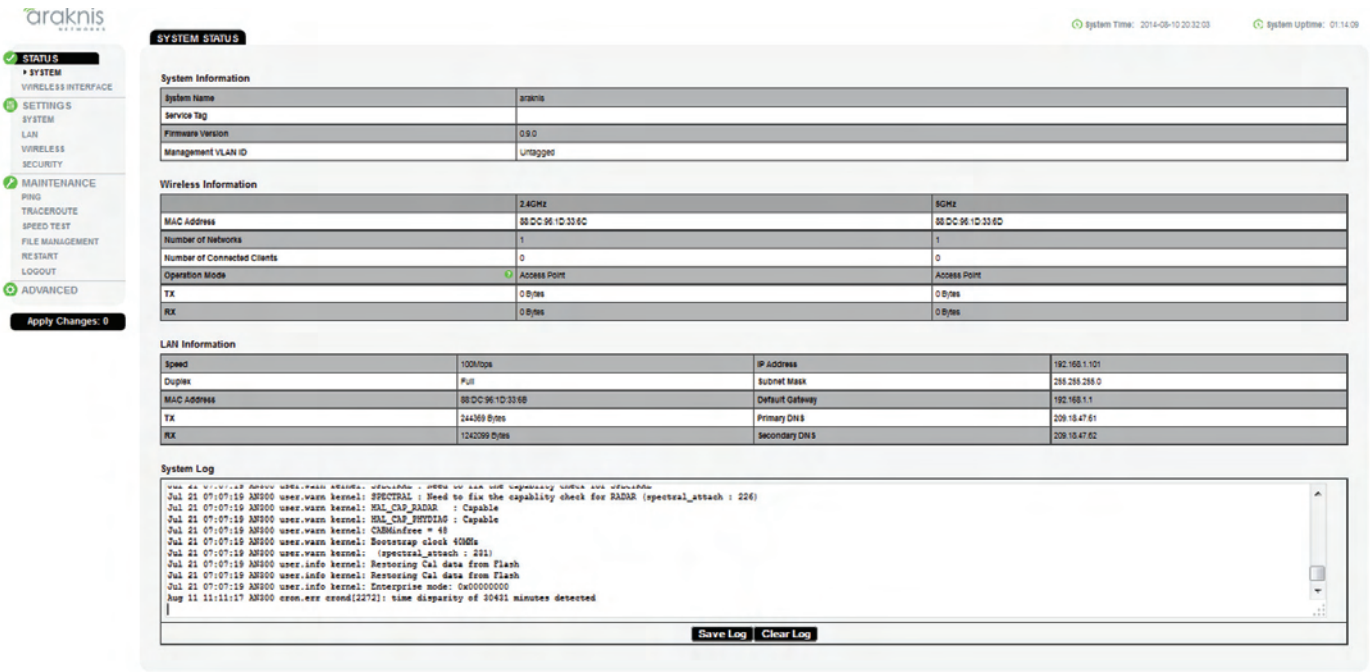
1. Status Menu

1.1. System Status

The System Status screen provides a real-time summary of AN100/300 settings and performance.

Figure 1. System Status Menu

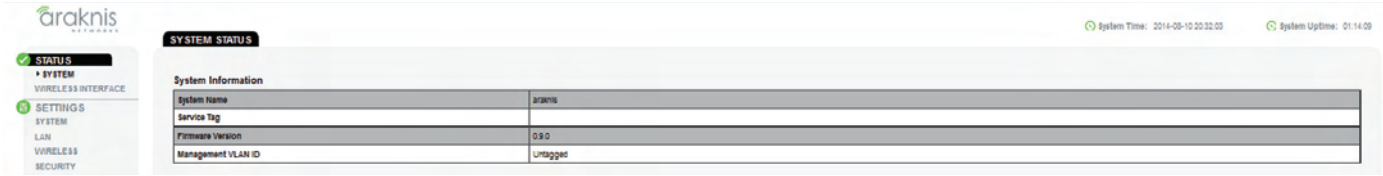


Path Status, System

1.1.1. System Information

The System Information screen provides basic information about the AN100/300.

Figure 2. System Information



Path Status, System, System Information

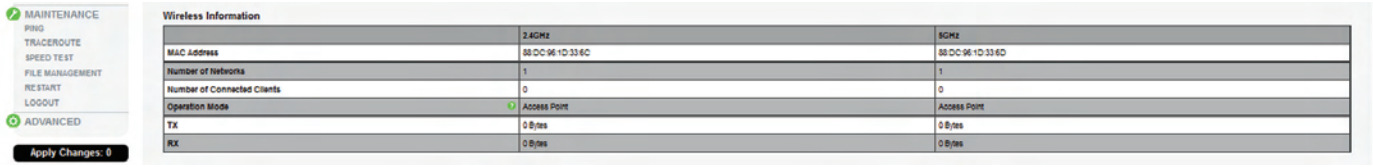
Parameters

- **System Name** – Name assigned to the system.
- **Service Tag** – An internal tracking number used to track every product sold by SnapAV .
- **Firmware Version** – The current version of firmware running on the AN100/300.
- **Management VLAN ID** – The VLAN through which a user can access the web interface of the AN100/300.

1.1.2. Wireless Information

The Wireless Information screen provides basic information about the radio sections of the AN100/300.

Figure 3. Wireless Information



Path Status, System, Wireless Information

Parameters

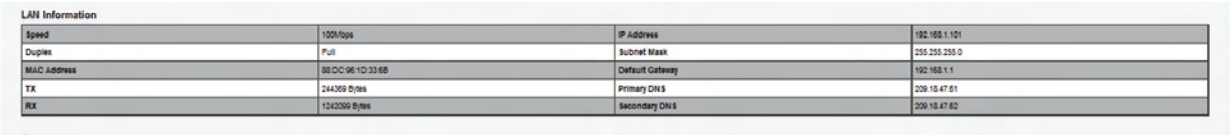
NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **MAC Address** – Device Media Access Control (MAC) Address. The 2.4GHz and 5GHz sections section each have individual MAC Addresses.
- **Number of Networks** – Number of active wireless networks (i.e. SSIDs) configured on the device.
- **Number of Connected Clients** – Number of currently connected wireless clients on all configured networks.
- **Operation Mode** – Indicates that the AN100/300 is setup as an Access Point.
- **TX** – Live counter of data, in bytes, transmitted on the respective radio interface.
- **RX** – Live counter of data, in bytes, received on the respective radio interface.

1.1.3. LAN Information

The LAN Information screen provides basic information about the AN100/300 LAN connection to a connected network device.

Figure 4. LAN Information



LAN Information

Speed	100Mbps	IP Address	192.168.1.101
Duplex	Full	Subnet Mask	255.255.255.0
MAC Address	88:DC:96:1D:33:6B	Default Gateway	192.168.1.1
TX	244369 Bytes	Primary DNS	209.18.47.61
RX	1242099 Bytes	Secondary DNS	209.18.47.62

Path Status, System, LAN Information

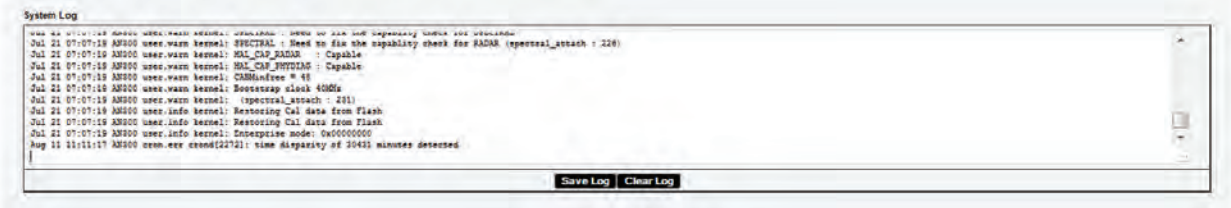
Parameters

- **Speed** – Indicates current LAN speed between the AN100/300 and connected network device.
- **MAC Address** – The LAN MAC Address serves as the device MAC Address.
- **Duplex** – Indicates the current negotiated duplex setting between the AN100/300 and connected network device.
- **TX** – Live counter of data, in bytes, transmitted to the connected network device via LAN connection.
- **RX** – Live counter of data, in bytes, received from the connected network device via LAN connection.
- **IP Address** – AN100/300 IP Address.
- **Subnet Mask** – AN100/300 subnet mask.
- **Default Gateway** – Router IP Address.
- **Primary DNS** – Indicates the Primary DNS for the AN100/300.
- **Secondary DNS** – Indicates the Secondary DNS for the AN100/300.

1.1.4. System Log

The System Log indicates AN100/300 activity in regard to configuration, connections, security conditions, etc. The window will update when the System Status Page is opened.

Figure 5. System Log



Path Status, System, System Log

Parameters

- **System Log** – The System Log indicates AN100/300 activity in regard to configuration, connections, security conditions, etc. The window will update when the System Status Page is opened.

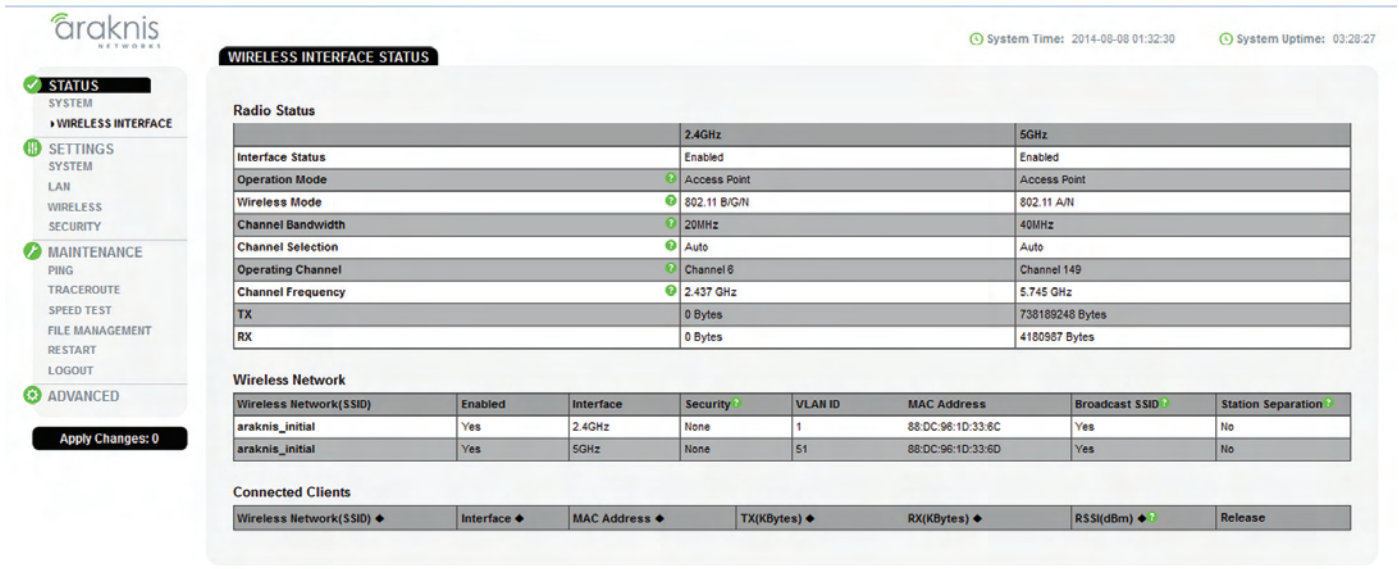
Configuration Instructions

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

1.2. Wireless Interface

The Wireless Interface Status screen provides a detailed look at AN100/300 wireless settings and performance for radio status and settings, Wireless Network configuration and connected client status.

Figure 6. Wireless Interface Status

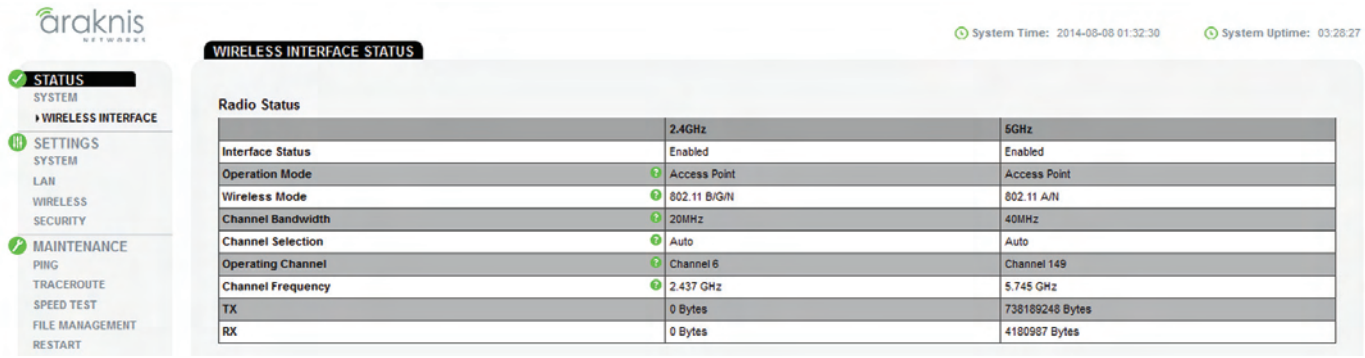


Path Status, Wireless Interface

1.2.1. Radio Status

The Radio Status screen provides a detailed look at AN100/300 radio settings and performance.

Figure 7. Radio Status



	2.4GHz	5GHz
Interface Status	Enabled	Enabled
Operation Mode	Access Point	Access Point
Wireless Mode	802.11 B/G/N	802.11 A/N
Channel Bandwidth	20MHz	40MHz
Channel Selection	Auto	Auto
Operating Channel	Channel 6	Channel 149
Channel Frequency	2.437 GHz	5.745 GHz
TX	0 Bytes	738189248 Bytes
RX	0 Bytes	4180987 Bytes

Path Status, Wireless Interface, Radio Status

Parameters

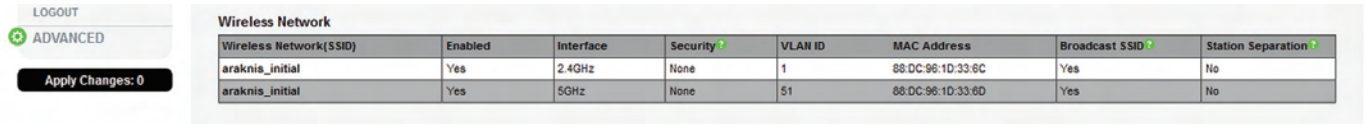
NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Interface Status** – Indicates whether the 2.4/5GHz Wireless Interface is Enabled or Disabled.
- **Operation Mode** – Indicates the current function of the AN100/300 2.4/5GHz Wireless Interface. (Access Point)
- **Wireless Mode** – Indicates the Wireless Mode for the 2.4/5GHz Wireless Interface. (802.11b/g/n; 802.11a/n)
- **Channel Bandwidth** – Indicates the bandwidth of the AN100/300 operating channel. (20MHz or 40MHz)
- **Channel Selection** – Indicates the channel selection mode of the AN100/300 2.4/5GHz Wireless Interface. (Auto or Manual)
- **Operating Channel** – Indicates the selected channel for the AN100/300 2.4/5GHz Wireless Interface.
- **Channel Frequency** – Indicates the frequency of the selected channel for the AN100/300 2.4/5GHz Wireless Interface.
- **TX** – Live counter of data, in bytes, transmitted on each radio interface.
- **RX** – Live counter of data, in bytes, received on each radio interface.

1.2.2. Wireless Network

The Wireless Network screen provides a detailed look at general AN100/300 wireless network settings.

Figure 8. Wireless Network Status



Wireless Network(SSID)	Enabled	Interface	Security	VLAN ID	MAC Address	Broadcast SSID	Station Separation
araknis_initial	Yes	2.4GHz	None	1	88:DC:96:1D:33:6C	Yes	No
araknis_initial	Yes	5GHz	None	51	88:DC:96:1D:33:6D	Yes	No

Path Status, Wireless Interface, Wireless Network

Parameters

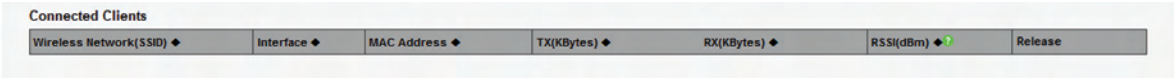
NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Wireless Network(SSID)** – Indicates the network name (SSID) of a AN100/300 wireless network.
- **Enabled** – Indicates that a AN100/300 wireless network is Enabled/Disabled (transmitting/receiving).
- **Interface** – Indicates the Operating Channel of an AN100/300 wireless network.
- **Security** – Indicates the security mode selected for a AN100/300 wireless network.
- **VLAN ID** – Indicates the VLAN ID a for a AN100/300 wireless network.
- **MAC Address** – MAC Address of the AN100/300 2.4/5GHz wireless section.
- **Broadcast SSID** – Indicates whether the network SSID is visible to other network devices and Wi-Fi discovery tools.
- **Station Separation** – Indicates whether AN100/300 client devices connected to different SSIDs can communicate with each other.

1.2.3. Connected Clients

The Wireless Interface Status screen provides a detailed look at AN100/300 connected wireless clients their SSIDs, Interface, MAC Addresses, TX/RX data and RSSI.

Figure 9. Connected Client Status



Path Status, Wireless Interface, Connected Clients

Parameters

- **Wireless Network (SSID)** – Indicates the SSID of a connected wireless client. (Populates as clients connect)
- **Interface** – Indicates the Channel Frequency of a connected wireless client.
- **MAC Address** – Indicates the MAC Address of a connected wireless client.
- **TX (KBytes)** – Live counter of data, in kilobytes, transmitted by AN100/300 to a connected wireless client.
- **RX (KBytes)** – Live counter of data, in kilobytes, received by AN100/300 from a connected wireless client.
- **RSSI (dBm)** – Indicates the wireless signal strength of a connected wireless client. The lower the value the stronger the signal.

Pro Tip – If the client RSSI is -90dBm or higher, the client is very far from the network and is connected at a very slow speed that affects other connected devices on the network.

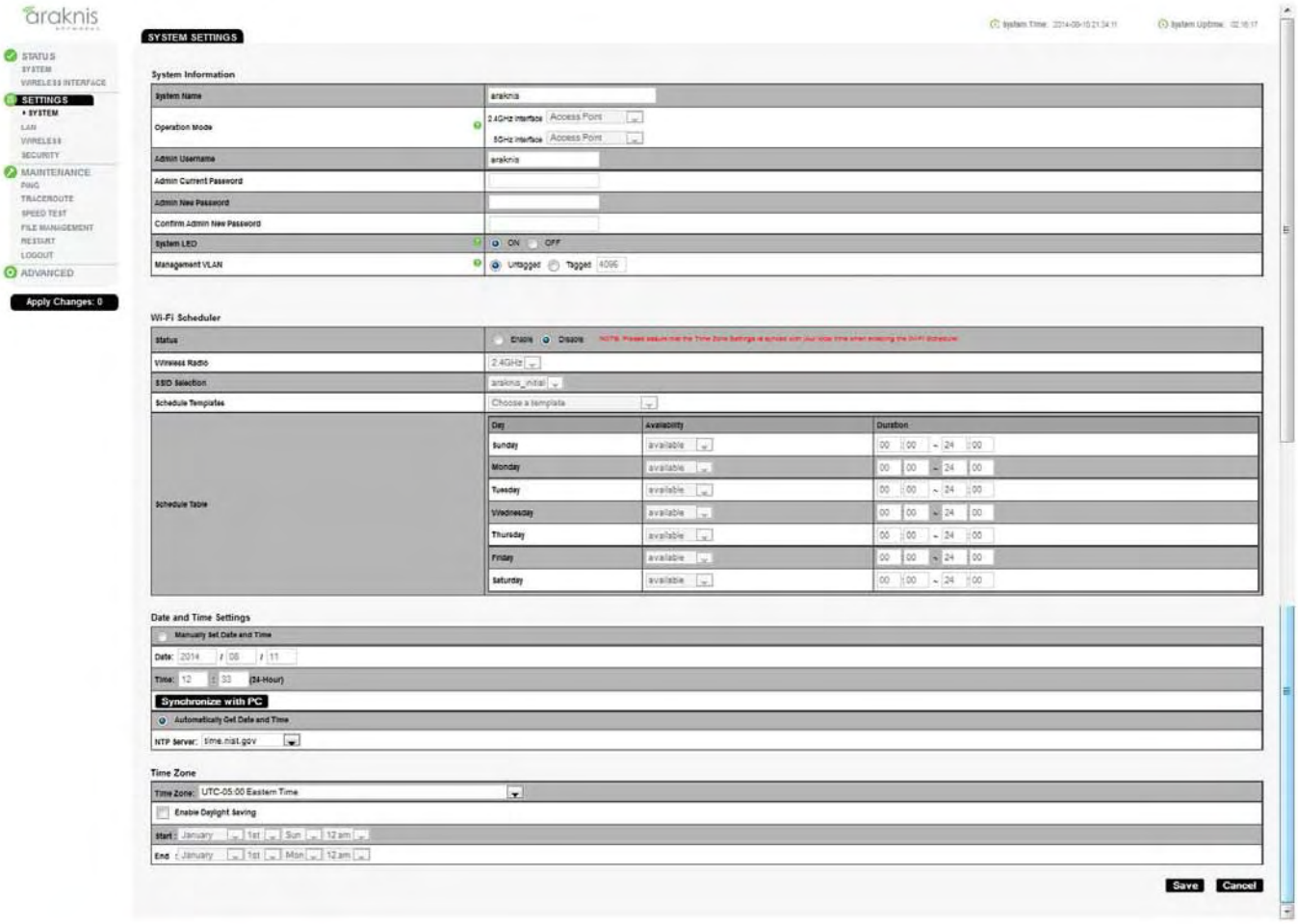
- **Release** – Click the Yes button to drop a client from the network. (Button appears when clients are connected, not shown in default screen image.)

2. Settings Menu

2.1. System Settings

The System Settings screen allows configuration of AN100/300 system settings such as System Name, User Name and Password, Admin Access and settings, Wi-Fi Scheduler, System Date and Time and Time Zone.

Figure 10. System Information

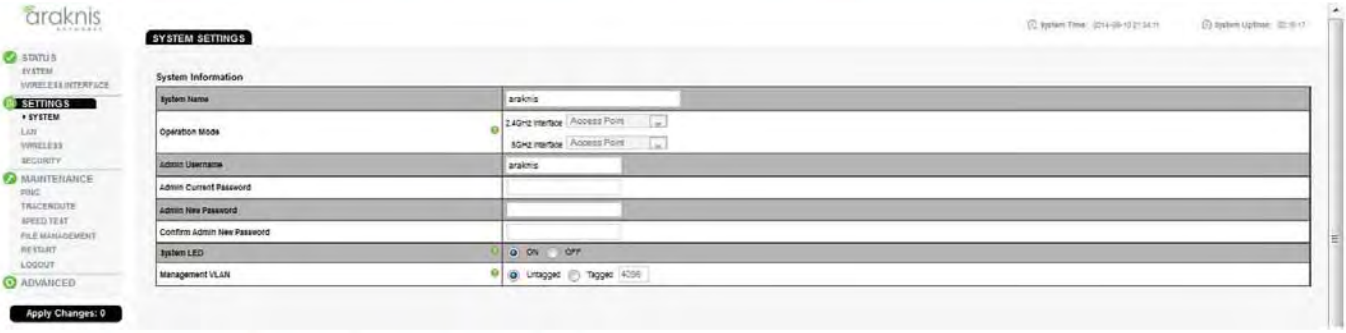


Path Settings, System

2.1.1. System Information

The System Information section allows configuration of AN100/300 admin and access settings.

Figure 11. System Information



Path Settings, System, System Information

Parameters

- **System Name –** Enter a meaningful name such as Jones Home or Jones Home AV Network. DEFAULT: an100/an300 depending upon model.

  NOTE 1: Do not use spaces or special characters when creating the System Name.

  NOTE 2: After a new System Name has been applied, the System Name can be included in a URL to access the AN100/300. Example: If the system name is 'bedroom', the user can use the following URL to access the web interface to the AN100/300: http://config.bedroom.wap
- **Admin Username –** Enter the username that will be used to login to the AN100/300. DEFAULT: araknis
- **Admin Current Password** – Enter the current password to login to the AN100/300. DEFAULT: araknis
- **Admin New Password** – Enter a new password to change the AN100/300 password.
- **Confirm Admin New Password** – Re-enter the exact same information entered in Admin New Password to confirm the new password.
- **System LED –** Select ON to leave AN100/300 System LED ON. Select OFF to turn AN100/300 System LED OFF OPTIONS: ON/OFF DEFAULT: ON
- **Management VLAN –** The VLAN ID the web interface of the AN100/300 can be accessed on. Example: If a VLAN is configured as Management VLAN=10, the user can only access the AN100/300 web interface through VLAN 10. DEFAULT: Untagged.

  CAUTION: Changing this setting may result in the loss of connectivity to the AN100/300. If this should occur, the only way to regain connectivity is to restore the hardware factory default settings. (Press AN100/300 Reset button for 10 seconds.)

Configuration Instructions

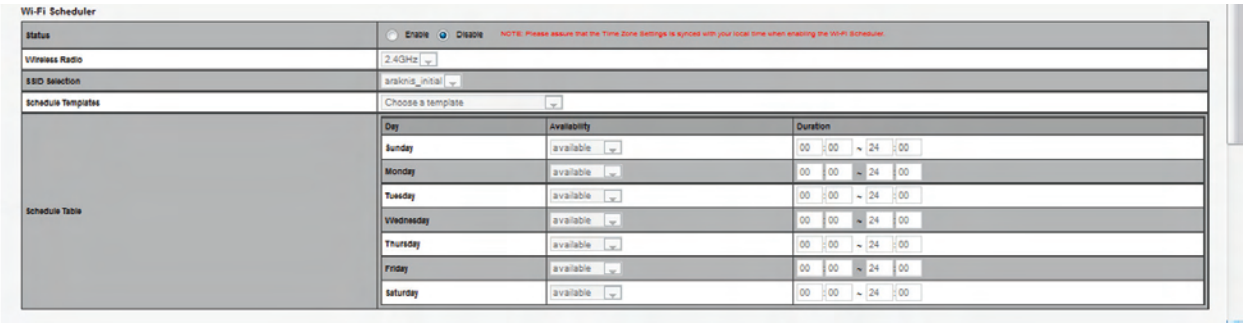
To configure System Information:

1. Click Settings, System.
2. Specify the System Information Settings.
3. Click Save.

2.1.2. Wi-Fi Scheduler

The Wi-Fi Scheduler can be used to determine when AN100/300 wireless networks are available/unavailable for use. The scheduler is based on a 24 hour clock, with 00:00 being 12:00AM, the start of a given day, and the network is enabled. 12:00 is 12:00PM (noon) and the network is still enabled. 24:00 is 12:00AM, the end of that same day, and the network is disabled. Consecutive days of 0:00-24:00 will have the network remain enabled.

Figure 12. Wi-Fi Scheduler



Path Settings, System

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Status** – Select Enable to turn the Wi-Fi Scheduler ON. Select Disable to turn the Wi-Fi Scheduler OFF. OPTIONS: Enable/Disable; DEFAULT: Disable
- **Wireless Radio** – Select 2.4GHz or 5GHz for the channel frequency to be scheduled. OPTIONS: 2.4GHz, 5GHz; DEFAULT: 2.4GHz.
- **SSID Selection** – Select the SSID for the specific radio (2.4GHz/5GHz) to be scheduled.
- **Schedule Templates** – Create different Wi-Fi schedules using the 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.

  Availability – Select Available, by day, to configure wireless network ON when setting up a Custom Schedule or to override the settings in a Schedule Template. Select Unavailable, by day, to configure wireless network OFF when setting up a Custom Schedule or to override the settings in a Schedule Template.

  Duration – Double click the text blocks to set wireless network ON/OFF times. The first two blocks are turn ON time in hours/minutes. The second two blocks are turn OFF time in hours/minutes. The Scheduler works on a 24 hour clock. Example: to set a turn ON time of 8:30AM, enter '08' in the first block and '30' in the second block; to set a turn OFF time of 5:30PM, enter '17' in the first block (12+5=17) and '30' in the second block.

Configuration Instructions

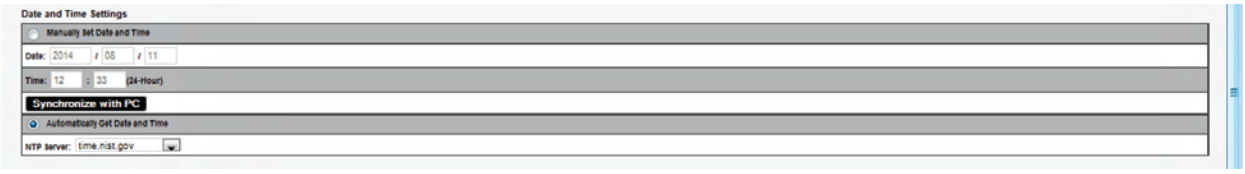
To configure the Wi-Fi Scheduler settings:

1. Click Settings, System.
2. Specify the Wi-Fi Scheduler Settings.
3. Click Save.

2.1.3. Date and Time Settings

The Date and Time section allows configuration of AN100/300 Date and Time settings.

Figure 13. Date and Time Settings



Path Settings, System

Parameters

The Date and Time Settings set the 'real world' time reference for all AN100/300 functions.

- **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, 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 AN100/300 to a connected computer.
- **Automatically Get Date and Time** – Select to automatically get date and time from various web resources.

  NTP Server – Select an NTP (Network Time Protocol) Server to set reference standard date and time. DEFAULT: time.nist.gov.

Configuration Instructions

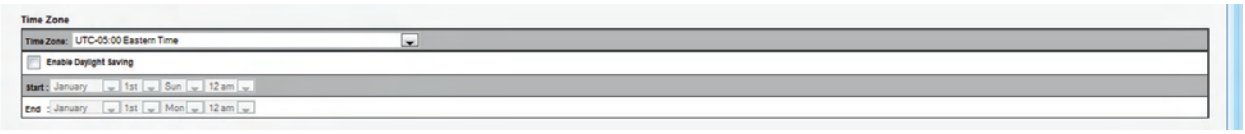
To configure Date and Time Settings:

1. Click Settings, System.
2. Specify the Date and Time Settings.
3. Click Save.

2.1.4. Time Zone

The System Settings screen allows configuration of AN100/300 Time Zone settings.

Figure 14. Time Zone



Path Settings, System

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.

  End – Select the Month, Date, Day and Time Daylight Saving Time ends.

Configuration Instructions

To configure Time Zone Settings:

1. Click Settings, System.
2. Specify the Time Zone.
3. Click Save.

THIS INFORMATION LEFT IN FOR USE IN SAVE/CANCEL INSTRUCTIONS. THIS WILL NOT BE PART OF THE FINAL TEXT.

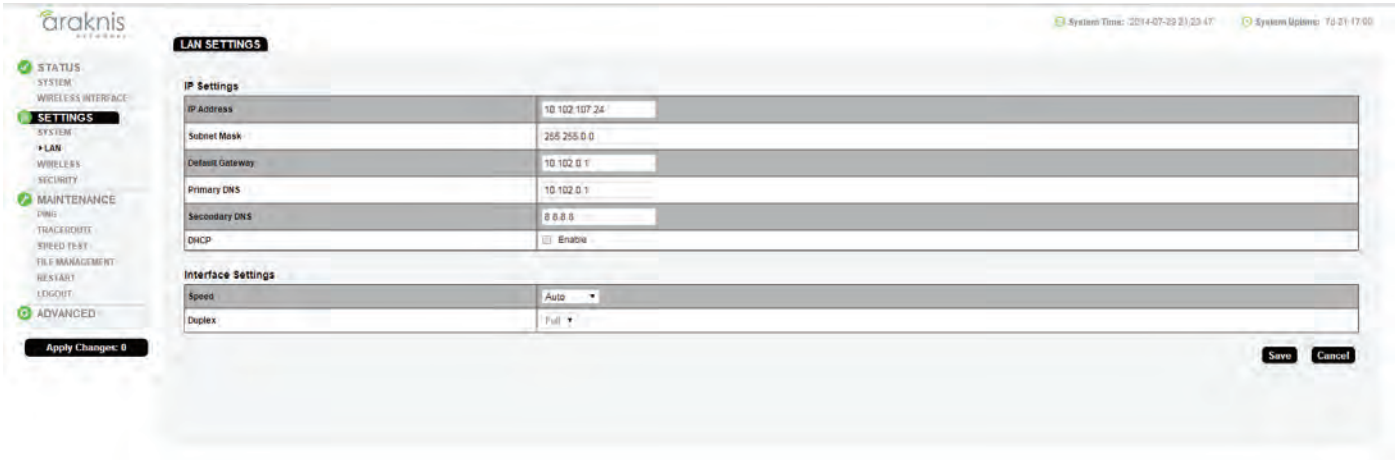
Save/Cancel

- **Save** – Click to save changes to the System Settings. The changes should appear as a numeric value on the Apply Changes button.
- **Cancel** – Click to cancel changes to System Settings.
- **Apply Changes** – Click to apply saved changes to System Settings. The Unsaved Changes List should appear.
- **Apply** – Click Apply at the bottom of the Unsaved Changes List to implement changes.
- **Revert** – Click to cancel Unsaved Changes List. No changes will have been made.
- Navigate to desired AN100/300 setup screen or Exit setup.

2.2. LAN Settings

The LAN Settings screen allows configuration of the AN100/300 LAN connection to the network router. In default mode the IP Settings section will show the DHCP IP Address and default Subnet Mask. A Static IP Address, Subnet Mask, Default Gateway and DNS Settings can be configured by disabling DHCP. LAN speed can be configured in the Interface Settings section.

Figure 15. LAN Settings

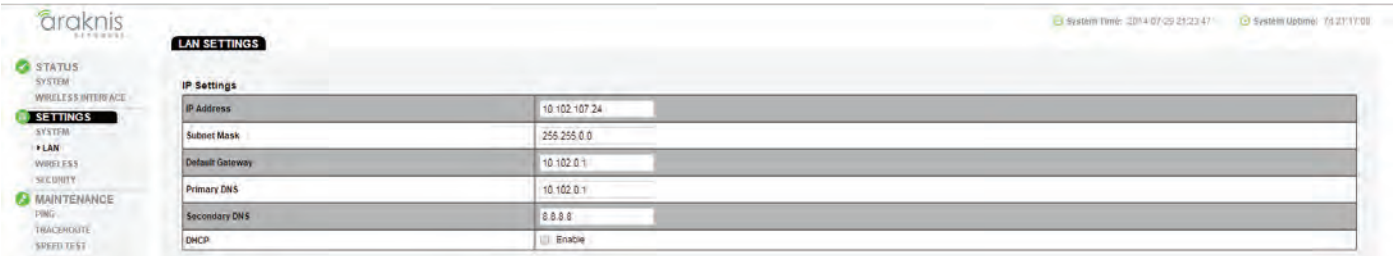


Path Settings, LAN

2.2.1. IP Settings

The IP Settings section allows configuration of the AN100/300 IP Address. In default mode the IP Settings section will show the DHCP IP Address and default Subnet Mask. A Static IP Address, Subnet Mask, Default Gateway and DNS Settings can be configured by disabling DHCP.

Figure 16. IP Settings



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 Static IP Address (and Subnet Mask) will be shown, (grayed out) and the Dynamic Address will be active. To confirm the active AN100/300 IP Address, see: System Status screen/LAN Information/IP Address.

- **IP Address** – Uncheck 'DHCP Enable' to enter a Static IP Address for the AN100/300. Use of a Static (permanent) IP Address is recommended. If using a Static IP Address be sure the Network Router is configured to allow Static IP Addresses and that the IP Address used is within the network address scheme. DEFAULT: 192.168.20.253
- **Subnet Mask** – Enter the Subnet Mask for the AN100/300. DEFAULT: 255.255.255.0
- **Default Gateway** – With DHCP disabled, enter the Default Gateway for the AN100/300 (Network Router IP Address). DEFAULT: Network Router IP Address
- **Primary DNS** – With DHCP disabled, enter the Primary DNS for the AN100/300. This will typically be the Network Router IP Address. DEFAULT: 0.0.0.0

  NOTE: The Primary and Secondary DNS Addresses are required when setting up a Static IP Address.
- **Secondary DNS** – With DHCP disabled, enter the Secondary DNS for the AN100/300. This will typically be the Network Router IP Address. DEFAULT: 0.0.0.0

  NOTE: The Primary and Secondary DNS Addresses are required when setting up a Static IP Address.
- **DHCP** – Select to allow automatic assignment of AN100/300 IP Address via the Network Router. De-select to allow configuration of a Static IP Address. Use of a Static IP Address is recommend for this device. DEFAULT: Enable.

Configuration Instructions

To configure IP Address Settings:

1. Click Settings, LAN.
2. Specify the IP Settings.
3. Click Save.

2.2.2. Interface Settings

The Interface Settings section allows configuration of the AN100/300 LAN Speed and Duplex settings.

Figure 17. Interface Settings

Path Settings, LAN

Parameters

- **Speed** – Select LAN speed from the drop-down. OPTIONS: Auto,1Gbps (300 Series only); 100Mbps; 10Mbps; Disable. (Disable turns the WAN100/300 LAN Port OFF.) DEFAULT: Auto
- **Duplex –** The current negotiated duplex setting between the AN100/300 and Network Router. OPTIONS: Half and Full. DEFAULT: Full

  NOTE: 1Gbps requires and will default to Full Duplex.

Configuration Instructions

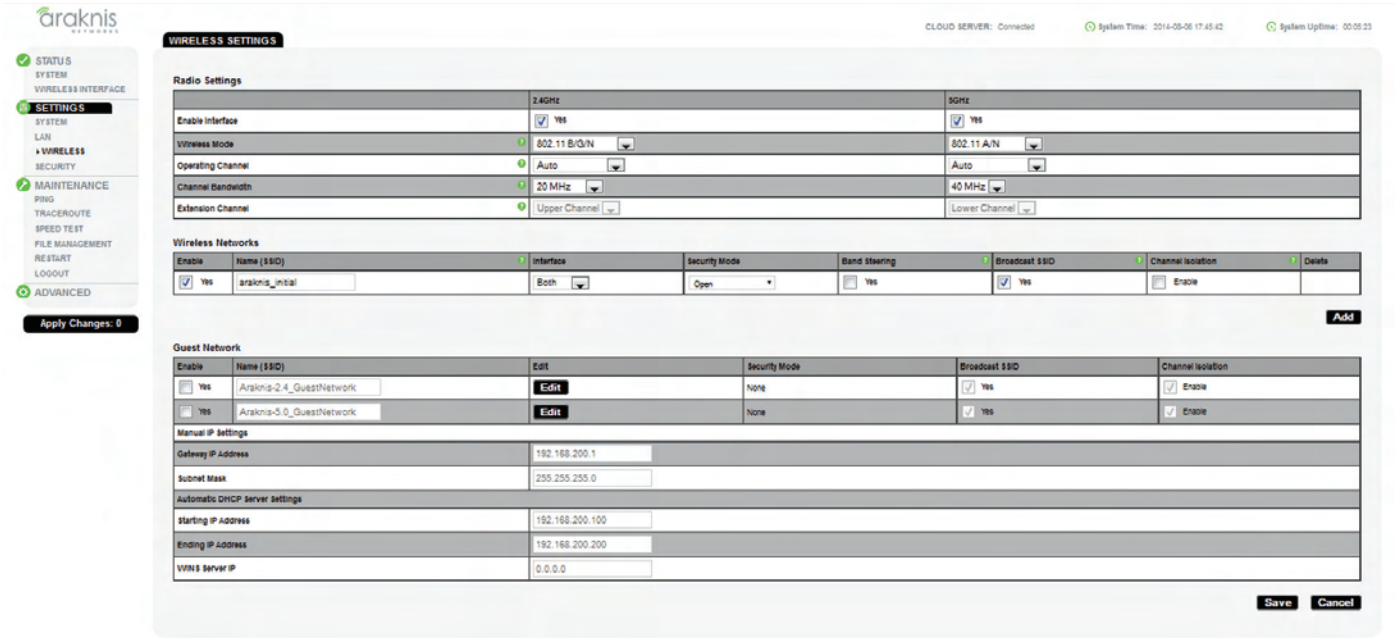
To configure Interface Settings:

1. Click Settings, LAN.
2. Specify the Interface Settings.
3. Click Save.

2.3. Wireless Settings

The Wireless Settings section allows configuration of the AN100/300 wireless settings and connections including 2.4GHz and 5GHz Radio settings, setup and configuration of Wireless Networks (SSIDs) and all required wireless modes, channels, security settings and Guest Network configuration.

Figure 18. Wireless Settings

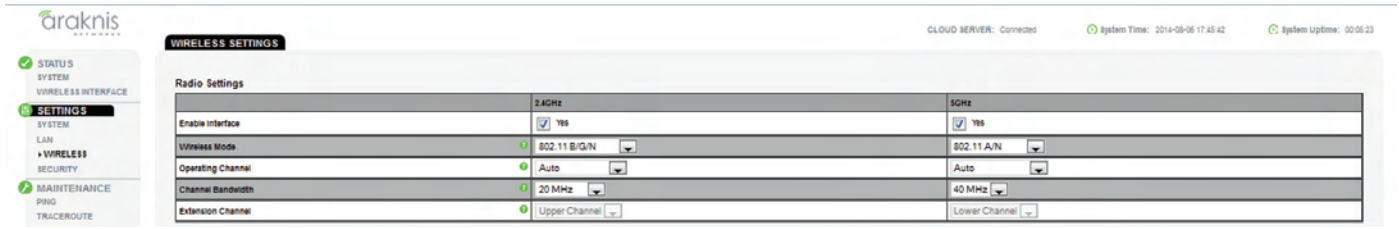


Path Settings, Wireless

2.3.1. Radio Settings

The Radio Settings section allows configuration of the AN100/300 radio settings including wireless modes, operating channels, channel bandwidth and extension channel.

Figure 19. Radio Settings



Path Settings, Wireless

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Enable Interface** – Select Yes to activate the 2.4GHz/5GHz Channel. Each radio interface can be enabled/disabled individually. DEFAULT: Yes.
- **Wireless Mode** – Select the appropriate wireless mode for the 2.4GHz/5GHz band. OPTIONS (2.4GHz): 802.11b/g/n; 802.11b/g; 802.11b; 802.11g; 802.11n (2.4Ghz); OPTIONS (5GHz): 802.11a/n; 802.11a; 802.11n (5GHz). DEFAULT: 2.4GHz - 802.11b/g/n; 5GHz - 802.11a/n.
- **Operating Channel** – Select the desired Wi-Fi Channel. Use a different channel than other APs on the network. Try to select a channel that is as far away from potentially conflicting channels as possible. OPTIONS: See on-screen drop-down. DEFAULT: Auto.

  NOTE: On the 2.4Ghz radio there are only three non-overlapping channels - 1, 6 and 11.

  PRO TIP: The AN100/300 features a Site Survey tool that shows all 2.4GHz/5GHz networks, their channels, signal strengths, etc. Use this tool to scan the wireless neighborhood to determine the channel with the least amount of interference for the AN100/300. See: Advanced Settings/Site Survey.
- **Channel Bandwidth** – Select 20/40MHz for auto select; Select 20MHz for better performance as needed; select 40MHz for greater speed as needed. This option is only available in 802.11n modes. OPTIONS: 40MHz; 20/40MHz; 20MHz. DEFAULT: 2.4GHz - 20MHz; 5GHz - 40MHz.
- **Extension Channel** – If Channel Bandwidth is set to 20/40MHz or 40MHz, the Extension Channel gives the option of extending the 20MHz channel to an upper or lower channel to achieve 40MHz bandwidth. Use the AN100/300 Site Survey, (Advanced Settings/Site Survey) to analyze the wireless neighborhood and select upper or lower depending upon where there is less traffic from other wireless devices. This option is only available when Wireless Mode is set to an 802.11n mode and Channel Bandwidth is set to 20/40MHz or 40MHz. OPTIONS: Upper Channel/Lower Channel; DEFAULT: 2.4GHz - Upper Channel; 5GHz - Lower Channel.

Configuration Instructions

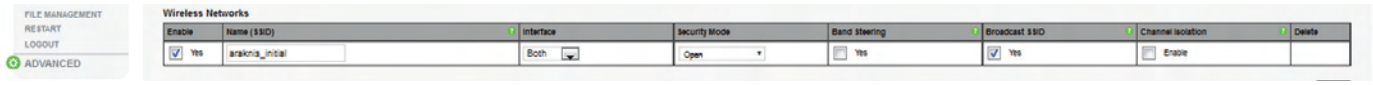
To configure Radio Settings:

1. Click Settings, Wireless.
2. Specify the Radio Settings.
3. Click Save.

2.3.2. Wireless Networks

The Wireless Networks section allows configuration of AN100/300 wireless networks (SSIDs), security settings, band steering and channel isolation.

Figure 20. Wireless Networks



Path Settings, Wireless

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Enable** – Select Yes to turn a Wireless Network ON. DEFAULT: Selected.
- **Name (SSID)** – Enter the network name for the specific network being configured. DEFAULT: araknis_initial; (Blank when adding a network).
- **Interface** – Select 2.4GHz/5GHz or Both Channel Frequency. OPTIONS: 2.4GHz, 5GHz, Both. 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 window.

  Wireless Security (All Modes)

  1. **Name (SSID)** – The network name of the network being configured
  2. **Security Mode** – Select a Security Mode from the drop-down. Use the same Security Mode used by the network router and all other APs on the same network. OPTIONS: Open; WPA2-PSK; WPA2-PSK Mixed; WPA2; WPA Mixed. DEFAULT: Open
  3. **Encryption** – The Encryption Mode will default to the Security Mode selected. DEFAULTS: WPA2-PSK will default to AES; WPA2-PSK Mixed will default to Both (TKIP+AES); WPA2 will default to AES; WPA Mixed will default to Both (TKIP+AES).
  4. **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
  5. **Group Key Update Interval** – Enter a value to specify how often in seconds the Group key changes. RANGE: 30-3600. DEFAULT: 3600 (60 minutes)
  6. **Save** – Click to save changes to the Wireless Security Settings for this network. The window will close. The changes should appear as a numeric value on the Apply Changes button. Proceed with setup if additional changes are required, or proceed to Save/Cancel at the end of this section.
  7. **Cancel** – Click to cancel changes to the Wireless Security Settings for this network. The window will close. Proceed with setup if additional changes are required.

  If using WPA2 or WPA2 Mixed:

  8. **Radius Server** – Enter the Radius Server IP Address. DEFAULT: Blank
  9. **Radius Port** – Enter the Radius Server connection port number. This is a dedicated TCP/UDP port and would typically not be changed. DEFAULT: 1812
  10. **Radius Secret** – Enter the Radius Server connection secret. DEFAULT: Blank
  11. **Radius Accounting** – Select Enable to enable Radius accounting. Select Disable to disable Radius Accounting. DEFAULT: Disable
  12. **Radius Accounting Server** – Enter the Radius Accounting Server IP Address. DEFAULT: Blank
  13. **Radius Accounting Port** – Enter the Radius Accounting Server connection port number. This is a dedicated TCP/UDP port and would typically not be changed. DEFAULT: 1813
  14. **Radius Accounting Secret** – Enter the Radius Accounting Server connection secret. DEFAULT: Blank

15. **Interim Accounting Interval** – Enter a value for how often the accounting data will be sent, in seconds. RANGE: 60-600. DEFAULT: 600 (10 minutes)
16. **Save** – Click to save changes to the Wireless Security Settings for this network. The window will close. The changes should appear as a numeric value on the Apply Changes button. Proceed with setup if additional changes are required, or proceed to Save/Cancel at the end of this section.
17. **Cancel** – Click to cancel changes to the Wireless Security Settings for this network. The window will close. Proceed with setup if additional changes are required.

- **Broadcast SSID** – Select Yes to have the SSID appear on wireless devices for connectivity. DEFAULT: Yes
- **Band Steering** – Enable Band Steering to assign 802.11n clients to the 5GHz band and 802.11b/g clients to the 2.4GHz band. This will relieve the traffic on both bands and provide better service to all affected clients. Band Steering works within the Access Point by directing 5GHz capable clients to the 5GHz band. The SSID and Security Settings must be the same in both the 2.4Ghz and 5GHz bands to have Band Steering work properly.
- **Channel Isolation** – Select to prevent communication between wireless clients on the same network. DEFAULT: Not selected.
- **Add** – Click the Add button to add a Wireless Network.
- **Delete** – Click the Trash icon to delete a Wireless Network.

Configuration Instructions

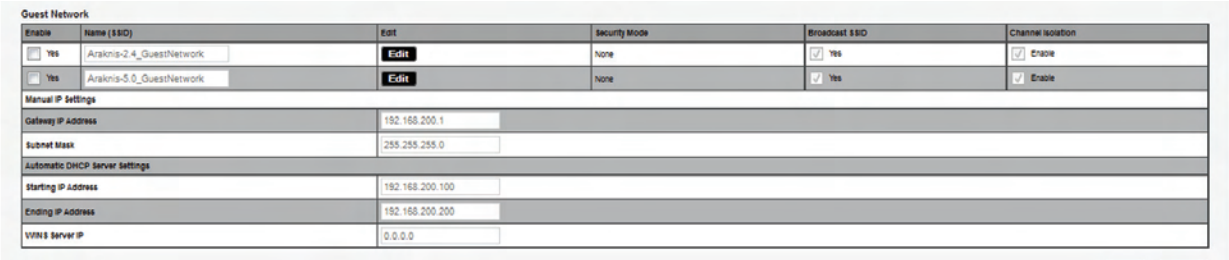
To configure Wireless Networks:

1. Click Settings, Wireless.
2. Specify the Wireless Network Settings.
3. Click Save.

2.3.3. Guest Network

The Guest Network section allows configuration of the AN100/300 Guest Network SSID settings for 2.4GHz/5GHz interface, security modes. Manual Guest Network Wireless IP Settings and Automatic DHCP Server settings can also be configured in this section.

Figure 21. Guest Network



Path Settings, Wireless

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Enable** – Select to create a Guest Network. This will allow guests to log in to the wireless system without having to compromise network security by giving guests the password to the home network. There are separate 2.4GHz and 5GHz Guest Networks. If the guest is using an 802.11b/g device, (2.4GHz) they will only need the password to the 2.4GHz Network. If the guest is using an 802.11b/g/n device (5GHz) they will need the password to the 5GHz Network, and if the guest is using a device that can connect on both 2.4GHz and 5GHz, (iOS devices) they should have both, particularly if Band Steering has been enabled, (see previous section). DEFAULT: Not Selected.
- **SSID** – Enter an SSID for the Guest Network. DEFAULTS: Araknis-2.4_GuestNetwork; Araknis-5.0_GuestNetwork
- **Edit** – Click the Edit button to open the Guest Network Security Setup Window.
    1. **Security Mode** – Select a Security Mode from the drop-down. Use the same Security Mode used by the network router and all other APs on the same network. Leaving the Security Mode 'Open' is not recommended. OPTIONS: Open, WPA2-PSK, WPA2-PSK Mixed. DEFAULT: Open
    2. **Encryption** – The Encryption Mode will default to the Security Mode selected. DEFAULTS: WPA2-PSK will default to AES; WPA2-PSK Mixed will default to TKIP+AES.
    3. **Passphrase** – Enter the appropriate password for the Guest Network. 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
    4. **Group Key Update Interval** – Enter a value to specify how often in seconds the Group key changes. RANGE: 30-3600. DEFAULT: 3600 (60 minutes)
- **Security Mode** – This indicates the Security Mode and Encryption selected in the Edit Mode, previous. DEFAULT: None
- **Broadcast SSID** – Selecting this option will allow the Guest Network SSID to appear in 'Network Lists' on wireless devices for user login. If not selected, the user will have to know the SSID and enter it manually to access the network. DEFAULT: Un-selected.
- **Client Isolation** – Select to prevent communication between wireless clients on the Guest Network. DEFAULT: Selected.
- **Manual IP Settings** – If the network router allows setup of subnets or VLANs, use the AN100/300 defaults or manually enter IP Address settings that conform to the network router capability. If the network router does not allow subnets, use IP Address settings from the IP Address scheme currently set on the network router.
    1. **Gateway IP Address** – Enter the AN100/300 Guest Network Gateway IP Address. DEFAULT: 192.168.200.1
    2. **Subnet Mask** – Enter the Subnet Mask for the AN100/300 Guest Network Gateway. DEFAULT: 255.255.255.0

- **Automatic DHCP Server Settings**
    1. **Starting IP Address** – Enter the lowest address available for the Guest Network. DEFAULT: 192.168.200.100
    2. **Ending IP Address** – Enter the highest address available for the Guest Network. DEFAULT: 192.168.200.200
    3. **WINS Server IP** – Enter the IP Address for the WINS Server for the Guest Network. DEFAULT: 0.0.0.0

Configuration Instructions

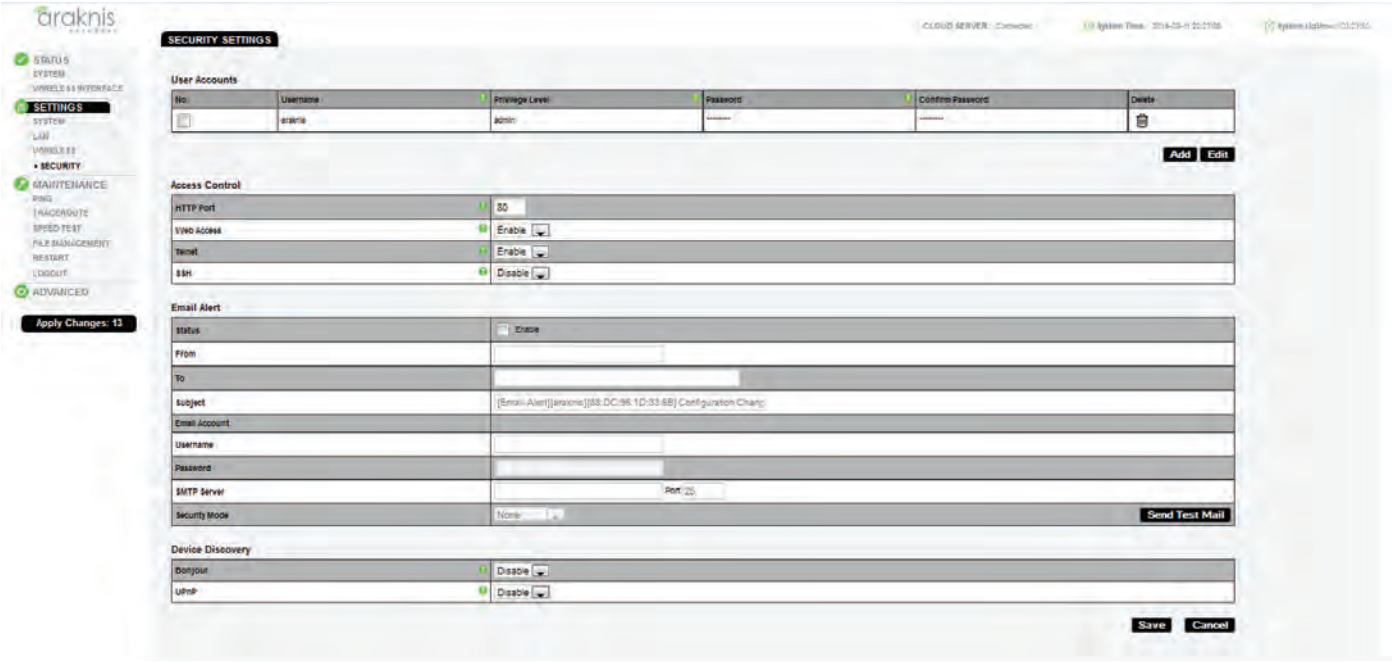
To configure Guest Network:

1. Click Settings, Wireless.
2. Specify the Guest Network Settings.
3. Click Save.

2.4. Security Settings

The Security Settings section allows configuration of who can login to the AN100/300 and what level of privileges they have, how the device can be accessed, email notification of system status and warnings and device discovery.

Figure 22. Security Settings

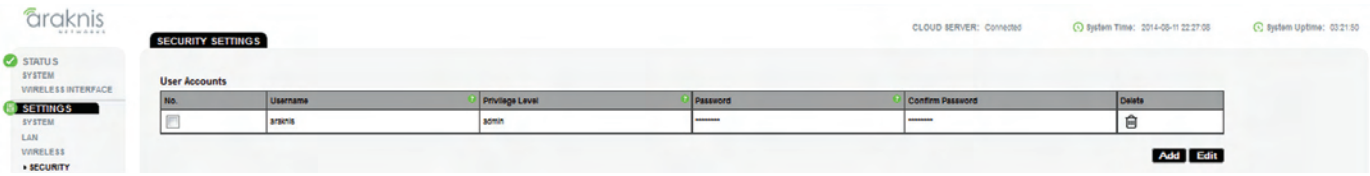


Path Settings, Security

2.4.1. User Accounts

The User Accounts section allows configuration of who can login to the AN100/300 and what level of privileges they have.

Figure 23. User Accounts



Path Settings, Security

Parameters

- **Select** – Select to allow editing of the selected table entry. DEFAULT: Not selected.
- **User Name** – Click the Edit button to allow access to the settings on a selected User Account. Enter the login Username for the selected account. 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 password for user login. DEFAULT: araknis; (Blank when adding a new account.)
- **Confirm Password** – Re-enter the password for the logged in user to confirm. DEFAULT: araknis; (Blank when adding a new account.)
- **Delete** – Click the Delete icon to delete a specific User Account. Click the Save button to save the change. Refresh the screen to see the change.

Configuration Instructions

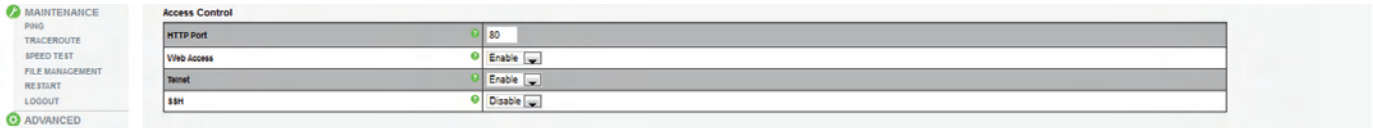
To configure User Accounts:

1. Click Settings, Security.
2. Specify the User Account Settings.
3. Click Save.

2.4.2. Access Control

The Access Control section allows configuration of how the AN100/300 can be accessed.

Figure 24. Access Control



Path Settings, Security

Parameters

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

  PRO TIP: A port number, other than the default, can be assigned to enable remote access to the AN100/300 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 lost connectivity to the AN100/300 web interface. If this should occur, the only way to regain this connectivity is to restore the hardware factory default settings. (Press AN100/300 Reset button for 10 seconds.)

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

Configuration Instructions

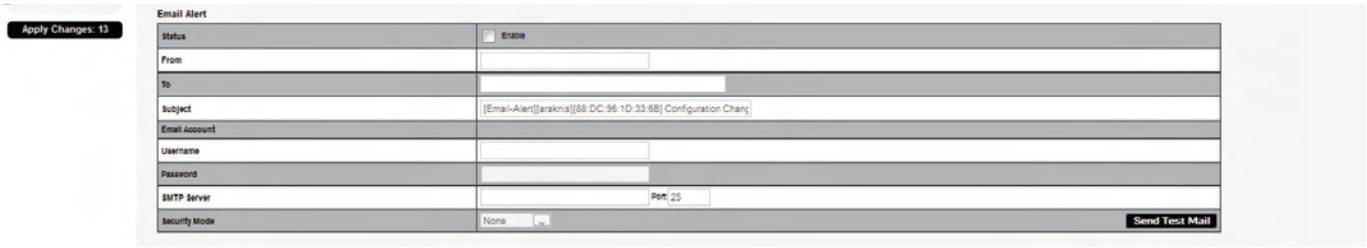
To configure Access Control:

1. Click Settings, Security.
2. Specify the Access Control Settings.
3. Click Save.

2.4.3. Email Alert

The Email Alert section allows configuration of the AN100/300 email notification system for status and warnings.

Figure 25. Email Alert



Path Settings, Security

Parameters

- **Status** – Select Enable to have the AN100/300 send notifications to a specific email address 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**

  User Name – Enter the User Name for the Email Account (Outlook, Gmail, etc) to be used to send the Email Alert. DEFAULT: Blank

  Password – Enter the Password for the Email Account (Outlook, Gmail, etc) to be used to send the Email Alert.

  DEFAULT: Blank

  SMTP Server – Enter the SMTP Server and Port Number of the Email Client (Outlook, Gmail, etc) to be used to send the Email Alert. DEFAULTS: SMTP Server Blank; Port: 25

  Security Mode – Select a security mode for sending Email Alerts. OPTIONS: None, SSL/TLS, STARTTLS DEFAULT: None

  Send Test Email – Click this button to send a test email to confirm Email Alert settings.

Configuration Instructions

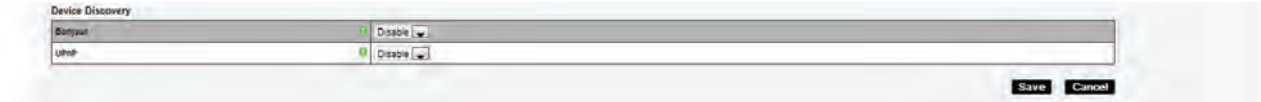
To configure Email Alert:

1. Click Settings, Security.
2. Specify the Email Alert Settings.
3. Click Save.

2.4.4. Device Discovery

The Device Discovery section allows configuration of how or if the AN100/300 can search for and connect to network devices via Bonjour and UPnP.

Figure 26. Device Discovery



Path Settings, Security

Parameters

- **Bonjour** – Enable to allow the AN100/300 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 AN100/300 to search for and connect to network devices via UPnP Protocol (Universal Plug and Play). DEFAULT: Disable

Configuration Instructions

To configure Device Discovery:

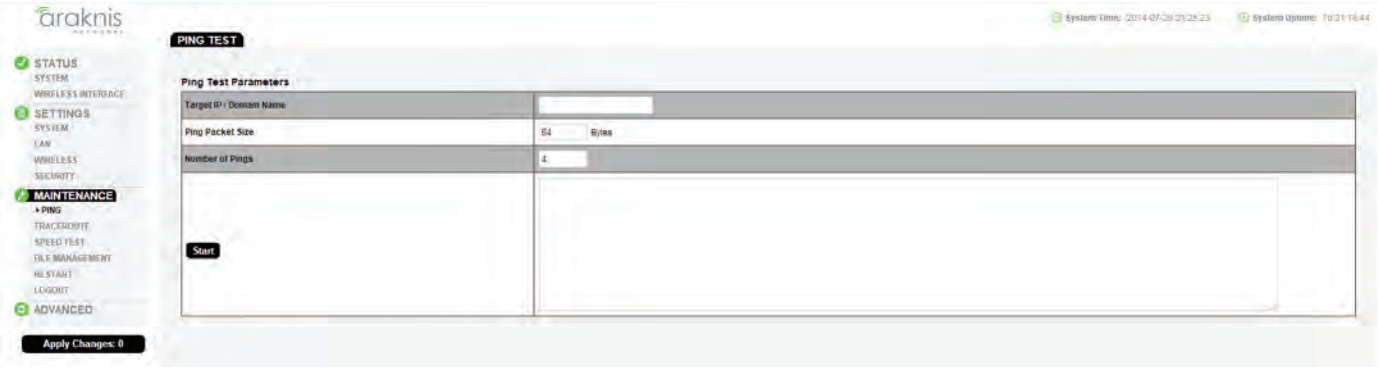
1. Click Settings, Security.
2. Specify the Device Discovery Settings.
3. Click Save.

3. Maintenance

3.1. Ping Test

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

Figure 27. 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. 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

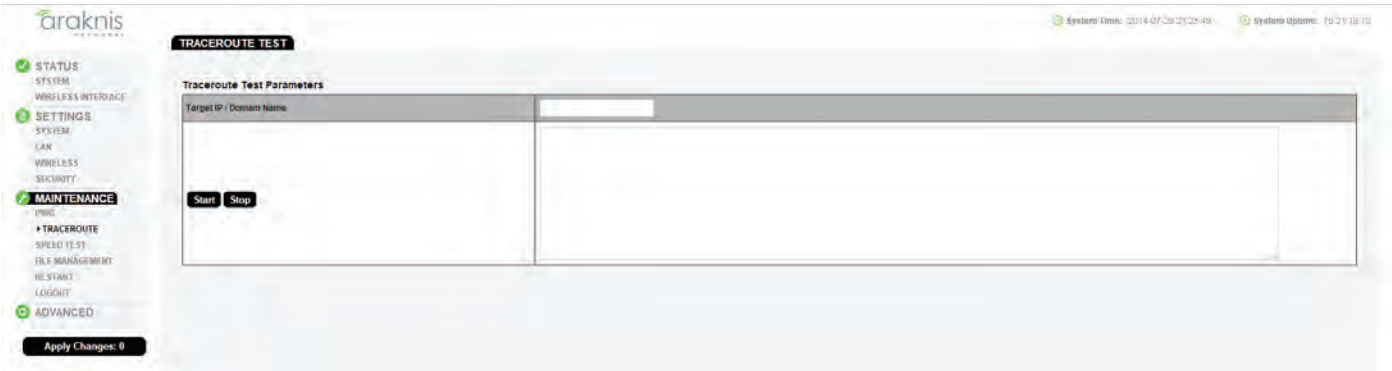
To run Ping Test:

1. Click Maintenance, Ping.
2. Specify the Ping Test Settings.
3. Click Start.

3.2. Traceroute Test

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

Figure 28. Traceroute Test Parameters



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

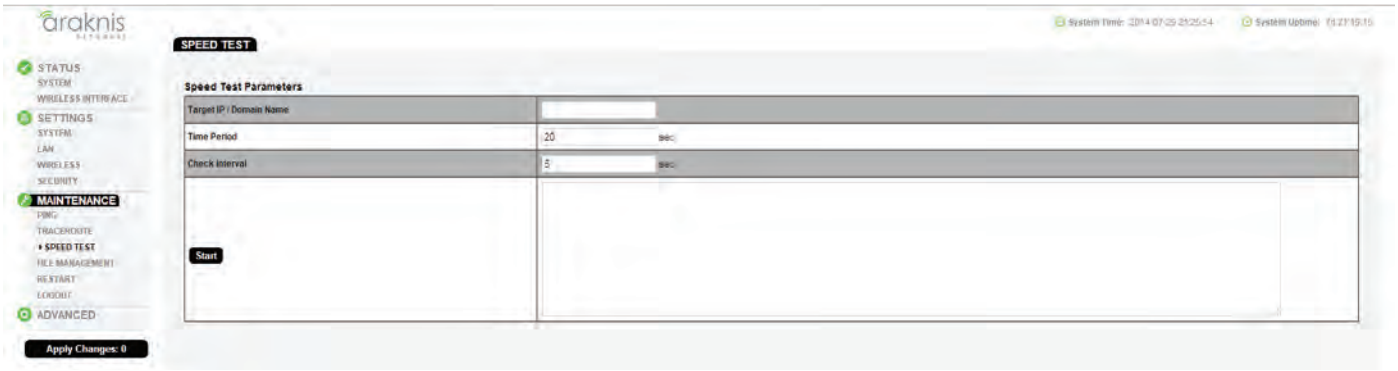
To configure Traceroute Test:

1. Click Maintenance, Traceroute.
2. Specify the Traceroute Test Settings.
3. Click Start.
4. Click Stop to end test.

3.3. Speed Test

The Speed Test can be used to determine the upload/download speed between two devices on an IP network.

Figure 29. Speed Test Parameters



Path Maintenance, Speed Test

Parameters

- **Target IP / Domain Name** – Enter the IP Address of a device or web page to test the upload/download speed to/from that device or website.
- **Time Period** – Enter the duration of the test in seconds. DEFAULT: 20 seconds
- **Check Interval** – Enter the time in seconds between each test. DEFAULT: 5 seconds
- **Start** – Click the Start button to start the speed test. Exit the screen to stop.

Configuration Instructions

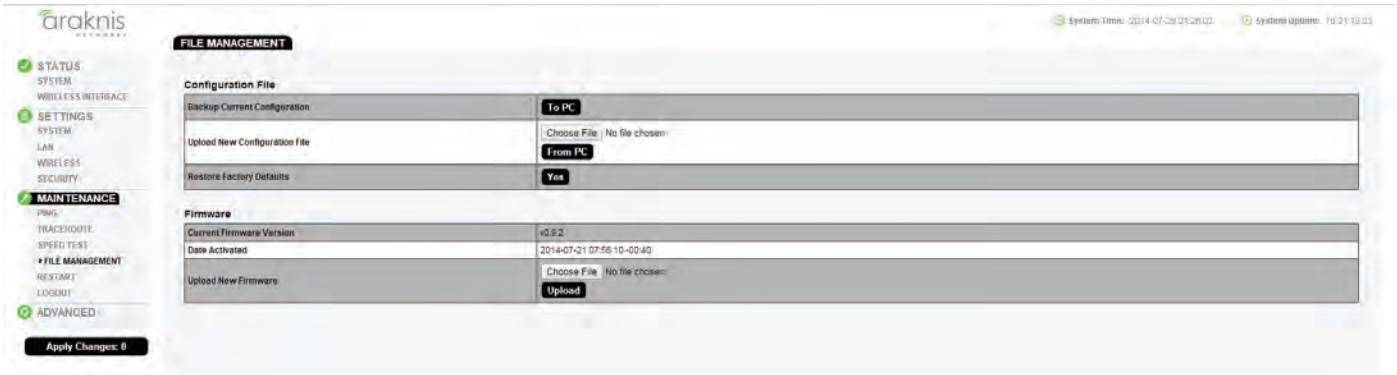
To configure Speed Test:

1. Click Maintenance, Speed Test.
2. Specify the Speed Test Settings.
3. Click Start.

3.4. File Management

The File Management screen facilitates simple AN100/300 configuration backup and firmware updates.

Figure 30. File Management



Path Maintenance, File Management

3.4.1. Configuration File

The Configuration File section facilitates simple AN100/300 configuration backup and restoring factory defaults.

Figure 31. File Management

Path Maintenance, File Management

3.4.1.1. Backup Current Configuration

Configuration Instructions

To save current configuration settings:

1. Click the To PC button to save the current configuration of the AN100/300. The file will save to the Downloads Folder.
2. Look for a file with a name similar to: ‘backup-AN300-YEAR-MONTH-DATE.tar.gz’. It is suggested that the file be moved to a folder containing all of the documentation for a specific project, or other easy to remember location.

3.4.1.2. Upload New Configuration File

Configuration Instructions

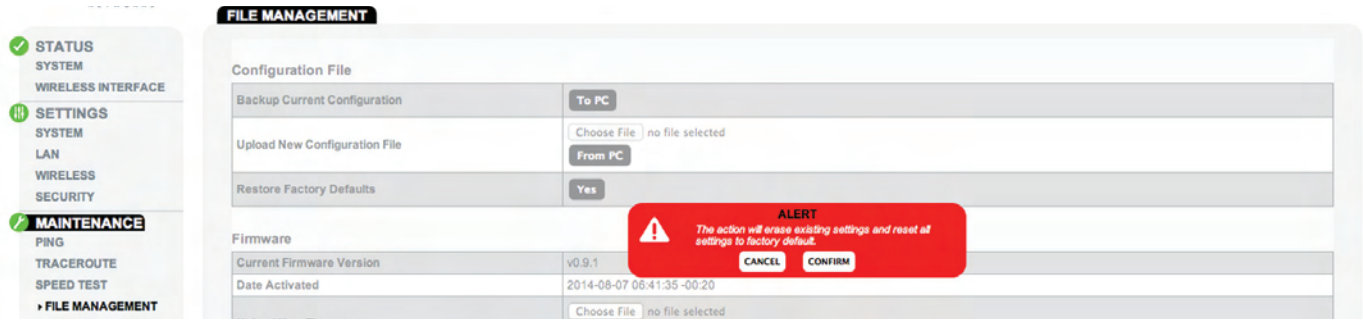
Use the Upload Configuration File option to restore previously saved configuration settings to the AN100/300 from your local management station.

1. Click the Browse button to navigate to where the configuration file is saved.
2. Press Enter/Return on the computer keyboard or click Open on the Upload Screen to select the file. (The Configuration File name should appear next to the Upload New Configuration File Browse Button.)
3. Click From PC to upload the configuration file. Please wait while the Rebooting screen is open and loading the selected configuration. When the configuration upload is finished the Authentication Required (Login) window will open.
4. Enter the User Name and Password.
5. Confirm Configuration settings.

3.4.1.3. Restore Factory Defaults

The File Management screen facilitates restoring original AN100/300 factory settings. Note that the IP Address, Subnet Mask and Gateway IP Address will be reset to their factory defaults.

Figure 32. 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.

1. Click the Yes button to restore the AN100/300 to factory default settings. The red Alert! message will appear.
2. Click Cancel to cancel. Click Confirm to Restore Factory Defaults. Please wait while the Rebooting screen is open and loading the selected configuration. When the configuration upload is finished the Authentication Required (Login) window will open.
3. Enter the User Name and Password.
4. Confirm Configuration settings.

3.4.1.4. Hardware Factory Default

If restoring factory defaults does not restore proper functionality to the AN100/300, a hardware reset may be performed to reload the original base configuration file (saved in the AN100/300 memory).

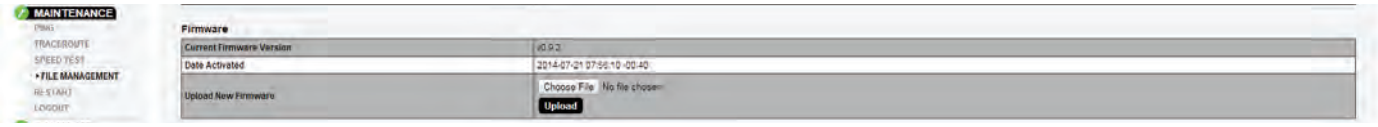
Configuration Instructions

1. Using a paper clip or other small blunt tool press the reset button located on the top of the AN100/300 for approx 30 seconds.
2. Restart the setup process or upload a previously saved configuration.

3.4.1.5. Firmware

The Firmware section facilitates uploading new firmware to the AN100/300.

Figure 33. Firmware



Path Maintenance, File Management, Firmware

Parameters

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

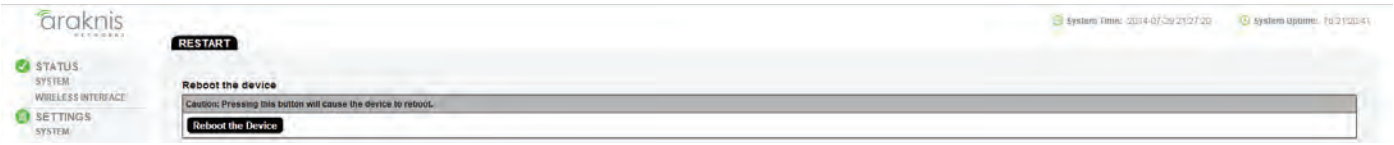
Configuration Instructions

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 Screen. (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. Please wait while the new firmware loads. When the configuration upload is finished the Authentication Required (Login) window will open.
5. Enter the User Name and Password.
6. Confirm Firmware version.

3.5. Restart

In the unlikely event that the AN100/300 locks up or has otherwise become unresponsive, it can be rebooted to return it to its previous, normal operating state.

Figure 34. Restart



Path Maintenance, Restart

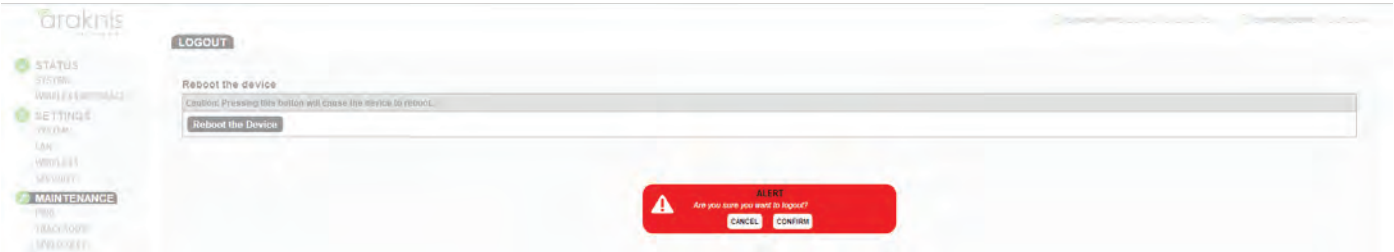
Configuration Instructions

1. Click the Reboot the Device button. The ‘This will reboot the device and may take a few seconds’ message will appear.
2. Click OK to reboot; Click Cancel to return to the Restart Screen.
3. Please wait while the AN100/300 reboots. When the device has rebooted, the Authentication Required (Login) window will open.
4. Enter the User Name and Password.
5. Confirm Firmware and configuration.

3.6. Logout

Logout can be used to change the user currently logged in to AN100/300 setup. When finished working in the AN100/300 set-up screens, a logged in user can simply close the Browser Tab with the AN100/300 Setup or Logout. Closing the Browser Tab will close setup screen completely, Logout will end the session for the logged in user and open the Authentication Required (Login) window.

Figure 35. Logout Alert



Path Maintenance, Logout

Configuration Instructions

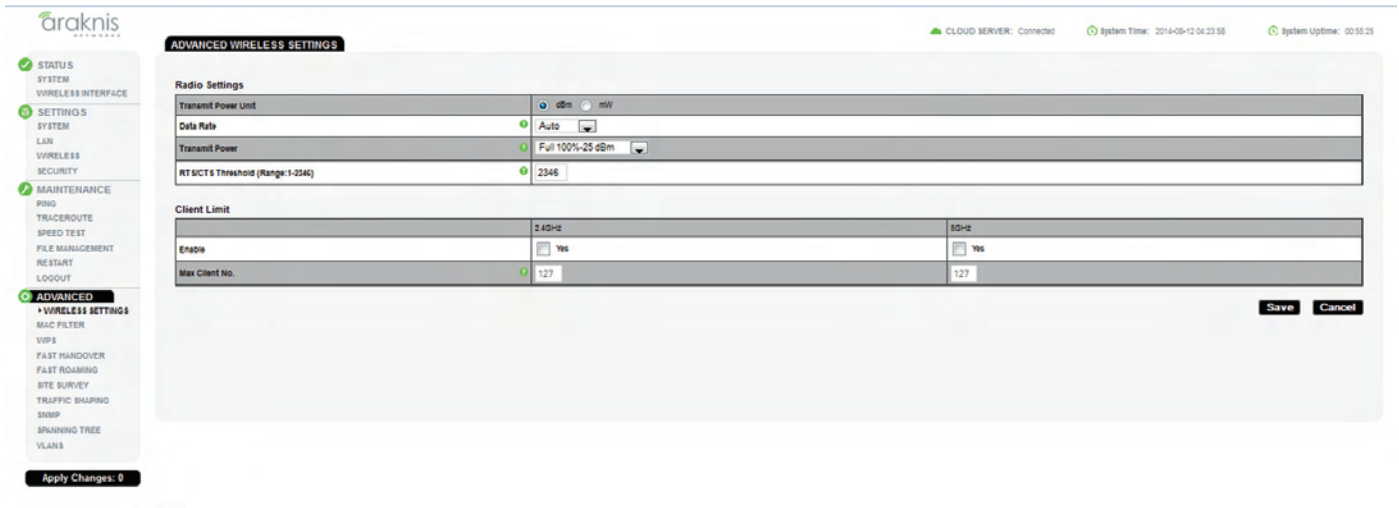
1. From any screen click Logout in the system menu. The Logout Alert! will appear on screen.
2. Click Cancel to return to the setup screen; click Confirm to Logout the current user.

4. Advanced

4.1. Advanced Wireless Settings

The Advanced Wireless Settings section allows configuration of AN100/300 radio settings for unit of measure, data rate, power and RTS/CTS Threshold as well as a client limit by band, (2.4GHz/5GHz).

Figure 36. Advanced Wireless Settings



Path Advanced, Wireless Settings

4.1.1. Radio Settings

The Advanced Wireless Settings section allows configuration of AN100/300 radio settings for unit of measure, data rate, power and RTS/CTS Threshold.

Figure 37. 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 AN100/300 radio power. Increasing the power should improve performance, but can cause interference with other access points in close range that are on the same channel. OPTIONS: See drop-down list. DEFAULT: Full 100% -25dBm.
- **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

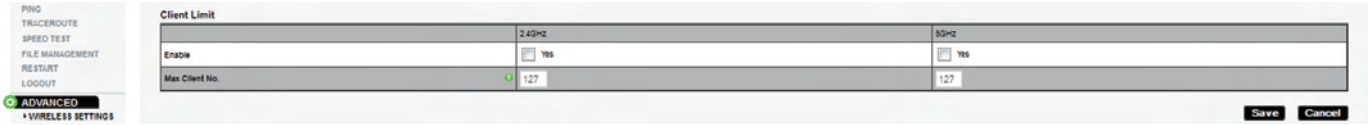
To configure Radio Settings:

1. Click Advanced, Wireless Settings.
2. Specify the Radio Settings.
3. Click Save.

4.1.2. Client Limit

The Advanced Wireless Settings section allows configuration of AN100/300 client limit by band, (2.4GHz/5GHz).

Figure 38. Client Limit Settings



Path Advanced, Wireless Settings, Client Limit

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Enable** – Select to enable Client Limit, by channel. DEFAULT: Not Selected.
- **Max Client No.** – Set the maximum number of clients that can be connected to a channel at a given time. (For WAP300, the maximum number of clients is for each channel.) RANGE: 1-127. DEFAULT: 127.

Configuration Instructions

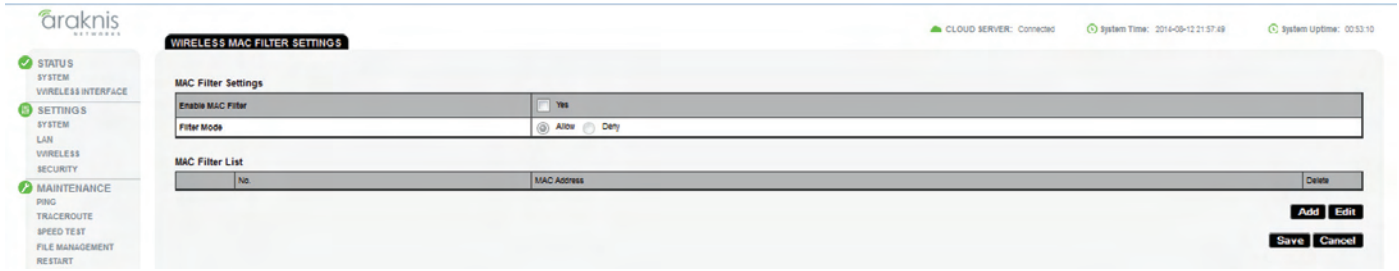
To configure Client Limit:

1. Click Advanced, Wireless Settings.
2. Specify the Client Limit Settings.
3. Click Save.

4.2. Wireless MAC Filter Settings

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

Figure 39. Wireless MAC Filter Settings



Path Advanced, MAC Filter

4.2.1. MAC Filter Settings

The MAC Filter Settings section enables/disables AN100/300 Wireless MAC Filtering.

Figure 40. MAC Filter Settings

Path Advanced, MAC Filter

Parameters

- **Enable MAC Filter** – Select 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

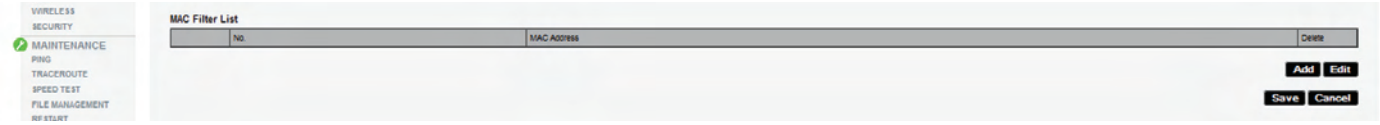
To configure Wireless MAC Filter:

1. Click Advanced, MAC Filter.
2. Specify the Wireless MAC Filter Settings.
3. Click Save.

4.2.2. MAC Filter List

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

Figure 41. MAC Filter Settings



Path Advanced, MAC Filter

Parameters

- **Check Box** - Select to enable MAC Filtering for a given wireless client.
- **No.** – The client number for a device being filtered by MAC Address. DEFAULT: Not Available if MAC Filtering not enabled; client number 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.
- **Edit** – Click to edit an existing client.

Configuration Instructions

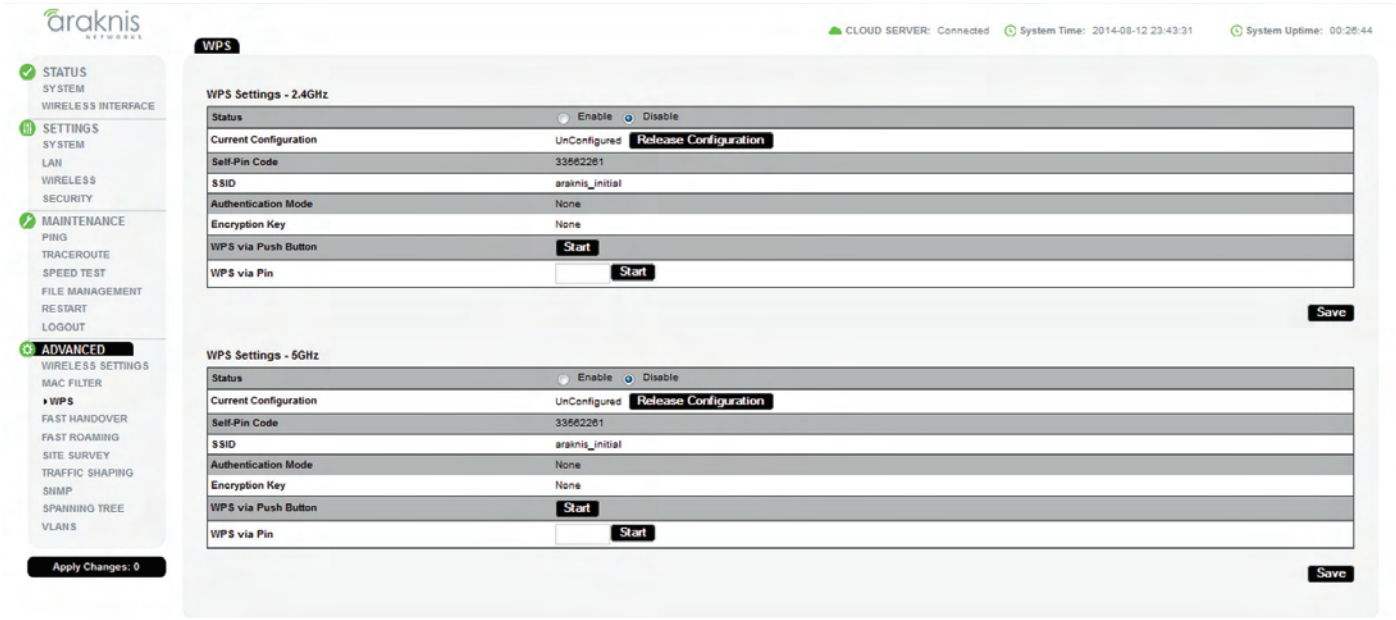
To configure MAC Filter List:

1. Click Advanced, MAC Filter.
2. Specify the MAC Filter Settings.
3. Click Save.

4.3. WPS Settings

WPS (Wi-Fi Protected Setup) is a standard of the Wi-Fi Alliance that allows quick and easy connection of wireless clients with a reduced overall setup requirement of network security settings.

Figure 42. WPS Settings

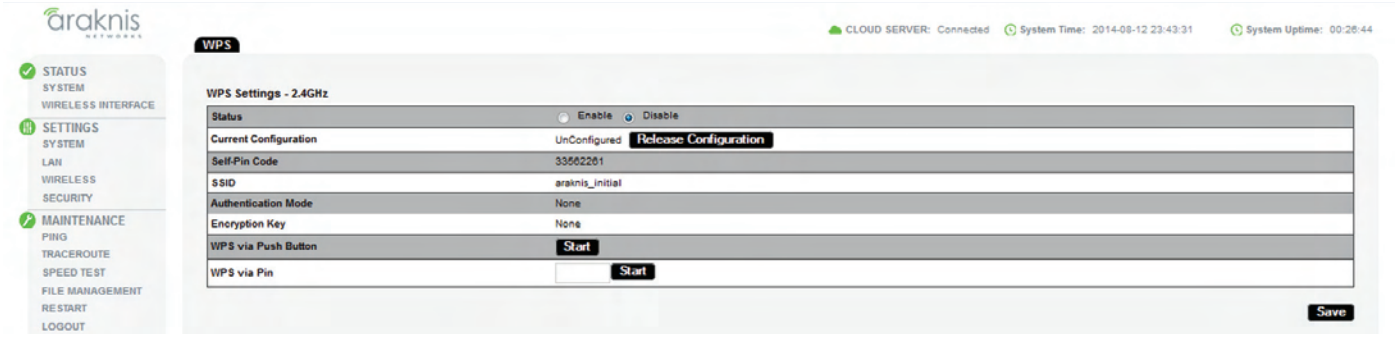


Path Advanced, WPS

4.3.1. WPS Settings - 2.4Ghz

The WPS Settings (2.4GHz) section can be used to configure WPS for wireless 2.4GHz clients.

Figure 43. WPS Settings - 2.4GHz



Path Advanced, WPS, WPS Settings - 2.4GHz

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Status** – Select Enable to enable WPS. Select Disable to disable WPS. DEFAULT: Disable.
- **Current Configuration** – Indicates whether WPS is Configured or Unconfigured. OPTIONS: Configured, Unconfigured. DEFAULT: Unconfigured.
- **Self-Pin Code** – The AN100/300 PIN Code. DEFAULT: Unique per AN100/300.
- **SSID** – Indicates the wireless network name for the WPS enabled network. DEFAULT: araknis_initial
- **Authentication Mode** – Indicates the Authentication Mode by WPS. DEFAULT: None
- **Encryption Key** – The password randomly generated by WPS to authenticate wireless client connection.
- **WPS via Push Button** – Click Start to initiate WPS via the on-screen push button.
- **WPS via PIN** – Enter the wireless device PIN code then click Start to initiate WPS.

Configuration Instructions

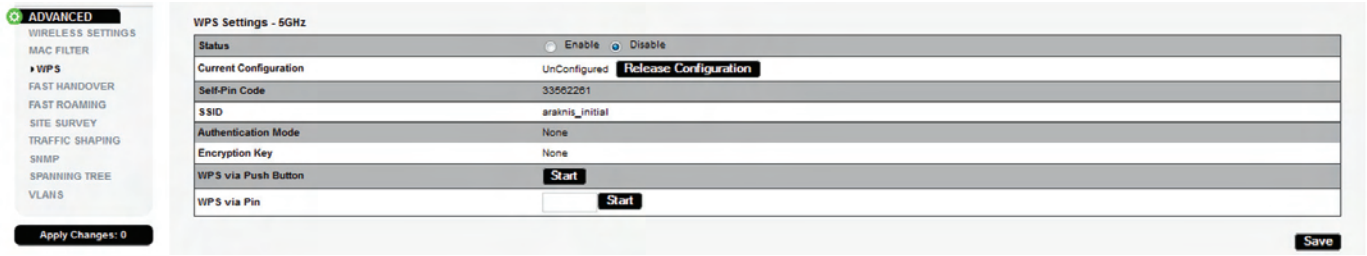
To configure WPS Settings (2.4GHz):

1. Click Advanced, WPS.
2. Specify the WPS Settings (2.4GHz).
3. Click Save.

4.3.2. WPS Settings - 5Ghz

The WPS Settings (5GHz) section can be used to configure WPS for wireless 5GHz clients.

Figure 44. WPS Settings



Path Advanced, WPS, WPS Settings - 5Ghz

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Status** – Select Enable to enable WPS. Select Disable to disable WPS. DEFAULT: Disable.
- **Current Configuration** – Indicates whether WPS is Configured or Unconfigured. OPTIONS: Configured, Unconfigured. DEFAULT: Unconfigured.
- **Self-Pin Code** – The AN100/300 PIN Code. DEFAULT: Unique per AN100/300.
- **SSID** – Indicates the wireless network name for the WPS enabled network. DEFAULT: araknis_initial
- **Authentication Mode** – Indicates the Authentication Mode by WPS. DEFAULT: None
- **Encryption Key** – The password randomly generated by WPS to authenticate wireless client connection.
- **WPS via Push Button** – Click Start to initiate WPS via the on-screen push button.
- **WPS via PIN** – Enter the wireless device PIN code then click Start to initiate WPS.

Configuration Instructions

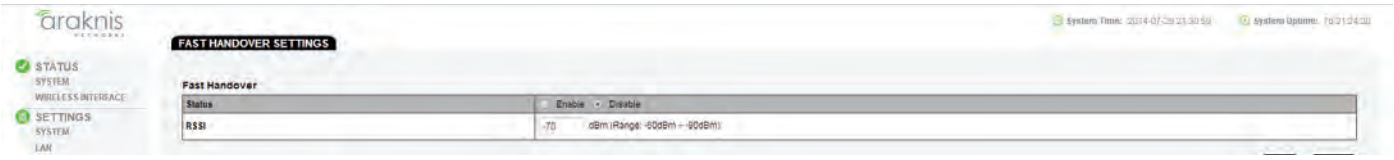
To configure WPS Settings (5Hz):

1. Click Advanced, WPS.
2. Specify the WPS Settings (5GHz).
3. Click Save.

4.4. Fast Handover Settings

On a wireless network with multiple access points, as a wireless client moves from one area to another, the RSSI (wireless signal strength) may drop to a less than optimal level. If enabled, Fast Hanover will detect the condition and send a disassociation request to the wireless client, allowing the client to search for another access point with a stronger signal.

Figure 45. Fast Handover Settings



Path Advanced, Fast Handover

Parameters

- **Status –** Select Enable to enable Fast Handover. Select Disable to disable Fast Handover. DEFAULT: Disable.
- **RSSI –** With Fast Handover enabled, enter a value for the signal strength that will trigger Fast Handover. Lowering the threshold will allow more clients to stay connected, but setting the level too low will cause more frequent re-connections. RANGE: -60dBm to -90dBm. DEFAULT: -70dBm.

Configuration Instructions

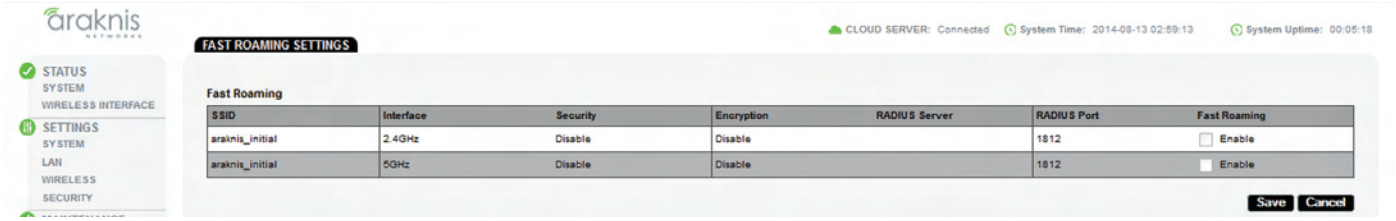
To configure Fast Handover:

1. Click Advanced, Fast Handover.
2. Specify the Fast Handover Settings.
3. Click Save.

4.5. Fast Roaming Settings

On a wireless network with multiple access points, as a wireless client moves from one coverage area to another, the wireless client may need to change access points. If enabled, Fast Roaming identifies other APs on the wireless network, determines which will provide the best and fastest connection for a particular wireless client as it moves between AP coverage areas. Fast Roaming 'pre-approves' the client and the APs to assure a constant connection for the client to the wireless network.

Figure 46. Fast Roaming Settings



Path Advanced, Fast Roaming

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **SSID** – Indicates the network name for the wireless network to which Fast Roaming is being applied. DEFAULT: araknis_initial.
- **Interface** – Indicates the 2.4GHz or 5GHz Interface.
- **Security** – Indicates the security mode selected for this wireless network in the Wireless Settings Screen under Wireless Networks. DEFAULT: Disabled.
- **Encryption** – Indicates the encryption mode selected for this wireless network in the Wireless Settings Screen under Wireless Networks. The encryption mode will default to the selected security mode. DEFAULT: Disabled.
- **Radius Server** – Enter the Radius Server IP Address. DEFAULT: Blank
- **Radius Port** – Enter the Radius Server connection port number. This is a dedicated TCP/UDP port and would typically not be changed. DEFAULT: 1812
- **Fast Roaming** – Select Enable for the 2.4GHz and/or 5GHz Interface to enable Fast Roaming.

Configuration Instructions

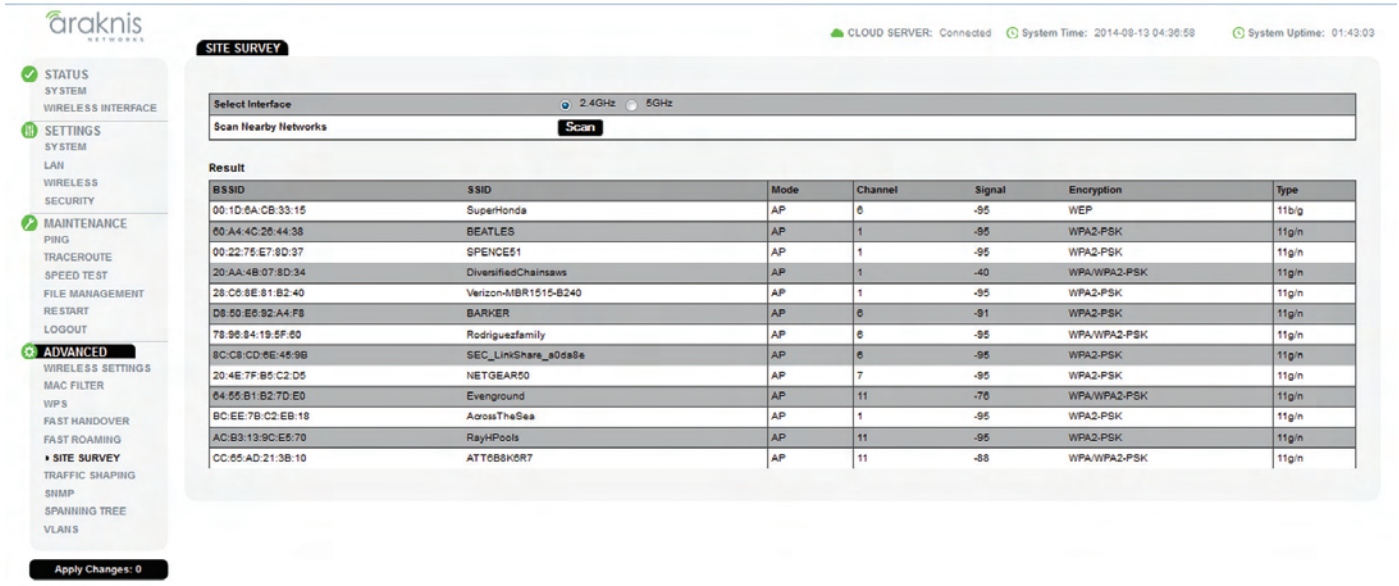
To configure Fast Roaming:

1. Click Advanced, Fast Roaming.
2. Specify the Fast Roaming Settings.
3. Click Save.

4.6. Site Survey

The AN100/300 provides a convenient on-board Wi-Fi detection tool or Wi-Fi ‘sniffer’. This feature can be used to detect the presence of other 2.4GHz and 5GHz wireless networks, their modes, channels, security settings, signal strengths, encryptions, and type. Having this information can be very useful helping avoid conflicts with other networks in the wireless neighborhood.

Figure 47. Site Survey Settings



Path Advanced, Site Survey

4.6.1. Select Interface

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

Figure 48. Site Survey Settings - Select Interface

Path Advanced, Site Survey, Select Interface

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Select Interface** – Select 2.4GHz to scan for 2.4GHz networks. Select 5GHz to scan for 5GHz networks.
- **Scan Nearby Networks** – Press the Scan button to start the scan. A list of 2.4GHz or 5GHz devices will appear as shown.
-

Configuration Instructions

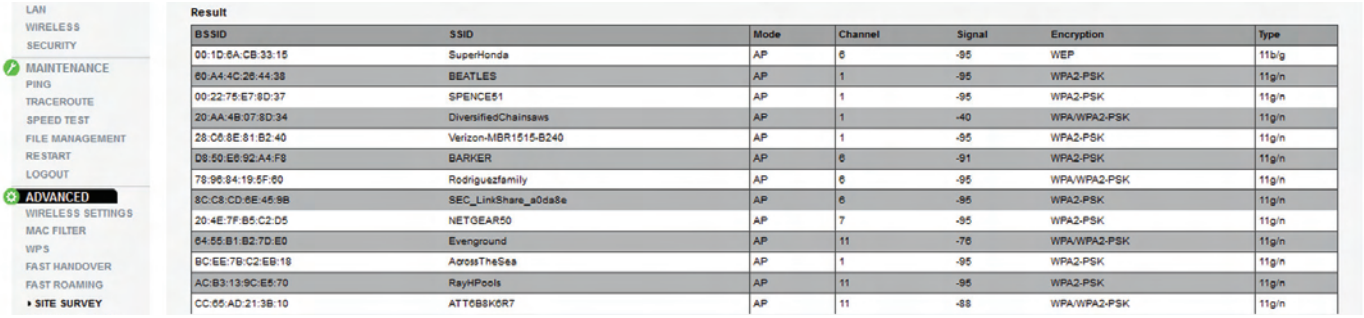
To configure Site Survey:

1. Click Advanced, Site Survey.
2. Specify the Site Survey Settings.
3. Click Scan.

4.6.2. Result

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

Figure 49. Site Survey Settings - shown with scan results



BSSID	SSID	Mode	Channel	Signal	Encryption	Type
00:1D:6A:CB:33:15	SuperHonda	AP	6	-95	WEP	11b/g
60:A4:4C:26:44:38	BEATLES	AP	1	-95	WPA2-PSK	11g/n
00:22:75:E7:8D:37	SPENCE51	AP	1	-95	WPA2-PSK	11g/n
20:AA:4B:07:8D:34	DiversifiedChainsaws	AP	1	-40	WPA/WPA2-PSK	11g/n
28:C6:8E:81:B2:40	Verizon-MBR1515-B240	AP	1	-95	WPA2-PSK	11g/n
D8:50:E6:92:A4:F8	BARKER	AP	6	-91	WPA2-PSK	11g/n
78:96:84:19:5F:60	Rodriguezfamily	AP	6	-95	WPA/WPA2-PSK	11g/n
8C:C8:CD:6E:45:9B	SEC_LinkShare_a0da8e	AP	6	-95	WPA2-PSK	11g/n
20:4E:7F:B5:C2:D5	NETGEAR50	AP	7	-95	WPA2-PSK	11g/n
64:55:B1:B2:7D:E0	Evenground	AP	11	-76	WPA/WPA2-PSK	11g/n
BC:EE:7B:C2:EB:18	AcrossTheSea	AP	1	-95	WPA2-PSK	11g/n
AC:B3:13:9C:E5:70	RayHPools	AP	11	-95	WPA2-PSK	11g/n
CC:65:AD:21:3B:10	ATT6B8K6R7	AP	11	-88	WPA/WPA2-PSK	11g/n

Path Advanced, Site Survey

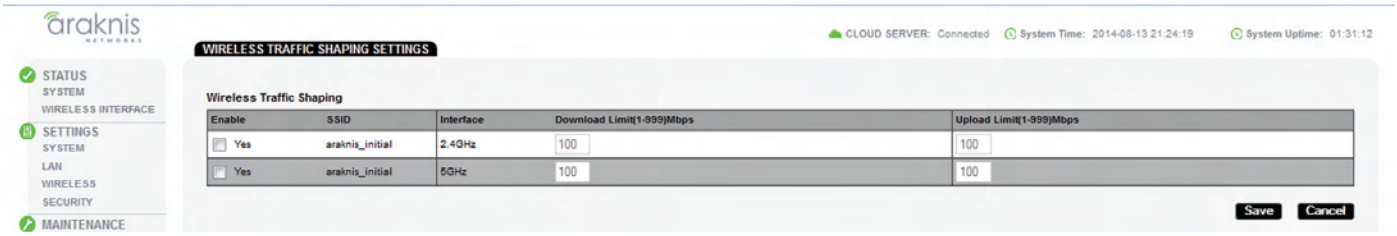
Parameters

- **BSSID** – Basic Service Set Identification. Indicates the MAC Address of a detected 2.4GHz or 5GHz network device.
- **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 AN100/300.
- **Encryption** – Indicates the security mode encryption of a detected device.
- **Type** – Indicates the wireless mode of the detected device.

4.7. Wireless Traffic Shaping Settings

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

Figure 50. Wireless Traffic Shaping Settings



Path Advanced, Traffic Shaping

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

- **Enable** – Select to enable Traffic Shaping on the 2.4GHz and/or 5GHz band.
- **SSID** – Indicates the network to which Traffic Shaping will be applied.
- **Interface** – Indicates 2.4GHz or 5GHz band.
- **Download Limit** – Enter a value to regulate download speed. RANGE: 1-999Mbps. DEFAULT: 100Mbps.
- **Upload Limit** – Enter a value to regulate upload speed. RANGE: 1-999Mbps. DEFAULT: 100Mbps.

Configuration Instructions

To configure Wireless Traffic Shaping:

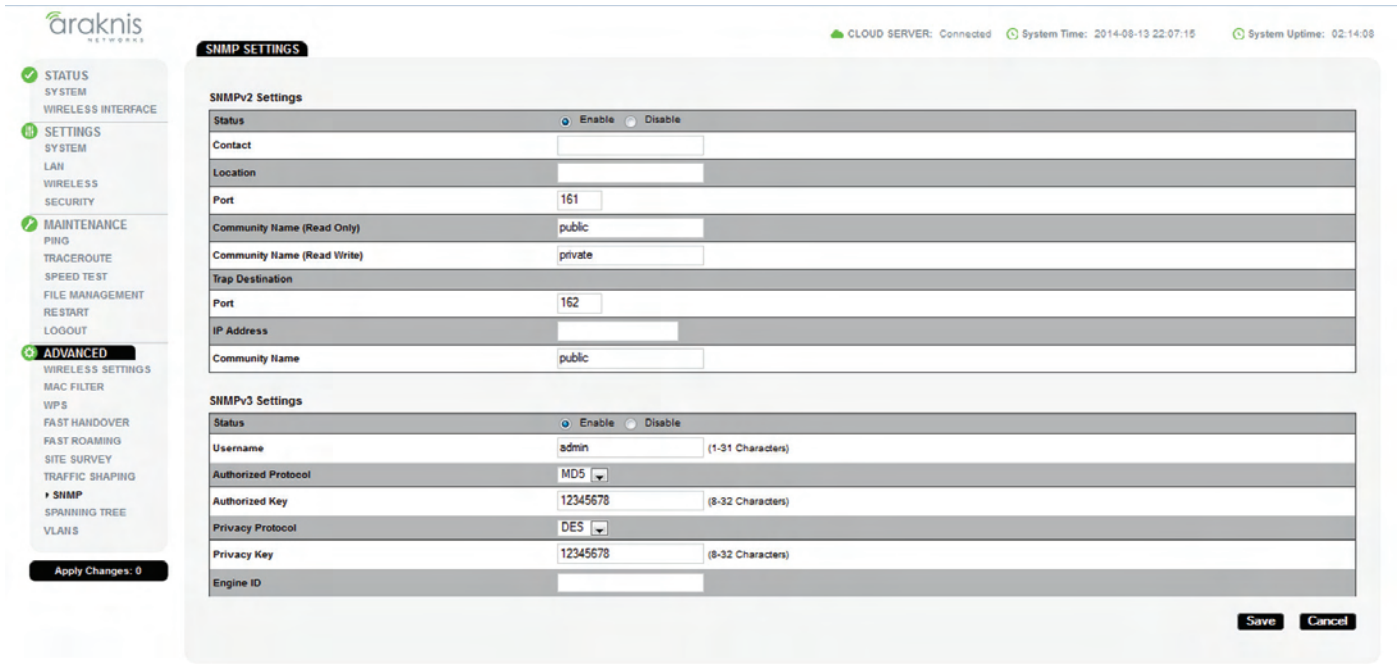
1. Click Advanced, Traffic Shaping.
2. Specify the Wireless Traffic Shaping Settings.
3. Click Save.

-

4.8. 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 51. SNMP Settings

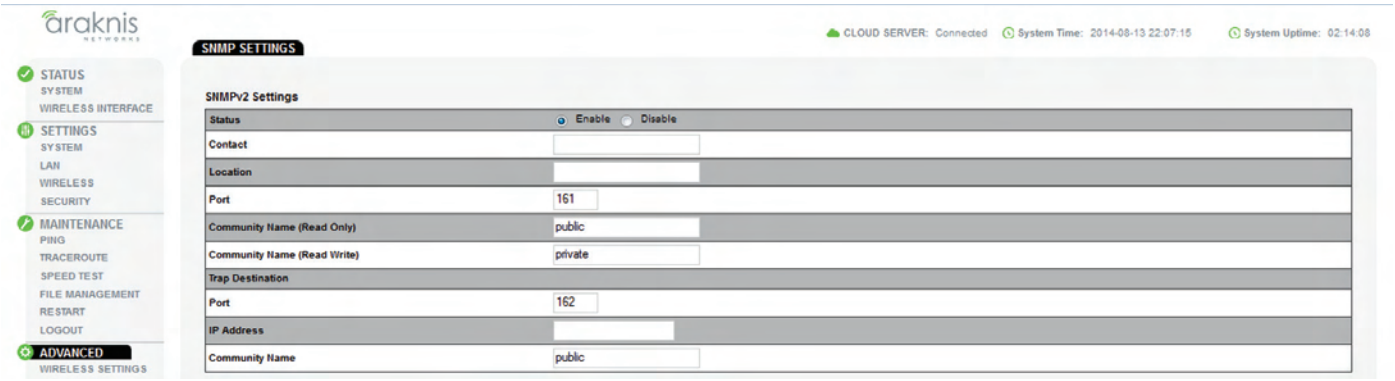


Path Advanced, SNMP

4.8.1. SNMPv2 Settings

This section allows configuration of SNMPv2 Settings.

Figure 52. SNMP Settings



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'. This is a dedicated UDP port and would typically not be changed. DEFAULT: 161
- **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'. This is a dedicated TCP/UDP port and would typically not be changed. DEFAULT: 162

  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

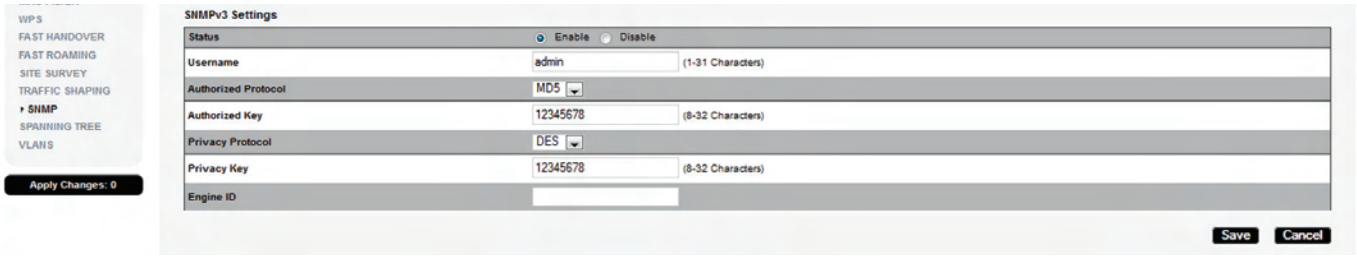
To configure SNMPv2 Settings:

1. Click Advanced, SNMP.
2. Specify the SNMPv2 Settings.
3. Click Save.

4.8.2. SNMPv3 Settings

This section allows configuration of SNMPv3 Settings.

Figure 53. SNMP Settings



Path Advanced, SNMP, SNMPv3

Parameters

- **Status** – Select Enable to enable SNMPv3. Select Disable to disable SNMPv3. DEFAULT: Enable
- **User Name** – Enter a User Name 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

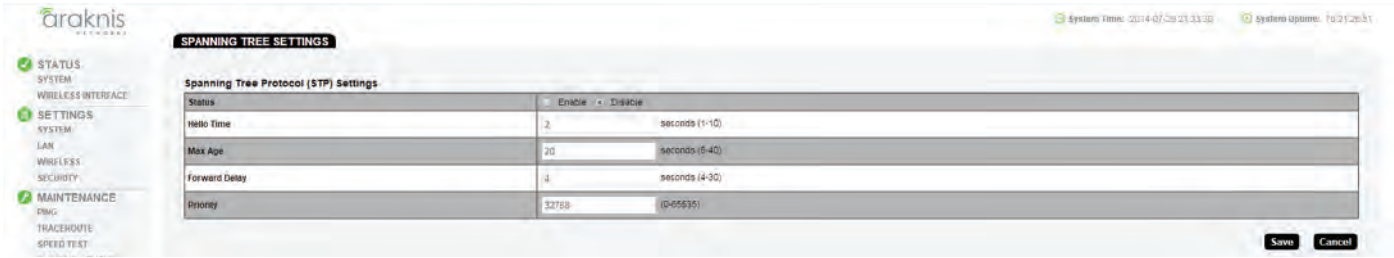
To configure SNMPv3 Settings:

1. Click Advanced, SNMP.
2. Specify the SNMPv3 Settings.
3. Click Save.

4.9. 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 54. Spanning Tree Settings



Path Advanced, SNMP, Spanning Tree

Parameters

- **Status** – Select Enable to enable STP. Select Disable to disable STP. DEFAULT: Disable
- **Hello Time** – Enter a value for Hello Time. This setting will determine how often in seconds the AN100/300 will send the Hello Message to network switches and bridges to asses network topology. RANGE: 1-10 seconds. DEFAULT: 2 seconds
- **Max Age** – Enter a duration for Max Age. This setting will determine how long the AN100/300 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 AN100/300 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. This setting will help determine which bridge is the root bridge, or essentially which switch controls the main road that network traffic is going to 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 so called root bridge. Setting a lower Priority will help generate a lower score for a given switch. RANGE: 0-65535. DEFAULT: 32768.

Configuration Instructions

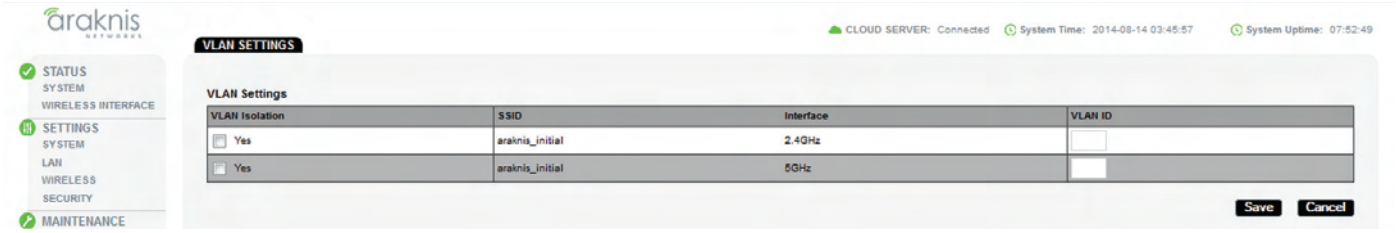
To configure Spanning Tree Settings:

1. Click Advanced, Spanning Tree.
2. Specify the Spanning Tree Settings.
3. Click Save.

4.10. 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 AN100/300 to maintain the integrity of the VLAN by identifying which data belongs to which VLAN.

Figure 55. VLAN Settings



Path Advanced, VLANS

Parameters

NOTE: The WAP100 will indicate settings and information for the 2.4Ghz Channel. The WAP300 will indicate settings and information for the 2.4GHz and 5GHz Channels.

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

Configuration Instructions

To configure VLAN Settings:

1. Click Advanced, VLANS.
2. Specify the VLAN Settings.
3. Click Save.

-