Filter** – Select an RSSI filter value to use in testing. Using a value closer to zero will eliminate results from weaker signals. The default value is recommended for most environments. **Default: -75**
• **Scan Action** –
  • **Start** – Click to begin a scan.
  • **Play/Pause** – Click to pause an in-progress scan. Click again to resume the scan.
  • **Stop** – Click to stop a scan.
• **Elapsed Time** – Amount of time since the Start button was pressed.

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

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

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

Usage View

Figure 61. Spectrum Analyzer Usage View

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

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

Waveform View

Figure 62. Spectrum Analyzer Waveform View

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

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

Figure 63. Spectrum Analyzer Real-time View

![Real-time View Graph]

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

- **Current** – Average power level shown in the Waveform view. If the current reading is closer to the maximum than the average, the frequency should typically be avoided.

- **Average** – Average power of Waveform view data since since the scan began. This view averages across time as well as data points for any one frequency. Avoid frequencies with spikes above the rest of the graph.

- **Maximum** – Maximum power of Waveform view data since since the scan began. This is the maximum recorded at any given time and frequency of the current scan. Compare to the average and current reading to determine if a channel should be avoided.
23.6 - Wireless Traffic Shaping Settings
Traffic shaping is used to regulate packet flow to control wireless network saturation and reduce latency.

Figure 64. Wireless Traffic Shaping Settings

Path – Advanced, Traffic Shaping

Parameters –

Note – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series 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.

Configuration Instructions –
1. Click Advanced, Traffic Shaping.
2. Specify the wireless traffic shaping settings.
3. Click Save, then Apply Changes to enable the new settings.
23.7 - SNMP Settings
Simple Network Management Protocol (SNMP) is an IP network protocol that can be used to monitor network devices, audit network usage, detect network faults or inappropriate access, and, in some cases, configure remote devices.

Figure 65. SNMP Settings

Path - Advanced, SNMP
23.7.1 - SNMPv2 Settings
This screen allows configuration of SNMPv2 Settings.

Figure 66. SNMPv2 Settings

<table>
<thead>
<tr>
<th>SNMPv2 Settings</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Enable</td>
</tr>
<tr>
<td>Contact</td>
<td>Blank</td>
</tr>
<tr>
<td>Location</td>
<td>Blank</td>
</tr>
<tr>
<td>Port</td>
<td>161</td>
</tr>
<tr>
<td>Community Name (Read Only)</td>
<td>public</td>
</tr>
<tr>
<td>Community Name (Read Write)</td>
<td>private</td>
</tr>
<tr>
<td>Trap Destination</td>
<td>Port 162</td>
</tr>
</tbody>
</table>

Path – Advanced, SNMP, SNMPv2

Parameters –

- **Status** – Select Enable to enable SNMPv2. Select Disable to disable SNMPv2.  
  *Default: Enable*

- **Contact** – Enter the name of the person managing the SNMPv2 server.  
  *Default: Blank*

- **Location** – Enter the physical location of the SNMPv2 server.  
  *Default: Blank*

- **Port** – Indicates the port number for SNMPv2 ‘listening’.  
  *Default: 161 (This is a dedicated TCP/UDP port and typically should not be changed.)*

- **Community Name (Read Only)** – Indicates the password for SNMPv2 read only access.  
  *Default: Public. ‘Public’ is a typical default of SNMP v2 devices for Read Only.*

- **Community Name (Read Write)** – Indicates the password for SNMPv2 read/write access.  
  *Default: Private.*

- **Trap Destination** – An SNMPv2 Trap is a notification of a network event such as a fault or security event. The Trap Destination is typically the IP address of the SNMP server where trap messages will be sent.
  
  - **Port** – Indicates the SNMPv2 port number for ‘receiving traps’.  
    *Default: 162 (This is a dedicated TCP/UDP port and typically should not be changed.)*

- **IP Address** – IP address of the SNMPv2 server that will receive SNMP traps.

- **Community Name** – Indicates the password for the SNMPv2 trap community.

Configuration Instructions –

1. Click **Advanced, SNMP**.
2. Specify the SNMPv2 settings.
3. Click **Save**, then **Apply Changes** to enable the new settings.
23.7.2 - SNMPv3 Settings
This screen allows configuration of SNMPv3 Settings.

Figure 67. SNMPv3 Settings

Path – Advanced, SNMP, SNMPv3

Parameters –
• **Status** – Select Enable to enable SNMPv3. Select Disable to disable SNMPv3.  
  *Default: Enable*

• **Username** – Enter a username for SNMPv3 implementation. RANGE: 1-31 Characters.  
  *Default: admin.*

• **Authorized Protocol** – Select the desired protocol from the drop-down.  
  OPTIONS: MD5, SHA, None.  
  *Default: MD5*

• **Authorized Key** – Enter an authentication key. This key acts as an electronic signature to authenticate an SNMPv3 message. RANGE: 8-32 Characters.  
  *Default: 12345678*

• **Privacy Protocol** – Select the desired protocol from the drop-down. OPTIONS: DES, None.  
  *Default: DES*

• **Privacy Key** – Enter a Privacy Key. This acts as an encryption for the data within a SNMPv3 message. RANGE: 1-8 Characters.  
  *Default: 12345678*

• **Engine ID** – Enter an Engine ID. The Engine ID identifies where a SNMPv3 message is coming from.  
  *Default: Blank*

Configuration Instructions –
1. Click **Advanced, SNMP.**
2. Specify the SNMPv3 settings.
3. Click **Save, then Apply Changes** to enable the new settings.
23.8 - Spanning Tree Settings
Spanning Tree Protocol (STP) is an IP network protocol that prevents undesirable loops caused by multiple active paths between network devices when multiple switches or bridges are used on a network.

Figure 68. Spanning Tree Settings

Path – Advanced, SNMP, Spanning Tree

Parameters –

- **Status** – Enable or Disable STP.
  
  Default: Disable

- **Hello Time** – Enter a value for Hello Time. This setting will determine how often in seconds the access point will send the Hello Message to network switches and bridges to assess network topology. RANGE: 1-10 seconds.
  
  Default: 2 seconds

- **Max Age** – Enter a duration for Max Age. This setting will determine how long the access point will wait for a Hello Message from another switch or bridge. If no message is received within the set duration, the device will be considered off-line and a new STP route will be configured.
  
  RANGE: 6-40 seconds.
  
  Default: 20 seconds.

- **Forward Delay** – Enter a value for Forward Delay. This setting will determine the length of time the access point will take to ‘listen’ to the network and either retain current topology or generate a new topology based upon network switch and bridge status.
  
  RANGE: 4-30 seconds.
  
  Default: 4 seconds.

- **Priority** – Enter a value for Priority from 0-65535. This setting will help determine which bridge is the root bridge, or essentially, the switch that controls the main road that network traffic is going to be routed around to avoid loops. In this game, the lowest score wins. The score is a total of MAC address, the Priority number and a bunch of tie-breaker values that determine the root bridge. Setting a lower Priority will help generate a lower score for a given switch.
  
  Default: 32768.

Configuration Instructions –

1. Click Advanced, Spanning Tree.

2. Specify the Spanning Tree settings.

3. Click Save, then Apply Changes to enable the new settings.
### 23.9 - VLAN Settings

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

**Figure 69. VLAN Settings**

![VLAN Settings](image)

**Path** – Advanced, VLANS

**Parameters –**

- **Note** – The 100 Series will indicate settings and information for the 2.4GHz channel. The 300/500/700 Series will indicate settings and information for the 2.4GHz and 5GHz channels.

- **VLAN Isolation** – Select Yes to assign a VLAN ID.
  
  *Default: Not selected.*

- **SSID** – Indicates the network name of the VLAN being tagged. Any Wireless VLANs that need to be tagged should be added in the Wireless Settings page under Wireless Networks. If a Wireless VLAN does not appear in the VLAN Settings List, check the Wireless Settings page under Wireless Networks to see if it is enabled. If it is not, Enable, Save, then Apply Changes.

- **Interface** – Indicates the 2.4GHz or 5GHz Interface for a given SSID.

- **VLAN ID** – Enter a value for the VLAN ID. RANGE: 1-4094.
  
  *Default: Blank*

**Configuration Instructions –**

1. Click **Advanced, VLANS**.

2. Specify the VLAN settings.

3. Click **Save**, then **Apply Changes** to enable the new settings.
24 - Appendix

24.1 - Configuring Guest Networks with Fast Roaming

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

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

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

Step 1 - Configure the WAPs (repeat for all)

1. Log in as an Administrator.

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

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

4. Be sure to apply changes after all settings have been changed. Setup in the WAPs is now complete. Continue to the next section and complete managed switch setup.
Step 2 – Configure the Managed Switch

1. Log in and go to the VLAN Settings menu.

2. Click Add to create a new VLAN for the guest network SSID(s).

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

4. Click Apply to save the changes. Managed switch setup is now complete. Continue to the next section and complete router setup.
Step 3 – Configure the Router

1. Log in and go to the Advanced VLANs menu.

2. Click Add to create a new VLAN entry.

3. Configure the settings for the VLAN:
   
   A.  **VLAN ID** – Enter the same ID number for the guest VLAN as used in the other devices (VLAN 2 in this example).

   B.  **Description** – Enter the same information used in the VLAN Name field of the managed switch.

   C.  **Inter VLAN Routing** – Set to Disabled for a guest network so guests don’t get access to the rest of the network.

   D.  **Device Management** – Select Disabled so that guest clients can’t access the router management interface.

   E.  **Route Binding** – Set whether routes use the WAN1 or WAN2 port. Leave set to none for link failover.

   F.  **LAN1/2/3/4** – Set all LAN ports to “Tagged” using the dropdowns.

4. Click Apply to save the settings. Configuration is complete.

Step 3 – Test the Guest Network

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

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

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

Figure 70. Reset Button

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

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Package Contents</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>Residential Access Point Location</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>Small Commercial Access Point Location</td>
<td>8</td>
</tr>
<tr>
<td>4</td>
<td>EIA/TIA 568B Termination Pattern</td>
<td>9</td>
</tr>
<tr>
<td>5</td>
<td>Network Wiring Diagram</td>
<td>10</td>
</tr>
<tr>
<td>6</td>
<td>Junction Box Mounting</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>Drywall Mounting</td>
<td>12</td>
</tr>
<tr>
<td>8</td>
<td>Ceiling Tile Mounting</td>
<td>12</td>
</tr>
<tr>
<td>9</td>
<td>Status LED Location</td>
<td>13</td>
</tr>
<tr>
<td>10</td>
<td>Default SSID</td>
<td>15</td>
</tr>
<tr>
<td>11</td>
<td>EZ Setup Login Screen</td>
<td>15</td>
</tr>
<tr>
<td>12</td>
<td>System Name Access</td>
<td>16</td>
</tr>
<tr>
<td>13</td>
<td>Fing IP Scanner Example</td>
<td>17</td>
</tr>
<tr>
<td>14</td>
<td>Web Interface Layout</td>
<td>21</td>
</tr>
<tr>
<td>15</td>
<td>Applying Changes</td>
<td>22</td>
</tr>
<tr>
<td>16</td>
<td>System Information Table</td>
<td>23</td>
</tr>
<tr>
<td>17</td>
<td>Wireless Information</td>
<td>24</td>
</tr>
<tr>
<td>18</td>
<td>LAN Information and System Log</td>
<td>25</td>
</tr>
<tr>
<td>19</td>
<td>Radio Status</td>
<td>26</td>
</tr>
<tr>
<td>20</td>
<td>Utilization of SSID Status</td>
<td>27</td>
</tr>
<tr>
<td>21</td>
<td>Wireless Network Status</td>
<td>27</td>
</tr>
<tr>
<td>22</td>
<td>Connected Client Status</td>
<td>28</td>
</tr>
<tr>
<td>23</td>
<td>System Information</td>
<td>29</td>
</tr>
<tr>
<td>24</td>
<td>Date and Time Settings</td>
<td>30</td>
</tr>
<tr>
<td>25</td>
<td>Time Zone</td>
<td>31</td>
</tr>
<tr>
<td>26</td>
<td>IP Settings</td>
<td>32</td>
</tr>
<tr>
<td>27</td>
<td>Interface Settings</td>
<td>33</td>
</tr>
<tr>
<td>28</td>
<td>Radio Settings</td>
<td>34</td>
</tr>
<tr>
<td>29</td>
<td>Utilization of SSID Status</td>
<td>35</td>
</tr>
<tr>
<td>30</td>
<td>Global Wireless Settings</td>
<td>35</td>
</tr>
<tr>
<td>31</td>
<td>Wireless Networks</td>
<td>38</td>
</tr>
<tr>
<td>32</td>
<td>Wireless Security - WEP Mode</td>
<td>39</td>
</tr>
<tr>
<td>33</td>
<td>Wireless Security - WPA-PSK and WPA2-PSK Modes</td>
<td>40</td>
</tr>
<tr>
<td>34</td>
<td>Wireless Security - WPA-PSK and WPA2-PSK Modes</td>
<td>41</td>
</tr>
<tr>
<td>35</td>
<td>Guest Network</td>
<td>42</td>
</tr>
<tr>
<td>36</td>
<td>User Accounts</td>
<td>46</td>
</tr>
<tr>
<td>37</td>
<td>Access Control</td>
<td>47</td>
</tr>
<tr>
<td>38</td>
<td>Email Alert Setup Example</td>
<td>48</td>
</tr>
<tr>
<td>39</td>
<td>Common Email Client Ports</td>
<td>49</td>
</tr>
<tr>
<td>Figure</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>40</td>
<td>Device Discovery</td>
<td>50</td>
</tr>
<tr>
<td>41</td>
<td>Auto Reboot Settings</td>
<td>51</td>
</tr>
<tr>
<td>42</td>
<td>Gateway Connection Monitor Settings</td>
<td>52</td>
</tr>
<tr>
<td>43</td>
<td>Wi-Fi Scheduler</td>
<td>53</td>
</tr>
<tr>
<td>44</td>
<td>Wi-Fi Scheduler Menu</td>
<td>54</td>
</tr>
<tr>
<td>45</td>
<td>Wi-Fi Scheduler Setup Complete</td>
<td>54</td>
</tr>
<tr>
<td>46</td>
<td>Ping Test</td>
<td>55</td>
</tr>
<tr>
<td>47</td>
<td>Traceroute Test</td>
<td>56</td>
</tr>
<tr>
<td>48</td>
<td>Configuration File</td>
<td>57</td>
</tr>
<tr>
<td>49</td>
<td>Uploading a New Configuration File</td>
<td>57</td>
</tr>
<tr>
<td>50</td>
<td>Restore Factory Defaults</td>
<td>58</td>
</tr>
<tr>
<td>51</td>
<td>Firmware</td>
<td>59</td>
</tr>
<tr>
<td>52</td>
<td>Restart</td>
<td>60</td>
</tr>
<tr>
<td>53</td>
<td>Logout Alert</td>
<td>61</td>
</tr>
<tr>
<td>54</td>
<td>Radio Settings</td>
<td>62</td>
</tr>
<tr>
<td>55</td>
<td>Client Limit Settings</td>
<td>63</td>
</tr>
<tr>
<td>56</td>
<td>MAC Filter Settings</td>
<td>64</td>
</tr>
<tr>
<td>57</td>
<td>MAC Filter List</td>
<td>65</td>
</tr>
<tr>
<td>58</td>
<td>WPS Settings Menu</td>
<td>66</td>
</tr>
<tr>
<td>59</td>
<td>Site Survey</td>
<td>69</td>
</tr>
<tr>
<td>60</td>
<td>Spectrum Analyzer Settings</td>
<td>70</td>
</tr>
<tr>
<td>61</td>
<td>Spectrum Analyzer Usage View</td>
<td>71</td>
</tr>
<tr>
<td>62</td>
<td>Spectrum Analyzer Waveform View</td>
<td>71</td>
</tr>
<tr>
<td>63</td>
<td>Spectrum Analyzer Real-time View</td>
<td>72</td>
</tr>
<tr>
<td>64</td>
<td>Wireless Traffic Shaping Settings</td>
<td>73</td>
</tr>
<tr>
<td>65</td>
<td>SNMP Settings</td>
<td>74</td>
</tr>
<tr>
<td>66</td>
<td>SNMPv2 Settings</td>
<td>75</td>
</tr>
<tr>
<td>67</td>
<td>SNMPv3 Settings</td>
<td>76</td>
</tr>
<tr>
<td>68</td>
<td>Spanning Tree Settings</td>
<td>77</td>
</tr>
<tr>
<td>69</td>
<td>VLAN Settings</td>
<td>78</td>
</tr>
<tr>
<td>70</td>
<td>Reset Button</td>
<td>82</td>
</tr>
</tbody>
</table>
## 27 - Specifications

### 100/300 Series Specifications

<table>
<thead>
<tr>
<th>Description</th>
<th>AN-100-AP-I-N</th>
<th>AN-300-AP-I-N</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Interfaces</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RJ45</td>
<td>10/100Base-T x1</td>
<td>10/100/1000Base-T x1</td>
</tr>
<tr>
<td>PoE 802.3at/af compliant</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Wireless Interface</td>
<td>802.11 b/g/n</td>
<td>802.11 a/b/g/n</td>
</tr>
<tr>
<td>Embedded Antennas</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>Performance</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antenna Type</td>
<td>Omni-directional</td>
<td></td>
</tr>
<tr>
<td>Transmit Power</td>
<td>See MCS table</td>
<td></td>
</tr>
<tr>
<td>Receiver Sensitivity</td>
<td>See MCS table</td>
<td></td>
</tr>
<tr>
<td>802.11n</td>
<td>2x2:2 MIMO</td>
<td></td>
</tr>
<tr>
<td>PHY Data Rate</td>
<td>Up to 300 Mbps</td>
<td>Up to 300 Mbps in both frequency bands</td>
</tr>
<tr>
<td>Operating Frequencies</td>
<td>2.4GHz</td>
<td>2.4GHz &amp; 5GHz</td>
</tr>
<tr>
<td>Channel Bonding</td>
<td>Yes (20MHz and 40MHz)</td>
<td></td>
</tr>
<tr>
<td>Memory</td>
<td>64MB</td>
<td>128MB</td>
</tr>
<tr>
<td>Flash Memory</td>
<td>16MB</td>
<td>16MB</td>
</tr>
<tr>
<td><strong>Wireless Features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto Channel Selection</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Operation Modes</td>
<td>Access Point</td>
<td></td>
</tr>
<tr>
<td>Multiple SSIDs</td>
<td>Yes - up to 8</td>
<td></td>
</tr>
<tr>
<td>Wireless Security</td>
<td>WPA2-PSK (AES + TKIP), WPA-Enterprise</td>
<td></td>
</tr>
<tr>
<td>MAC Address Filtering</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Hide SSID</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Guest Network</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td><strong>L2 features</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLANs</td>
<td>Yes - 802.1Q</td>
<td></td>
</tr>
<tr>
<td>QoS</td>
<td>Yes - WME 802.11e</td>
<td></td>
</tr>
<tr>
<td>RJ45 Auto-sensing</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>RJ45 Auto-negotiation</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
<td>Yes, 802.1Qd</td>
<td></td>
</tr>
</tbody>
</table>
### Specifications

<table>
<thead>
<tr>
<th>Description</th>
<th>AN-100-AP-I-N</th>
<th>AN-300-AP-I-N</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Telnet</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP v1, v2c, v3</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP client</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Log</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bonjour</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Araknis EZ Access</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UPnP</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Config File Download/Upload</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OvrC Cloud Services</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wi-Fi Scheduler</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Survey</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LED Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto Reboot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Environmental &amp; Physical</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Dimensions (W-H-D)</td>
</tr>
<tr>
<td>External Power Supply</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Temperature Range</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Humidity</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Certifications</td>
</tr>
</tbody>
</table>
### 100/300 Series MCS Table (RF Performance)

<table>
<thead>
<tr>
<th>Channel</th>
<th>Data Rate</th>
<th>Transmit Power (combined, dBm)</th>
<th>Receive Sensitivity (combined, dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AN-100-AP-I-N</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11b @ 2.4 GHz</td>
<td>1 Mbps</td>
<td>29</td>
<td>≤ -93</td>
</tr>
<tr>
<td></td>
<td>11 Mbps</td>
<td>29</td>
<td>≤ -90</td>
</tr>
<tr>
<td>802.11g @ 2.4 GHz</td>
<td>6 Mbps</td>
<td>28</td>
<td>≤ -89</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>25</td>
<td>≤ -71</td>
</tr>
<tr>
<td>802.11n HT20 @ 2.4 GHz</td>
<td>MCS 0/8</td>
<td>27</td>
<td>≤ -87</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>24</td>
<td>≤ -69</td>
</tr>
<tr>
<td>802.11n HT40 @ 2.4GHz</td>
<td>MCS 0/8</td>
<td>27</td>
<td>≤ -87</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>24</td>
<td>≤ -69</td>
</tr>
<tr>
<td><strong>AN-300-AP-I-N</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>802.11a @ 5GHz</td>
<td>6 Mbps</td>
<td>26</td>
<td>≤ 90</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>23</td>
<td>≤ -72</td>
</tr>
<tr>
<td>802.11b @ 2.4 GHz</td>
<td>1 Mbps</td>
<td>29</td>
<td>≤ -99</td>
</tr>
<tr>
<td></td>
<td>11 Mbps</td>
<td>29</td>
<td>≤ -93</td>
</tr>
<tr>
<td>802.11g @ 2.4 GHz</td>
<td>6 Mbps</td>
<td>29</td>
<td>≤ -96</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>23</td>
<td>≤ -82</td>
</tr>
<tr>
<td>802.11n HT20 @ 2.4 GHz</td>
<td>MCS 0/8</td>
<td>29</td>
<td>≤ -97</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>23</td>
<td>≤ -78</td>
</tr>
<tr>
<td>802.11n HT40 @ 2.4GHz</td>
<td>MCS 0/8</td>
<td>29</td>
<td>≤ -86</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>23</td>
<td>≤ -69</td>
</tr>
<tr>
<td>802.11n HT20 @ 5GHz</td>
<td>MCS 0/8</td>
<td>26</td>
<td>≤ -89</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>23</td>
<td>≤ -70</td>
</tr>
<tr>
<td>802.11n HT40 @ 5GHz</td>
<td>MCS 0/8</td>
<td>26</td>
<td>≤ -87</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15</td>
<td>23</td>
<td>≤ -68</td>
</tr>
</tbody>
</table>
# 500/700 Series Specifications

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

<table>
<thead>
<tr>
<th>Description</th>
<th>AN-500-AP-I-AC</th>
<th>AN-700-AP-I-AC</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Management</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Telnet</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SNMP v1, v2c, v3</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DHCP client</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>System Log</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Bonjour</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Araknis EZ Access</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>UPnP</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote Config File</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Download/Upload</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OvrC Cloud Services</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Wi-Fi Scheduler</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Site Survey</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>LED Control</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Auto Reboot</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Environmental &amp; Physical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dimensions (W-H-D)</td>
<td>6.9” x 6.9” x 1.3”</td>
<td>6.9” x 6.9” x 1.6”</td>
</tr>
<tr>
<td>External Power Supply</td>
<td>12V 2A DC</td>
<td></td>
</tr>
<tr>
<td>Temperature Range</td>
<td>Operating: 32º to 122ºF (0 to 50ºC)</td>
<td>Storage: -4ºF to 140ºF (-20ºC to 60ºC)</td>
</tr>
<tr>
<td>Humidity</td>
<td>Operating: 90% or less</td>
<td>Storage: 90% or less</td>
</tr>
<tr>
<td>Certifications</td>
<td>CE, FCC, IC, Wi-Fi*</td>
<td></td>
</tr>
</tbody>
</table>
## AN-500-AP-I-AC MCS Table (RF Performance)

<table>
<thead>
<tr>
<th>Channel</th>
<th>Data Rate</th>
<th>Transmit Power (combined, dBm)</th>
<th>Receive Sensitivity (combined, dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>802.11b @ 2.4 GHz</strong></td>
<td>1 Mbps</td>
<td>28</td>
<td>-96</td>
</tr>
<tr>
<td></td>
<td>11 Mbps</td>
<td>28</td>
<td>-93</td>
</tr>
<tr>
<td><strong>802.11g @ 2.4 GHz</strong></td>
<td>6 Mbps</td>
<td>27</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>23</td>
<td>-76</td>
</tr>
<tr>
<td><strong>802.11a @ 5 GHz</strong></td>
<td>6 Mbps</td>
<td>26</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>22</td>
<td>-76</td>
</tr>
<tr>
<td><strong>802.11n HT20 @ 2.4 GHz</strong></td>
<td>MCS 0/8/16</td>
<td>26</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>23</td>
<td>-73</td>
</tr>
<tr>
<td><strong>802.11n HT40 @ 2.4 GHz</strong></td>
<td>MCS 0/8/16</td>
<td>26</td>
<td>-88</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>23</td>
<td>-72</td>
</tr>
<tr>
<td><strong>802.11n HT20 @ 5 GHz</strong></td>
<td>MCS 0/8/16</td>
<td>25</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>22</td>
<td>-73</td>
</tr>
<tr>
<td><strong>802.11n HT40 @ 5 GHz</strong></td>
<td>MCS 0/8/16</td>
<td>24</td>
<td>-88</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>21</td>
<td>-72</td>
</tr>
<tr>
<td><strong>802.11ac VHT20 @ 5 GHz</strong></td>
<td>MCS 0_1SS/2SS/3SS</td>
<td>25</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>MCS 8_1SS/2SS/3SS</td>
<td>21</td>
<td>-69</td>
</tr>
<tr>
<td><strong>802.11ac VHT40 @ 5 GHz</strong></td>
<td>MCS 0_1SS/2SS/3SS</td>
<td>24</td>
<td>-88</td>
</tr>
<tr>
<td></td>
<td>MCS 9_1SS/2SS/3SS</td>
<td>20</td>
<td>-64</td>
</tr>
<tr>
<td><strong>802.11ac VHT80 @ 5 GHz</strong></td>
<td>MCS 0_1SS/2SS/3SS</td>
<td>24</td>
<td>-86</td>
</tr>
<tr>
<td></td>
<td>MCS 9_1SS/2SS/3SS</td>
<td>19</td>
<td>-62</td>
</tr>
</tbody>
</table>

**Note** - Maximum transmit power is limited by local regulation.

**Note** - The supported frequency band is restricted by local regulatory requirements.
## AN-700-AP-I-AC MCS Table (RF Performance)

<table>
<thead>
<tr>
<th>Channel</th>
<th>Data Rate</th>
<th>Transmit Power (combined, dBm)</th>
<th>Receive Sensitivity (combined, dBm)</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11b @ 2.4 GHz</td>
<td>1 Mbps</td>
<td>28</td>
<td>-96</td>
</tr>
<tr>
<td></td>
<td>11 Mbps</td>
<td>28</td>
<td>-93</td>
</tr>
<tr>
<td>802.11g @ 2.4 GHz</td>
<td>6 Mbps</td>
<td>27</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>23</td>
<td>-76</td>
</tr>
<tr>
<td>802.11a @ 5 GHz</td>
<td>6 Mbps</td>
<td>26</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>54 Mbps</td>
<td>22</td>
<td>-76</td>
</tr>
<tr>
<td>802.11n HT20 @ 2.4 GHz</td>
<td>MCS 0/8/16</td>
<td>26</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>23</td>
<td>-73</td>
</tr>
<tr>
<td>802.11n HT40 @ 2.4 GHz</td>
<td>MCS 0/8/16</td>
<td>26</td>
<td>-88</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>23</td>
<td>-72</td>
</tr>
<tr>
<td>802.11n HT20 @ 5 GHz</td>
<td>MCS 0/8/16</td>
<td>25</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>22</td>
<td>-73</td>
</tr>
<tr>
<td>802.11n HT40 @ 5 GHz</td>
<td>MCS 0/8/16</td>
<td>24</td>
<td>-88</td>
</tr>
<tr>
<td></td>
<td>MCS 7/15/23</td>
<td>21</td>
<td>-72</td>
</tr>
<tr>
<td>802.11ac VHT20 @ 5 GHz</td>
<td>MCS 0_1SS/2SS/3SS</td>
<td>25</td>
<td>-92</td>
</tr>
<tr>
<td></td>
<td>MCS 8_1SS/2SS/3SS</td>
<td>21</td>
<td>-69</td>
</tr>
<tr>
<td>802.11ac VHT40 @ 5 GHz</td>
<td>MCS 0_1SS/2SS/3SS</td>
<td>24</td>
<td>-88</td>
</tr>
<tr>
<td></td>
<td>MCS 9_1SS/2SS/3SS</td>
<td>20</td>
<td>-64</td>
</tr>
<tr>
<td>802.11ac VHT80 @ 5 GHz</td>
<td>MCS 0_1SS/2SS/3SS</td>
<td>24</td>
<td>-86</td>
</tr>
<tr>
<td></td>
<td>MCS 9_1SS/2SS/3SS</td>
<td>19</td>
<td>-62</td>
</tr>
</tbody>
</table>

**Note** – Maximum transmit power is limited by local regulation.

**Note** – The supported frequency band is restricted by local regulatory requirements.
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

---

<table>
<thead>
<tr>
<th>Česky [Czech]</th>
<th>Araknis Networks tímto prohlašuje, že tento wireless access point je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dansk [Danish]</td>
<td>Undertegnede Araknis Networks erklærer herved, at følgende udstyr wireless access point overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.</td>
</tr>
<tr>
<td>English</td>
<td>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.</td>
</tr>
<tr>
<td>Language</td>
<td>Translation</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Español</td>
<td>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.</td>
</tr>
<tr>
<td>Ελληνική</td>
<td>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.</td>
</tr>
<tr>
<td>Français</td>
<td>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.</td>
</tr>
<tr>
<td>Italiano</td>
<td>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.</td>
</tr>
<tr>
<td>Latvies</td>
<td>Ar šo Araknis Networks deklarē, ka wireless access point atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.</td>
</tr>
<tr>
<td>Lietuvių</td>
<td>Šiuo Araknis Networks deklaruoją, kad šis wireless access point atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.</td>
</tr>
<tr>
<td>Nederlands</td>
<td>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/EC.</td>
</tr>
<tr>
<td>Malti</td>
<td>Hawnehkx, Araknis Networks, jiddikjara li dan wireless access point jikkonforma mahtigijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.</td>
</tr>
<tr>
<td>Magyar</td>
<td>Alulírott, Araknis Networks nyilatkozom, hogy a wireless access point megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.</td>
</tr>
<tr>
<td>Polski</td>
<td>Niniejszym Araknis Networks oświadcza, że wireless access point jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.</td>
</tr>
<tr>
<td>Português</td>
<td>Araknis Networks declara que este wireless access point está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</td>
</tr>
<tr>
<td>Slovenščina</td>
<td>Araknis Networks izjavlja, da je ta wireless access point v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.</td>
</tr>
<tr>
<td>Suomi</td>
<td>Araknis Networks vakuuttaa tätän että wireless access point tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.</td>
</tr>
<tr>
<td>Svenska</td>
<td>Härem 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.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Language</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Česky [Czech]</td>
<td>Araknis Networks tímto prohlašuje, že tento wireless access point je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES.</td>
</tr>
<tr>
<td>Dansk [Danish]</td>
<td>Undertegnede Araknis Networks erklærer herved, at følgende udstyr wireless access point overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.</td>
</tr>
<tr>
<td>English</td>
<td>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.</td>
</tr>
<tr>
<td>Español [Spanish]</td>
<td>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.</td>
</tr>
<tr>
<td>Ελληνική [Greek]</td>
<td>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.</td>
</tr>
<tr>
<td>Français [French]</td>
<td>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.</td>
</tr>
<tr>
<td>Italiano [Italian]</td>
<td>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.</td>
</tr>
<tr>
<td>Latviski [Latvian]</td>
<td>Ar šo Araknis Networks deklarē, ka wireless access point atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citem ar to saistītajiem noteikumiem.</td>
</tr>
<tr>
<td>Nederlands [Dutch]</td>
<td>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.</td>
</tr>
<tr>
<td>Language [Language]</td>
<td>Declaration</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Malti [Maltese]</td>
<td>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.</td>
</tr>
<tr>
<td>Magyar [Hungarian]</td>
<td>Alulírott, Araknis Networks nyilatkozom, hogy a wireless access point megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EC irányelv egyéb előírásainak.</td>
</tr>
<tr>
<td>Polski [Polish]</td>
<td>Niniejszym Araknis Networks oświadcza, że wireless access point jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.</td>
</tr>
<tr>
<td>Português [Portuguese]</td>
<td>Araknis Networks declara que este wireless access point está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.</td>
</tr>
<tr>
<td>Slovensko [Slovenian]</td>
<td>Araknis Networks izjavlja, da je ta wireless access point v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.</td>
</tr>
<tr>
<td>Slovensky [Slovak]</td>
<td>Araknis Networks týmto vyhlasuje, že wireless access point splňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.</td>
</tr>
<tr>
<td>Suomi [Finnish]</td>
<td>Araknis Networks vakuuttaa tätä että wireless access point tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.</td>
</tr>
<tr>
<td>Svenska [Swedish]</td>
<td>Häremed 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.</td>
</tr>
</tbody>
</table>
2-Year Limited Warranty
Araknis Networks® products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to SnapAV or a designated service center with prior notification and an assigned return authorization number (RA).

Contacting Technical Support
P: (866) 838-5052
E: Techsupport@araknisnetworks.com