

### Wireless Handoff/Fast Roaming/802.11rk

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

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

### 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. Setup instructions: "Configuring Guest Networks with Fast Roaming" on page 10.
- **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.
  - We have reports of HP wireless printers not connecting but no model numbers have been provided yet.

\*This list will be updated as we discover any new issues.

### Fast Roaming Setup Instructions

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

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 Yes	Outdated	Both	WPA2-PSK	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

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

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

3. Click Save 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) as you move around the job.

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

### 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.

### Wireless Repeater Mode

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.

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

### Setup Requirements

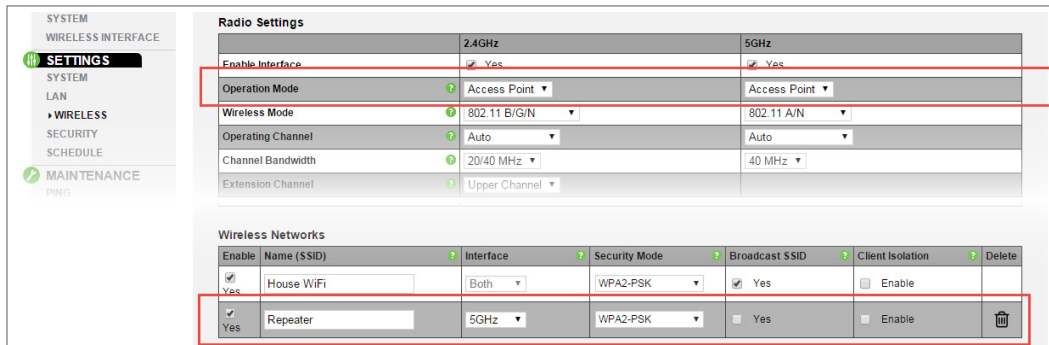
- At least one WAP with a wired LAN connection
- Additional WAP(s) with local power but no LAN connection (must be in range of the wired WAP)
- SSID configuration on each WAP

### FAQs

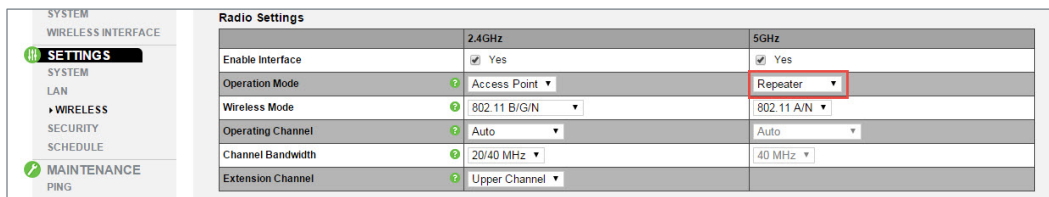
- **Do Fast Roaming and Repeater mode work together?**  
Not for the radio being used as a repeater.
- **Can repeater WAPs be used as a wireless bridge? (LAN port to switch or client device)**  
Yes. Connect an Ethernet patch cable from the Ethernet port on the repeater WAP to the client device LAN port.
- **Can multiple unwired repeater WAPs connect to one wired WAP?**  
Yes, but this can cause further interference issues.
- **If a 300 series WAP is configured using one radio in repeater mode, can I configure more SSIDs on the other radio?**  
Yes. All traffic will be sent to the wired LAN over the repeater antenna.
- **Can 100 and 300 series WAPs work together using Repeater mode?**  
Yes.

### Wireless Repeater Mode Setup Instructions

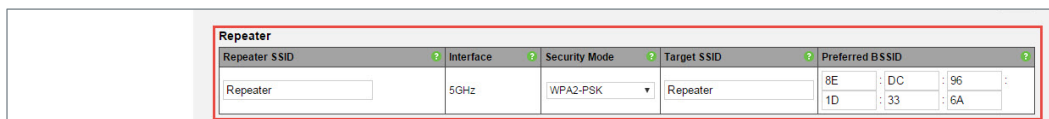
1. Configure the wired WAP normally, with the radio/s set to Access Point mode. Optionally, configure an SSID just for the repeater WAP connection on the 2.4 or 5 GHz antenna.



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

### WPS (Wireless Protected Setup)

WPS (Wi-Fi Protected Setup) allows setup of WPS-equipped Wi-Fi devices. This feature is not recommended for use because WPS can be exploited to gain access to a network if left enabled.

 **Note** - On the WPS Settings page, if you click the Release Configuration button and save the settings, the SSID associated with WPS will revert to default settings.

### Setup Requirements

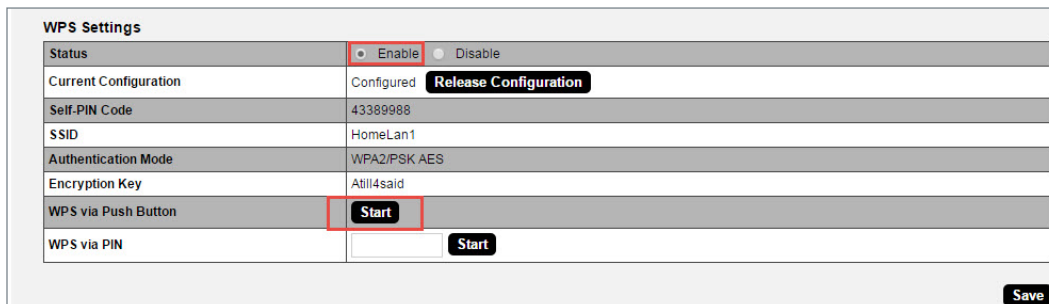
- Client device equipped with WPS
- Administrator access to the WAP interface

### FAQs

- **If I disable WPS after connecting devices using this feature, will the devices remain connected to the network?**  
Yes. Once a device is connected using WPS, it will remain connected. To remove these devices, manually remove them from the network or change the settings for the SSID used for WPS mode.

### Configuring a Device Using WPS Push Button Setup

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).

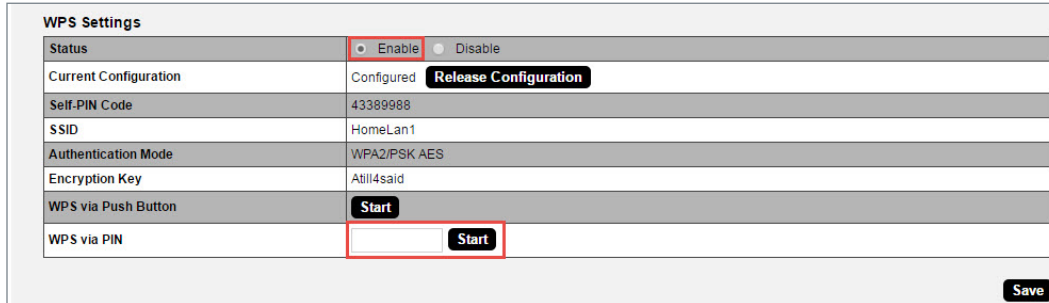


WPS Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Current Configuration	Configured <b>Release Configuration</b>
Self-PIN Code	43389988
SSID	HomeLan1
Authentication Mode	WPA2/PSK AES
Encryption Key	Atll4said
WPS via Push Button	<b>Start</b>
WPS via PIN	<input type="text"/> <b>Start</b>
<b>Save</b>	

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

### Configuring a Device Using WPS PIN Setup

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



WPS Settings	
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Current Configuration	Configured <b>Release Configuration</b>
Self-PIN Code	43389988
SSID	HomeLan1
Authentication Mode	WPA2/PSK AES
Encryption Key	AtI1l4said
WPS via Push Button	<b>Start</b>
WPS via PIN	<input type="text"/> <b>Start</b>
<b>Save</b>	

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

### WPS Troubleshooting

- Not all devices support WPS. If you can't find a WPS feature, use the standard method of connecting to Wi-Fi.
- **I clicked Release Configuration and lost my SSID settings. What do I do now?**  
If you haven't completed the Apply Settings process yet, click the Apply Settings button, then Click Reject to revert your settings. If you have already applied the new settings, go to the Wireless Settings page and reconfigure the SSID.

### 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.

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

Elapsed time: 00:00:09

Path – Advanced, Site Survey, Result

#### Parameters –

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

### 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.

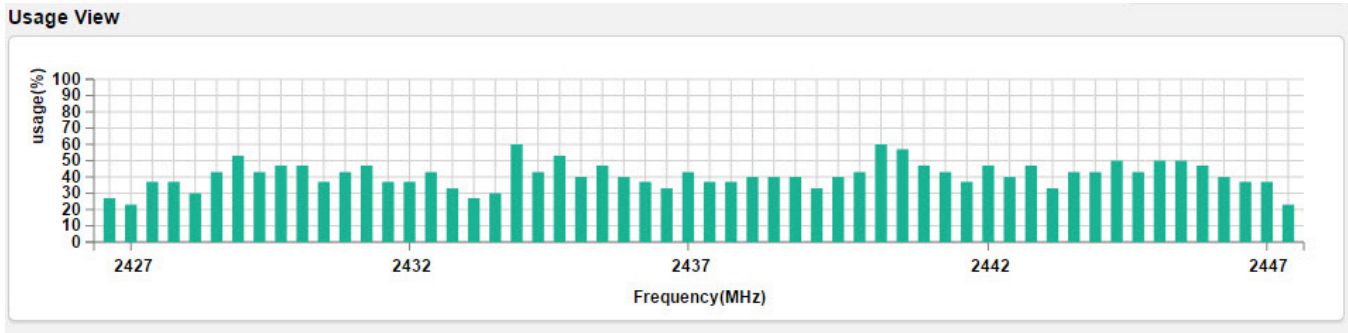
If the channel is set to auto, the scan will be performed using the channel currently in use.

### 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.

### Understanding Spectrum Analyzer Results

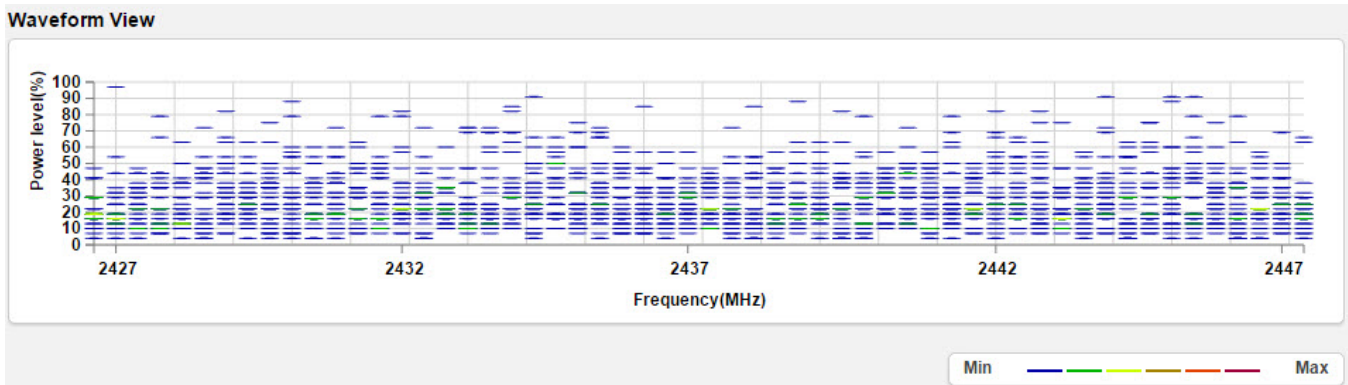
#### Usage View



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

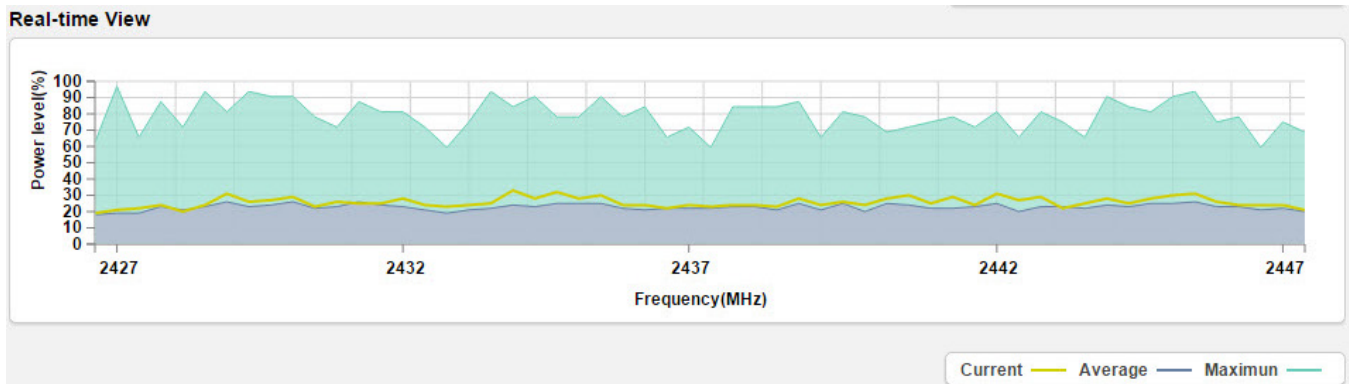


The Waveform view shows the aggregate energy recorded at each scanned frequency. Marks on the graph represent the power level at which signals are being recorded, and the color of the mark roughly estimates how much data is flowing at that level.

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



### Real-time View



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.

### Configuring Guest Networks with Fast Roaming

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

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

### Setup Requirements

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

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

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

Apply Changes: 0

**Global Settings**

Band Steering	?	ON	NOTE: Band Steering is not supported in repeater mode.
Fast Roaming	?	ON	NOTE: Fast Roaming is not supported on the radio in use as the repeater.

**Wireless Networks**

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

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

STATUS

SYSTEM  
WIRELESS INTERFACE

SETTINGS

SYSTEM  
LAN  
WIRELESS  
SECURITY  
SCHEDULE

MAINTENANCE

PING

**VLAN SETTINGS**

**VLAN Settings**

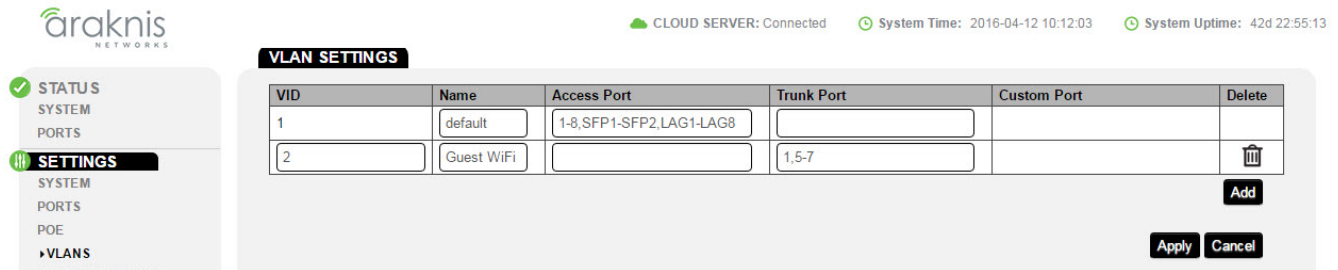
Enable	SSID ▲	Interface ▼	VLAN ID
<input type="checkbox"/> Yes	Employee WiFi	2.4GHz	[ ]
<input type="checkbox"/> Yes	Employee WiFi	5GHz	[ ]
<input checked="" type="checkbox"/> Yes	Guest WiFi	5GHz	2
<input checked="" type="checkbox"/> Yes	Guest WiFi	2.4GHz	2

Save
Cancel

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

### Step 2 – Configure the Managed Switch

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



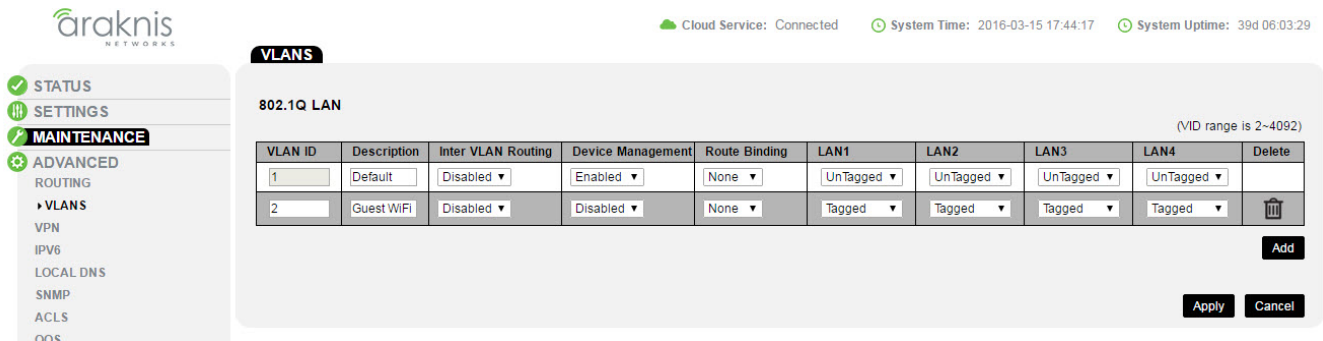
VID	Name	Access Port	Trunk Port	Custom Port	Delete
1	default	1-8,SFP1-SFP2,LAG1-LAG8			
2	Guest WiFi		1,5-7		

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

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

### Step 3 – Configure the Router

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



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

araknis NETWORKS

STATUS  
SETTINGS  
MAINTENANCE  
ADVANCED  
ROUTING  
VLANs  
VPN  
IPV6  
LOCAL DNS  
SNMP  
ACLS  
QoS

802.1Q LAN (VID range is 2-4092)

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

Add  
Apply Cancel

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

### Step 3 – Test the Guest Network

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

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