araknis NETWORKS

210/310 SERIES MANAGED NETWORK SWITCH
PRODUCT MANUAL

Models:

AN-210-SW-F/R-8-POE
AN-210-SW-F/R-16-POE
AN-210-SW-F/R-24-POE
AN-310-SW-F/R-8
AN-310-SW-F/R-16
AN-310-SW-F/R-24
AN-310-SW-F/R-8-POE
AN-310-SW-F/R-16-POE
AN-310-SW-F/R-24-POE

About this Manual

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

Pro Tip – Pro tips are included in sections of the manual to add information that provides extra value, utility, or ease-of-use for the installer or end user of the product. These items are not required, but have been added for your convenience.

Note – Notes emphasize information important to the installation, setup, or use of the product that is not essential to follow for safety of the equipment or user. These items contain essential information that, if missed, would cause the installer or end user extra work to overcome.

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

Warning – Warnings indicate information vital to the safety of the installer or end user of the product. Not following a warning may result in permanent damage to equipment and serious injury or death of the installer or end user.

© 2016 Araknis Networks®

Table of Contents

1 - Welcome to Araknis Networks™ 7
2 - Package Contents 7
3 - Series Overview 7
4 - Device Layout 8
Rear Facing Models 9
Front Facing Models 9
5 - Hardware Installation 10
Mounting 10
Rack Mounting Guidelines 10
Rack Mount 10
Wall Mount 10
Shelf Mount 10
Connections 11
Input Power Requirements 11
Network Cable Requirements 11
SFP Ports 11
Switch 11
PoE Budget Calculation Example 12
6 - OvrC Setup 13
7 - Interface Access 14
OvrC Web Connect Access 14
Direct Access Using LAN IP Address (DHCP) 15
Default IP Address Access 16
8 - Interface Overview 19
Page Layout 19
Applying or Canceling Changes 19
9 - Switch Status Pages 20
System Status Page 20
System Information 20
Port Status 20
Events Log 21
Port Status Page 22
10 - System Settings 23
System Information 23
IP Address Settings 24
IPv4 IP Settings 24
IPv6 IP Settings 24
Date and Time Settings 25
UPnP Setting 25
11 - Recommended Setup – System Settings 26
12 - Port Configuration Settings 27
Jumbo Frame Setting 27
Basic Port Settings 27
Advanced Port Settings 28

© 2016 Araknis Networks®

13 - PoE Settings 29
PoE Setup and Troubleshooting 30
Checking Status of PoE Devices 30
Configuring PoE Ports 30
Troubleshooting PoE Issues 30
14 - VLAN Settings (Basic Port-Based) 31
Access and Trunk Port Selection 31
Creating a New VLAN 32
15 - Link Aggregation Settings 33
Creating a New Link Aggregation Rule 34
16 - Access Management Settings 35
User Management 35
HTTP/Telnet/SSH 35
17 - Maintenance Menus 36
Ping Test 36
Running a Ping Test 36
Understanding Ping Test Results 37
Troubleshooting Using Ping Test Results 37
Trace Route Test 38
Running a Trace Route Test 38
Understanding Trace Route Test Results 39
File Management Settings 40
Configuration File 40
Firmware 40
Dual Image 41
Firmware Update Instructions 41
Restart 42
Log Out 42
18 - Advanced Menus 43
19 - Advanced Port Statistics 44
20 - Neighbors – MAC Address Table 46
Static and Dynamic MAC Address 46
21 - Neighbors – LLDP 47
Information Table 47
Settings 48
Remote Device Table 48
22 - Multicast – IGMP Snooping 49
Settings 49
VLAN Settings 49
Querier Settings 50
Group List 51
Router Settings 51
URC Settings 51

© 2016 Araknis Networks®

23 - Multicast – MLD Snooping 52
Settings 52
VLAN Settings 52
Group List 52
Router Settings 53
24 - STP – Overview 54
STP – Global Settings 54
Settings 54
Root Bridge Information 55
Basic Setting 56
25 - STP (Spanning Tree Protocol) Overview 57
STP – CIST Settings 57
Port Settings 57
STP – MST Settings 59
Instance Settings 59
Port Settings 60
26 - Advanced VLANs – Overview 61
Advanced VLANs – 802.1Q VLANs 61
VLAN Settings 61
PVID Settings 61
Advanced VLANs – Private VLANs 62
Advanced VLANs – Voice VLANs 63
General Settings 63
OUI Settings 64
Port Settings 64
27 - Security – Port Mirroring 65
28 - Security – 802.1x 65
802.1x Global Setting 65
Port Settings 66
Authenticated Host 67
29 - Security – Radius Server 68
30 - Security – DOS 69
Global Settings 69
Global DOS Security Settings, Continued 70
Port Settings 70
31 - Security – Port Security 71
32 - Security – MAC Address Filter 71
33 - RMON Overview 72
RMON – Event List 72
RMON – Event Log Table 72
RMON – Alarm List 73
RMON – History List 74
RMON – History Log Table 74
34 - QoS – Overview 75
QoS – Global Settings 75

© 2016 Araknis Networks®

QoS – COS Mapping 75
QoS – DSCP Mapping 76
QoS – Port Settings 76
QoS – Bandwidth Control 76
QoS – Storm Control 77
35 - ACL – Overview 78
ACL – MAC ACL 78
MAC ACL List 78
MAC ACE List 78
MAC ACE List Editor 79
ACL – IPV4 ACL 80
IPv4 ACL List 80
IPv4 ACE List 80
IPv4 ACE List Editor 81
ACL – IPV6 ACL 82
IPv6 ACL List 82
IPv6 ACE List 82
IPv6 ACE List Editor 83
ACL – ACL Binding 84
36 - SNMP – Overview 85
SNMP – Global Settings 85
Settings 85
Trap Settings 86
Remote Engine ID List 86
SNMP – Lists 87
Group Lists 87
View List 87
SNMP Community List 88
User List 88
37 - Advanced LACP 89
Settings 89
LACP Timeout 89
38 - Advanced Log 90
Settings 90
Local Logging 90
Remote Logging 90
39 - AN-210-SW Specifications 94
40 - AN-310-SW Specifications 96
41 - Appendix – Safety and Regulatory Information 98
FCC Warning 98
CE Warning 98
UL Statement 98
42 - Warranty 99
2 Year Limited Warranty 99
Contact Information 99

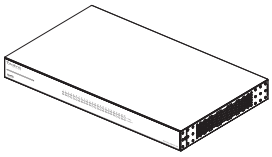
© 2016 Araknis Networks®

1 - Welcome to Araknis Networks™

Thank you for purchasing an Araknis 210/310 series network switch. This manual details the installation and setup of the hardware and the managed interface.

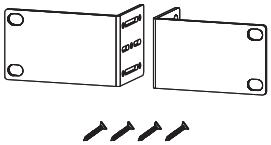
2 - Package Contents

Figure 1. Package Contents



Switch (1)

Rubber Feet for Flat Surfaces (4)



Rack-Mount Kit: Ears (2), Screws (8)

Quick Start Guide

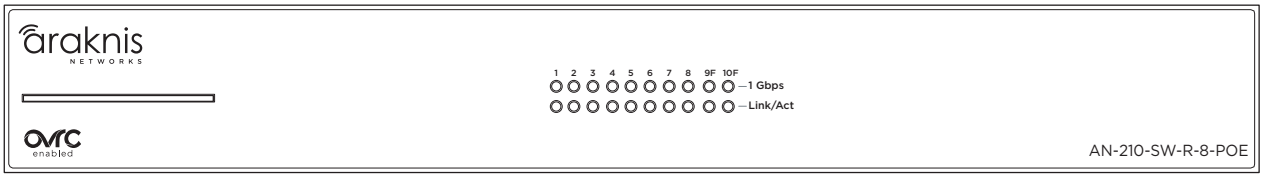
AC Power Cord

3 - Series Overview

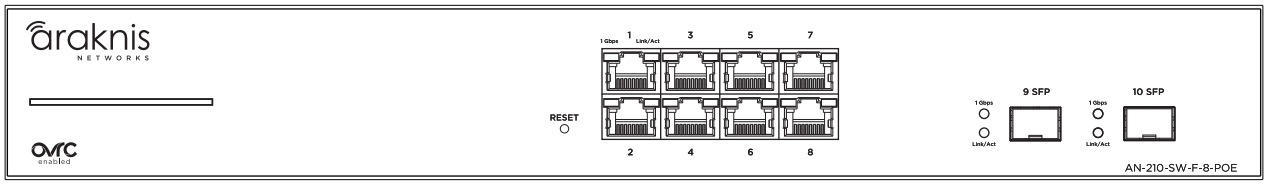
Model	Ethernet Ports	SFP Ports	PoE Budget
AN-210-SW-F/R-8-POE	8	2	65w
AN-210-SW-F/R-16-POE	16	2	130w
AN-210-SW-F/R-24-POE	24	2	190w
AN-310-SW-F/R-8	8	2	-
AN-310-SW-F/R-16	16	2	-
AN-310-SW-F/R-24	24	2	-
AN-310-SW-F/R-8-POE	8	2	130w
AN-310-SW-F/R-16-POE	16	2	250w
AN-310-SW-F/R-24-POE	24	2	375w

© 2016 Araknis Networks®

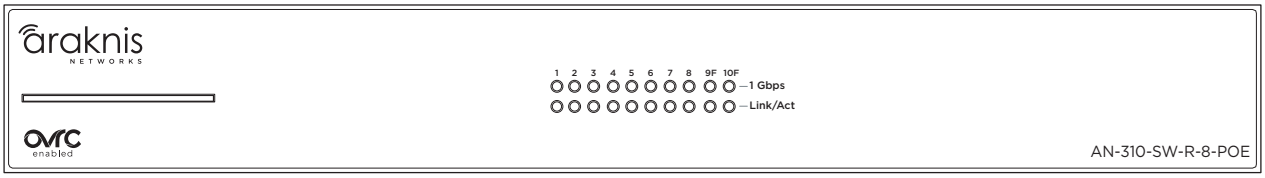
4 - Device Layout



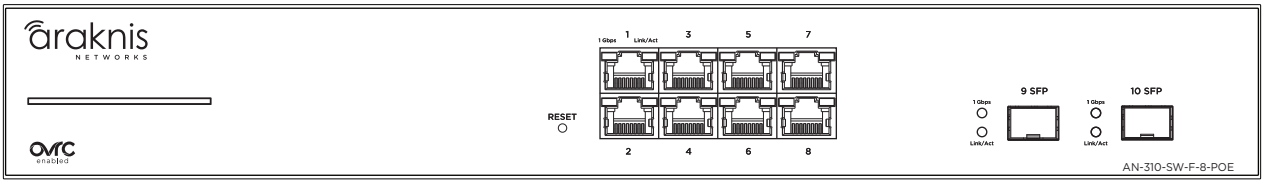
AN-210-SW-R-8-POE



AN-210-SW-F-8-POE



AN-310-SW-R-8-POE



AN-310-SW-F-8-POE

1. **Power LED –** **On: system is up.**
   Off: system is down.

2. **1Gbps LED –** **On: port connected at 1000Mbps speed.**
   Off: port is connected at 10/100Mbps speed.

3. **Link/Act LED –** **On: port is connected to another device.**
   Blinking: packets are running through the port.
   Off: port is not connected to a device.

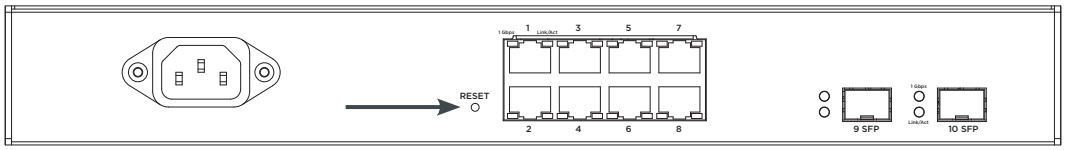
Note – The 1Gbps LED behavior may be configured to indicate other information. See instructions in section “10 - System Settings” on page 23.

© 2016 Araknis Networks®

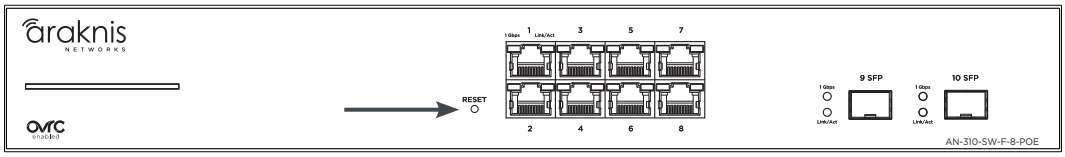
Factory Reset

Reboot or default the switch configuration settings.

Rear Facing Models



Front Facing Models



1. **Reboot –** Press and hold the RESET button on the back of the switch for 5 seconds, then release. The switch will power cycle and the front status lights will flash.

2. **Factory Reset** – Press and hold the RESET button for 10-15 seconds until the status LEDs flash once. The switch will power cycle and be reset to factory default settings.

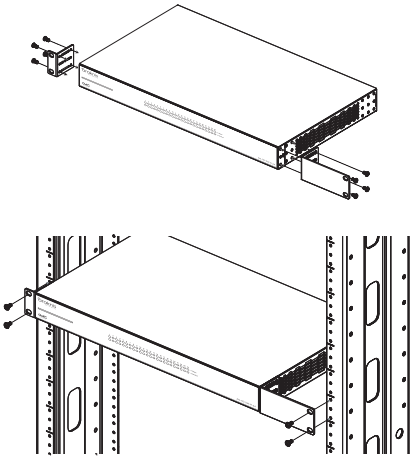
© 2016 Araknis Networks®

5 - Hardware Installation

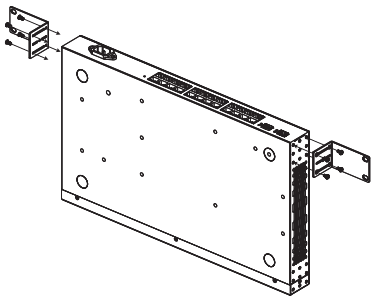
Mounting

Figure 2. Mounting Methods

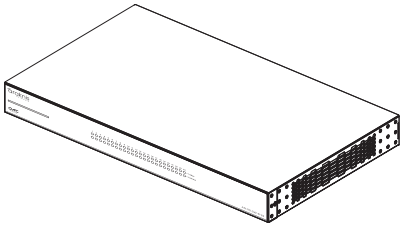
Ⓐ Rack Mount



Ⓑ Wall Mount



Ⓒ Shelf Mount



Note – Do not stack other equipment on top of the switch to avoid possible interference or damage.

Note – Mounting is the same for models with both front- and rear-facing ports.

Rack Mounting Guidelines

Elevated Operating Ambient – If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the maximum ambient temperature of 104°F.

Reduced Air Flow – Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading – Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.

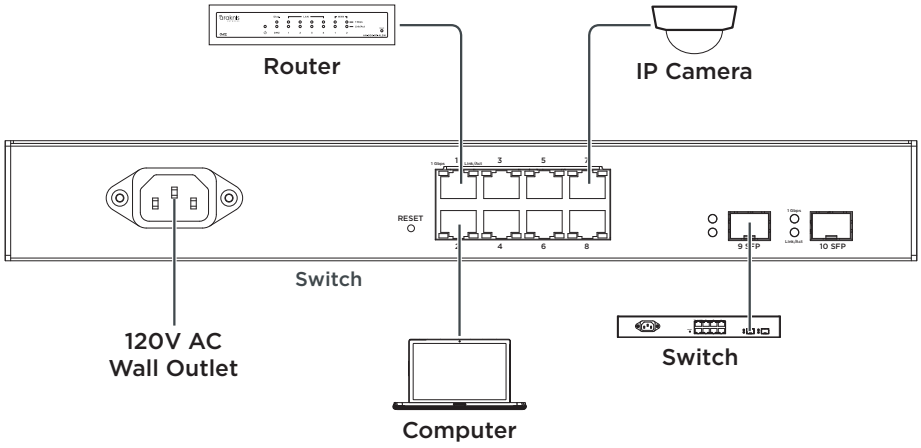
Circuit Overloading – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing – Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).

© 2016 Araknis Networks®

Connections

Figure 3. Connection Diagram



Note – AN-210-SW-R-8-POE shown. Connection is the same for models with both front- and rear-facing ports.

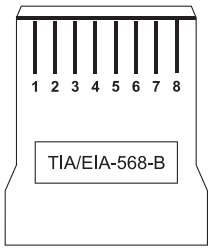
Input Power Requirements

AC Input Voltage: 100-240V AC, 50-60 Hz.

Network Cable Requirements

568B termination is recommended (Figure 4. EIA/TIA 568B Termination Pattern) Connect a Cat5e/6 straight-through cable between the switch and other equipment.

Figure 4. EIA/TIA 568B Termination Pattern



(Gold pins facing up)

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

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

SFP Ports

The SFP (Small Form Factor Pluggable) ports guarantee a 1 Gbps connection and are typically used to connect switches together. Connect SFP ports using Araknis SFP adapters for RJ45 or multi-mode fiber cables. SFP adapters sold separately.

© 2016 Araknis Networks®

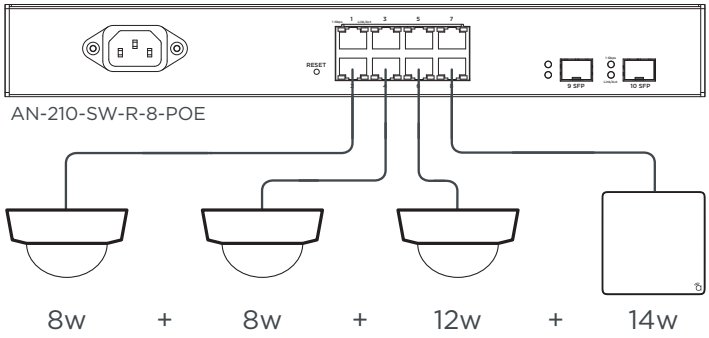
PoE Budgeting

The power budget for delivering Power over Ethernet limits the total number of watts available between all of the ports (limited to 30w total consumption on each port). Add the total number of watts consumed by all connected PoE devices to ensure that every thing can be powered, as illustrated in the example below.

Model	PoE Budget
AN-210-SW-F/R-8-POE	65w
AN-210-SW-F/R-16-POE	130w
AN-210-SW-F/R-24-POE	190w
AN-310-SW-F/R-8-POE	130w
AN-310-SW-F/R-16-POE	250w
AN-310-SW-F/R-24-POE	375w

PoE Budget Calculation Example

Figure 5. PoE Calculation Example



Total PoE Budget Available	=	65w
Total PoE Device Consumption	=	42w
PoE Budget Left Available	=	23w

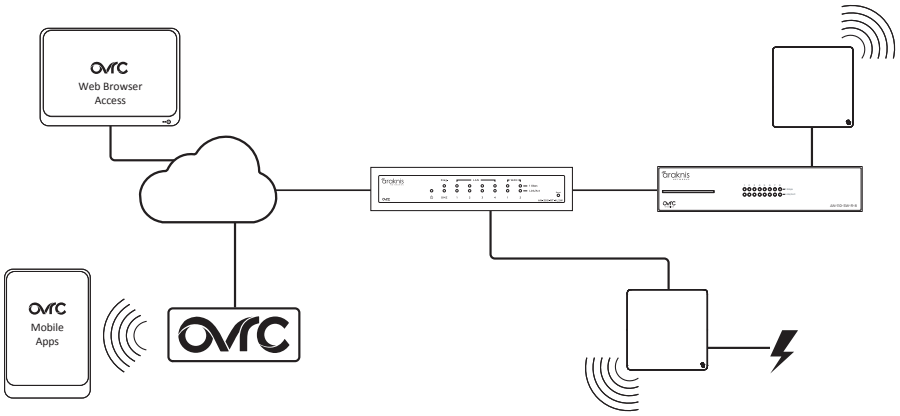
Note – Port PoE settings may be modified using the PoE Settings menu. Click to see information and instructions.

© 2016 Araknis Networks®

6 - OvrC Setup

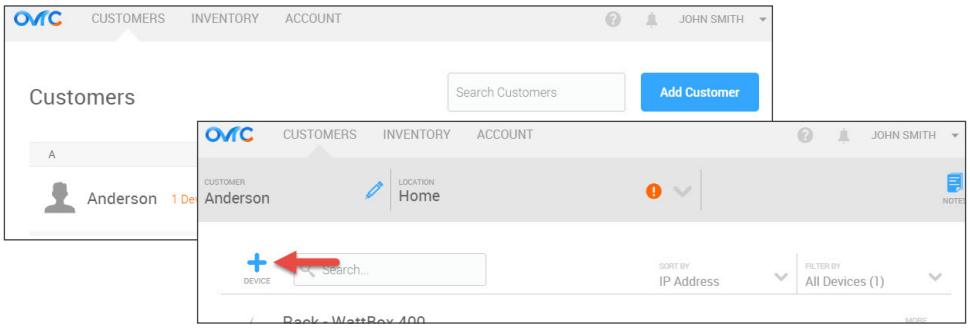
OvrC provides remote firmware upgrades, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

Figure 6. OvrC Operation Diagram

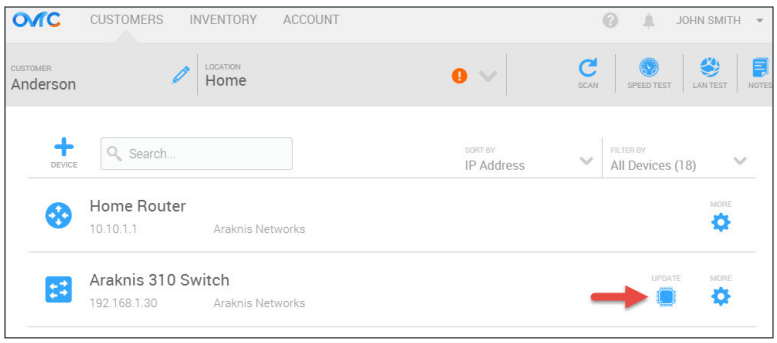


To add this device to your OvrC account:

1. Connect the switch to the network (Internet access required).
2. Log Into OvrC (www.ovrc.com) or load the OvrC app.
3. Select or create a customer account.



4. Add the device (MAC address and Service Tag numbers needed for authentication).
5. Check for OvrC firmware updates and apply if available.



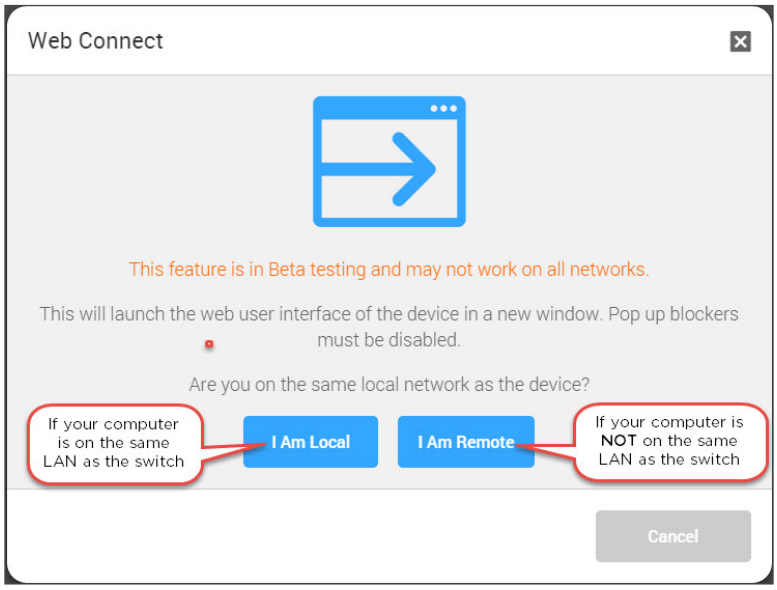
© 2016 Araknis Networks®

7 - Interface Access

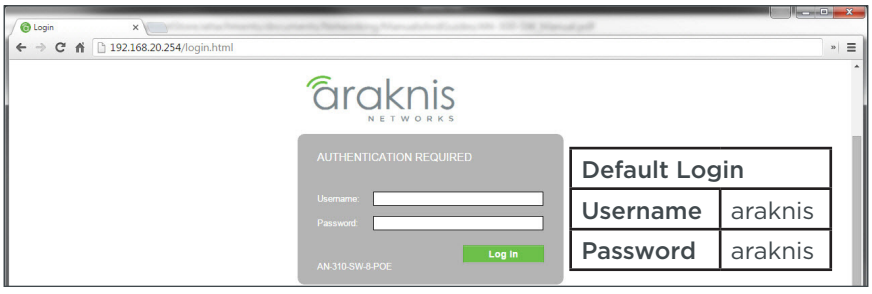
OvrC Web Connect Access

1. Log into the Ovrc app and find the switch. The OvrC web interface is easier to use than mobile for Web Connect access. Popup blockers must be disabled.

2. Click the **More** button and then click **Web Connect**. In the Web Connect menu, click the appropriate button to access the web interface.



3. OvrC will open a new tab in your web browser and load the login screen. Enter your username and password, then click **Log In**.



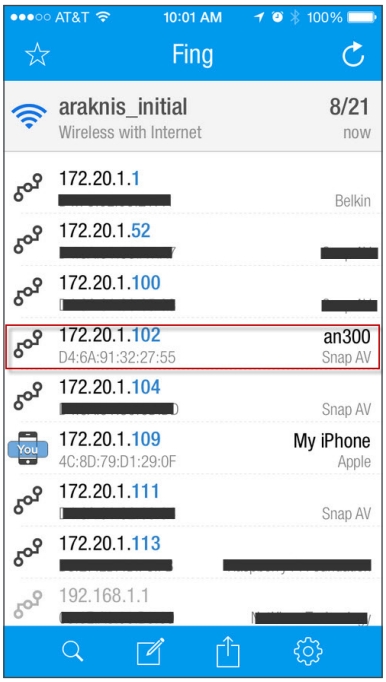
4. If you were able to log in successfully, go to the System Settings menu to begin completing the recommended setup for all users. See section “11 - Recommended Setup – System Settings” on page 26.

5. If this access method does not work for your application, see the next section for instructions to access the interface using a DHCP IP address.

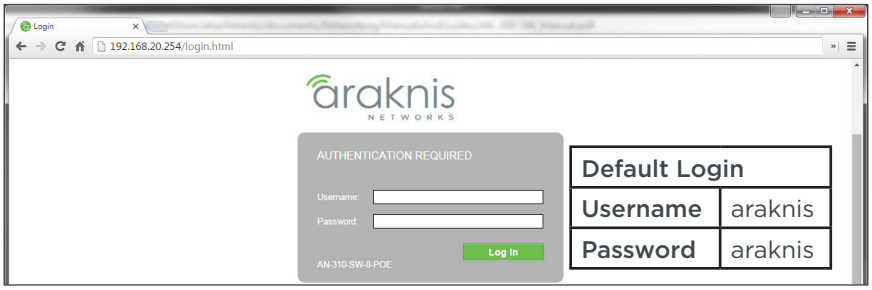
© 2016 Araknis Networks®

Direct Access Using LAN IP Address (DHCP)

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



2. Enter the IP address in your web browser to load the login screen. Enter your username and password, then click **Log In**.



3. If you were able to log in successfully, go to the System Settings menu to begin completing the recommended setup for all users. See section “11 - Recommended Setup – System Settings” on page 26.

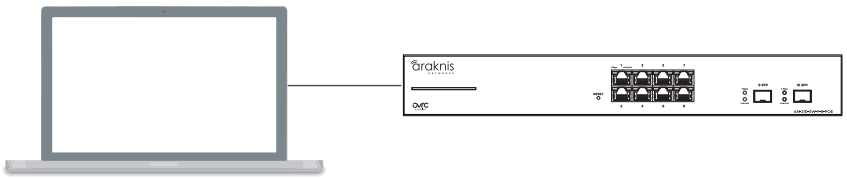
4. If this access method does not work for your application, see the next section for instructions to access the interface using the switch’s default IP address.

© 2016 Araknis Networks®

Default IP Address Access

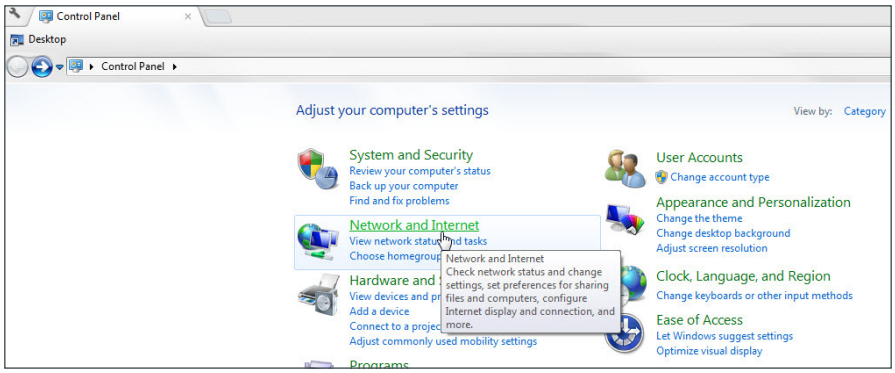
Access the interface using the default IP address, **192.168.20.254**.

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

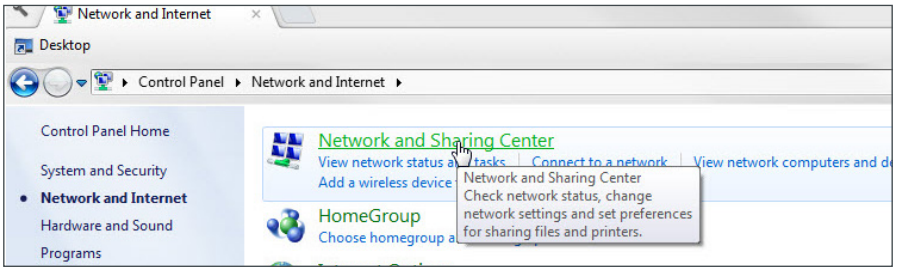


Computer Switch

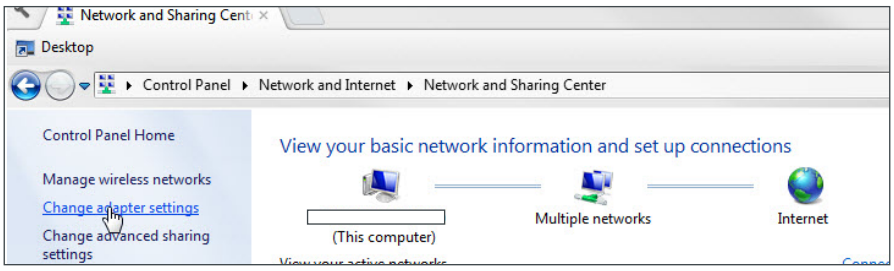
2. On your PC, open the Control Panel and left-click **Network and Internet**.



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

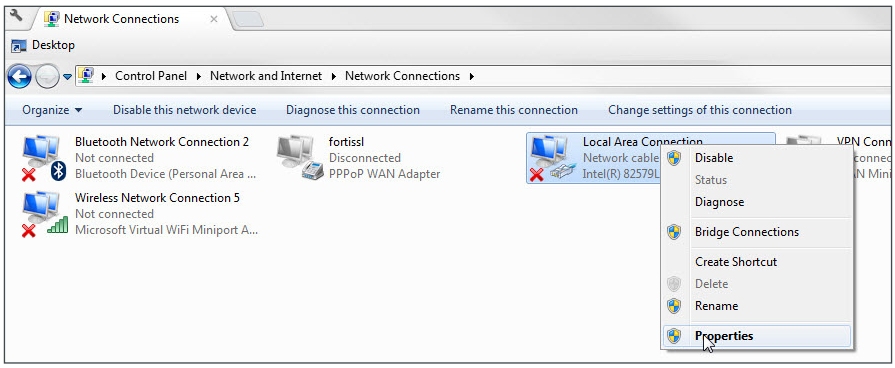


4. In the left bar, left-click **Change adapter settings**.

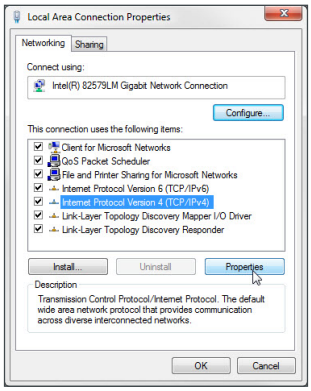


© 2016 Araknis Networks®

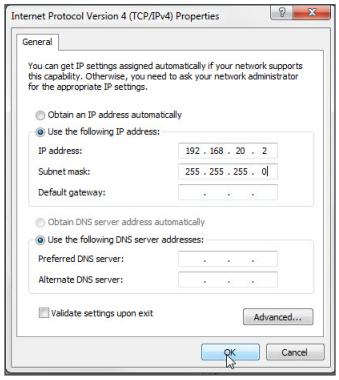
5. Right-click the icon for the wired network connection and left-click **Properties**.



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

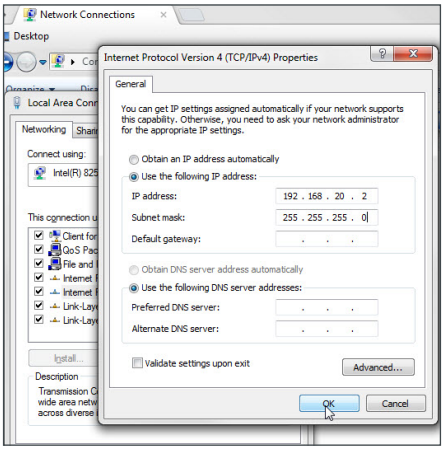


7. In the General tab, left-click **Use the following IP address:** and enter the IP address and subnet mask.
   - IP Address: ***192.168.20.2***
   - Subnet Mask: ***255.255.255.0***

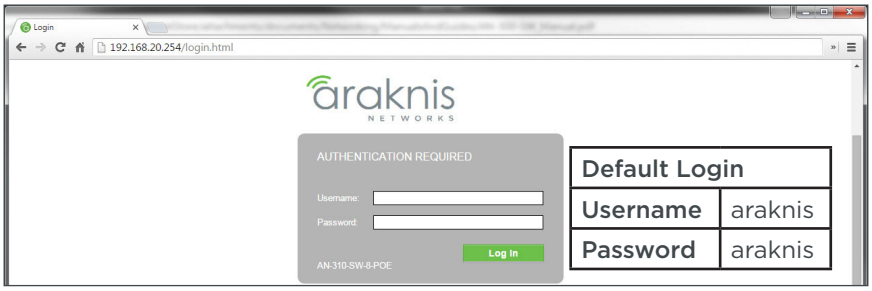


© 2016 Araknis Networks®

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



9. Open a web browser and navigate to ***http://192.168.20.254/*** to load the login screen. Enter your username and password, then click **Log In**.



10. If you were able to log in successfully, go to the System Settings menu to begin completing the recommended setup for all users. See section “11 - Recommended Setup – System Settings” on page 26.

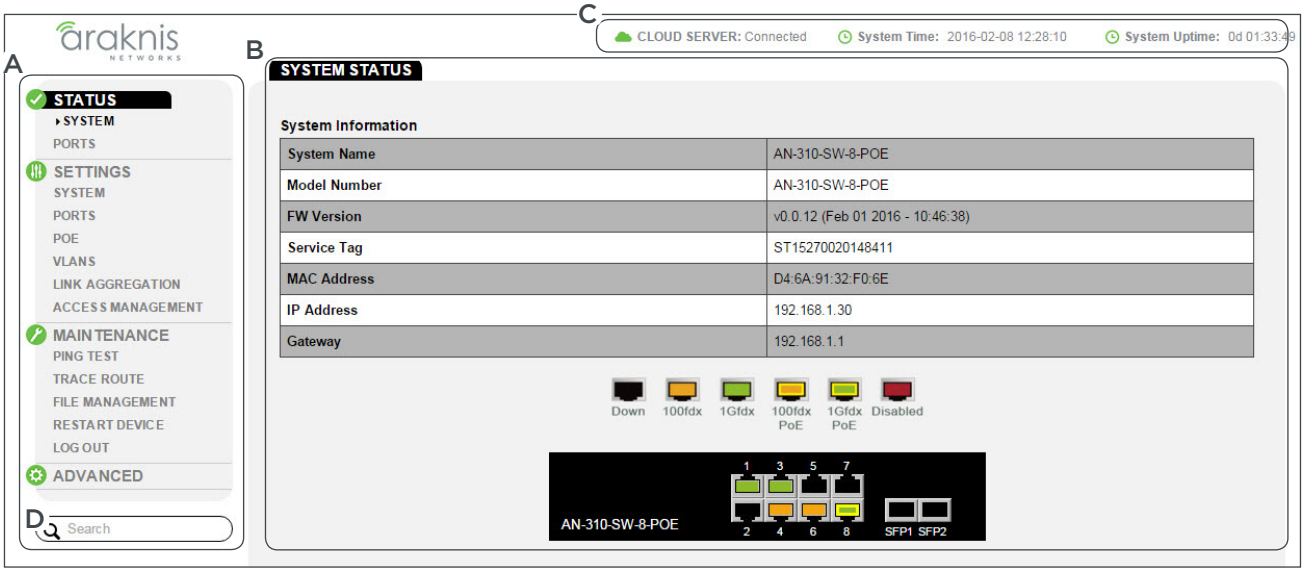
© 2016 Araknis Networks®

8 - Interface Overview

Page Layout

Use this section to become familiar with the common parts of the interface.

Figure 7. Interface Layout

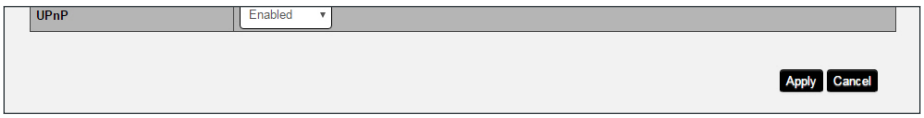


- **A - Main Navigation Menu**
  Use the submenus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the switch.
- **B - Main Window**
  The main window displays the currently selected submenu.
- **C - Top Bar**
  The top bar displays the current connection status to the OvrC server, the current internally-set system time, and the current system uptime in DAYS:HOURS:MINUTES.
- **D - Search**
  Search for menu functions by entering a term, then selecting the appropriate item from the drop down results. Do not press enter when searching.

Applying or Canceling Changes

After changes are made to a menu page, you must click the **Apply** button to save the new settings or **Cancel** to revert the changes. These buttons are always located at the bottom-right corner of the page.

Figure 8. Apply Button



© 2016 Araknis Networks

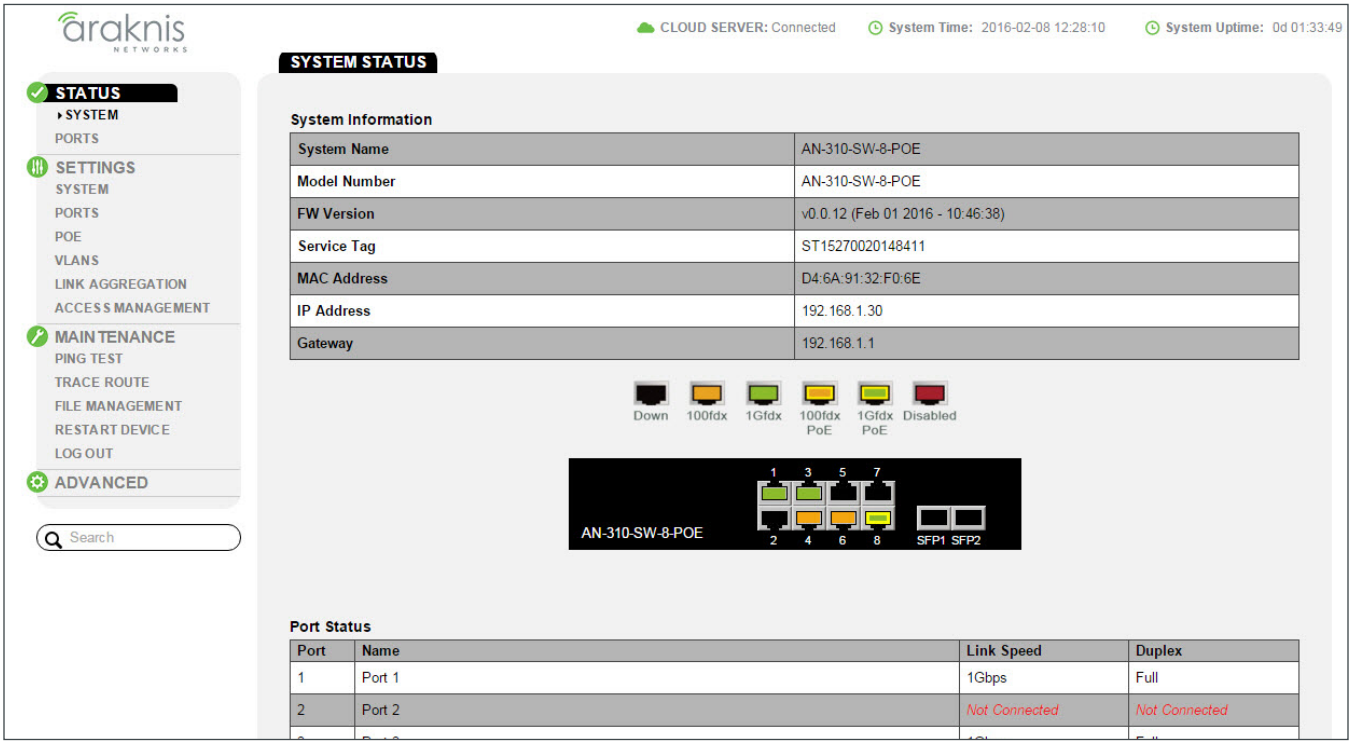
9 - Switch Status Pages

System Status Page

Use the System Status page to review current system information and operating status.

Path – Status, System (Default Login Landing Page)

Figure 9. System Information and Port Status



System Information

- **System Name –** Name assigned to the system.
- **Model Number –** Product SKU.
- **FW Version –** Current operating firmware version.
- **MAC Address –** Media Access Control (MAC) address of the switch.
- **IP Address –** Device management IP address.
- **Service Tag –** Internal tracking number used to track every product sold by Araknis Networks.
- **Gateway –** Default gateway of the management VLAN.

Port Status

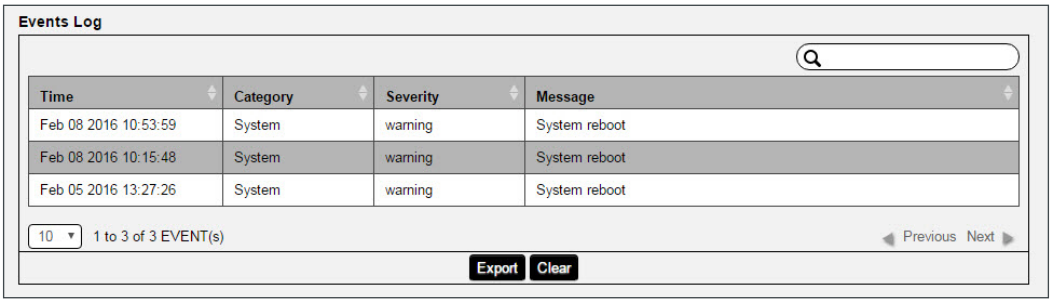
- **Port –** Port number. Corresponds to the physical location of the port on the switch.
- **Name –** Name assigned to the port.
- **Link Speed –** Current port speed. 1Gbps, 100Mbps, 10Mbps, or Not Connected.
- **Duplex –** Current duplex mode. Full or Half.

© 2016 Araknis Networks®

Events Log

Use the Events Log to review messages about the operating state of the switch. The log can be cleared or saved to your computer in a text file (.txt).

Figure 10. Events Log



- **Search Bar –** Enter terms to search for in the Message Field column.
- **Time –** Log entry recorded time.
- **Category –** Type of event.
- **Severity –** Level of entry severity.
- **Message –** Detailed entry information. Example: System reboot
- **Navigation –** Use the left drop down to select a page of entries to navigate to. Use the Previous and Next buttons on the right side to toggle between screens.
- **Export –** Click to export a .txt file of the log to your computer.
- **Clear –** Click to erase all entries in the Events Log.

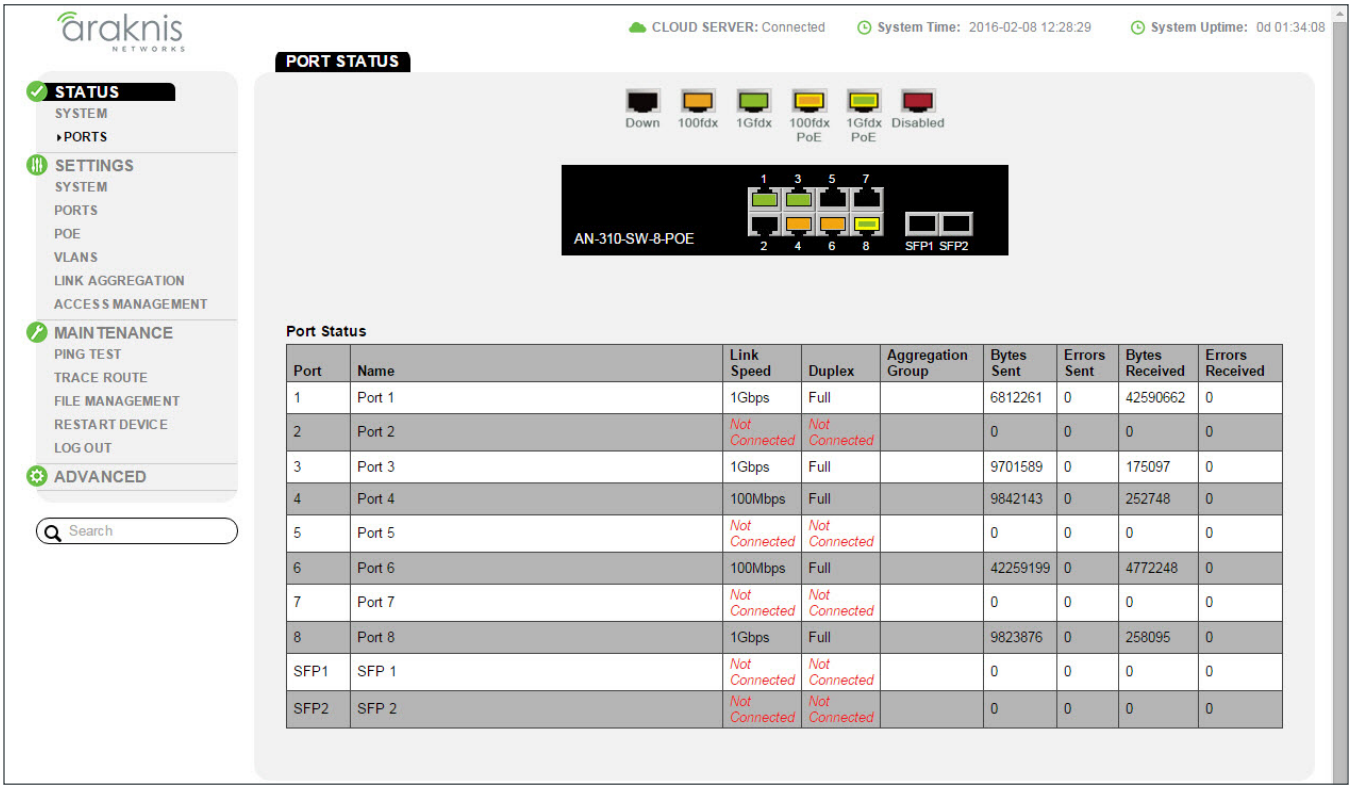
© 2016 Araknis Networks®

Port Status Page

This page provides in-depth details about the status of each physical port.

Path – Status, Ports

Figure 11. Port Status



Port Status

Port	Name	Link Speed	Duplex	Aggregation Group	Bytes Sent	Errors Sent	Bytes Received	Errors Received
1	Port 1	1Gbps	Full		6812261	0	42590662	0
2	Port 2	Not Connected	Not Connected		0	0	0	0
3	Port 3	1Gbps	Full		9701589	0	175097	0
4	Port 4	100Mbps	Full		9842143	0	252748	0
5	Port 5	Not Connected	Not Connected		0	0	0	0
6	Port 6	100Mbps	Full		42259199	0	4772248	0
7	Port 7	Not Connected	Not Connected		0	0	0	0
8	Port 8	1Gbps	Full		9823876	0	258095	0
SFP1	SFP 1	Not Connected	Not Connected		0	0	0	0
SFP2	SFP 2	Not Connected	Not Connected		0	0	0	0

- **Port –** The number of the physical switch port.
- **Name –** The assigned name of the port.
- **Link Speed –** The current speed of the port based off of the connected device in use. 1Gbps, 100Mbps, 10Mbps, or Not Connected.
- **Duplex –** The current duplex setting with the connected device. Full or Half.
- **Aggregation Group –** The aggregation group the port is member of. No ports are members of any aggregation group by default.
- **Bytes Sent –** A live count of the number of bytes being transmitted on a specific port.
- **Errors Sent –** A live count of the number of outgoing errors sent on a specific port. Use this number to determine whether there is a problem with the physical interface of the specific port.
- **Bytes Received –** A live count of the number of bytes being received on a specific port.
- **Errors Received –** A live count of the number of incoming errors received on a specific port. Use this number to determine whether there is a problem with the physical interface of the port.

© 2016 Araknis Networks®

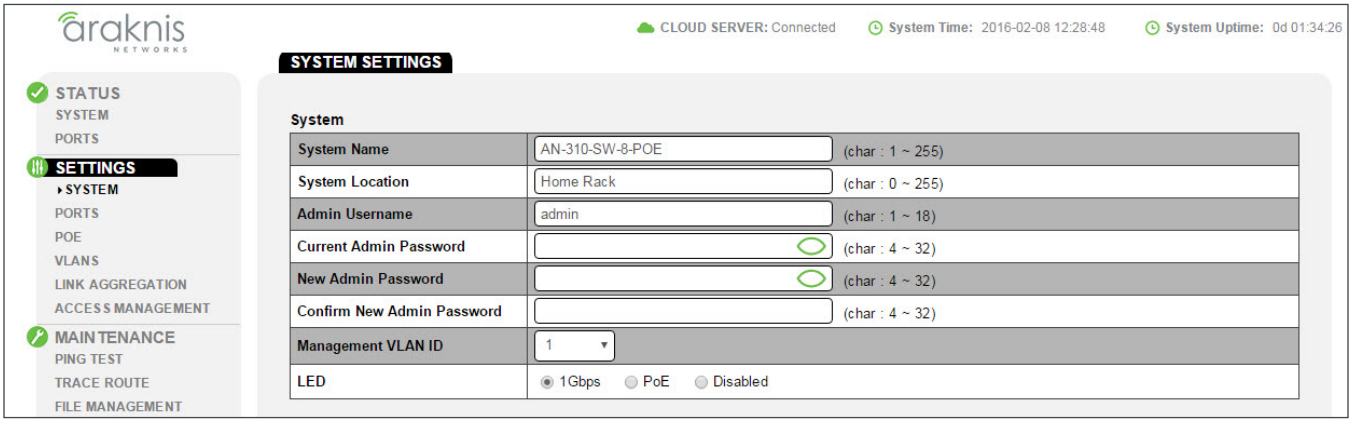
10 - System Settings

Configure system level settings.

System Information

Path – Settings, System, System

Figure 12. System Information Settings



- **System Name –** Assign a name for identifying the system.
- **System Location –** Describe the location of the switch.
- **Admin Username –** Enter a username for administrator access.
  Default: araknis.
- **Current Admin Password –** Enter the current password when changing the system name.
  Default: araknis.
- **New Admin Password –** Enter the new value when changing the administrator password.
- **Confirm New Admin Password –** Re-enter the new value when changing the administrator password. Must be the same as the above field.
- **Management VLAN ID –** Select the VLAN to be used when accessing the switch interface. All ports are set to VLAN 1 by default. Do not change this setting unless additional VLANs have been configured. Once the setting is changed, you will lose access to the interface unless your computer is connected to a port on the specified VLAN.
  Default: 1
- **LED –** Select what information is represented by the front panel port status LEDs. Options:
  - **1Gbps (default) –** Left RJ45 LED and front status LED ON indicates 1 Gbps connection.
  - **PoE –** Left RJ45 LED and front status LED ON indicates that a PoE-powered device is connected.
  - **Disabled –** All port and status LEDs are disabled.

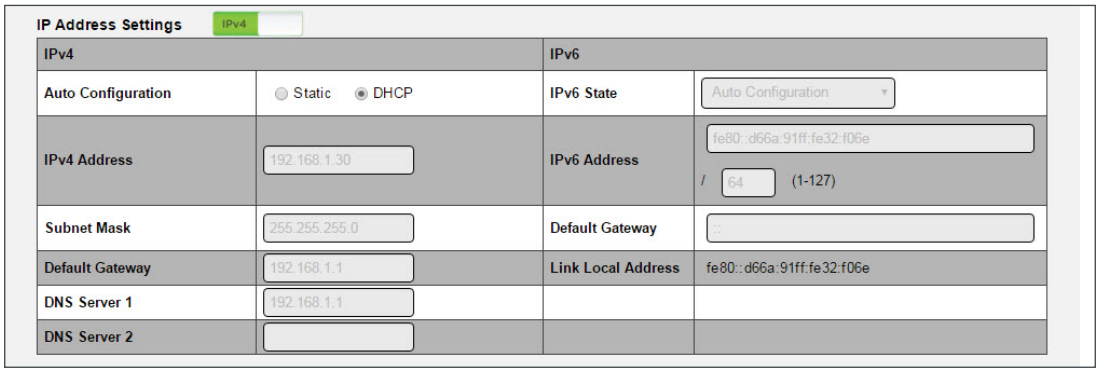
© 2016 Araknis Networks®

IP Address Settings

The switch may be addressed using either IPv4 or IPv6 addressing. Use the toggle at the top of the page to select the desired setting.

Path – Settings, System, IP Address Settings

Figure 13. IP Address Settings Menu



IPv4 IP Settings

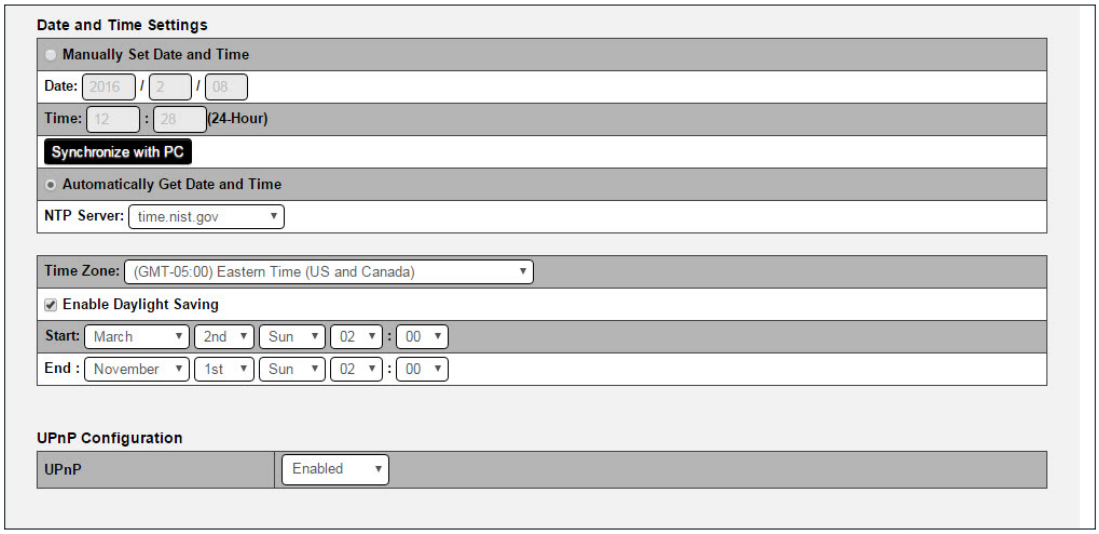
- **Auto Configuration –** Select the IP address mode. In DHCP mode, the switch will be issued IPv4 address settings by the DHCP server (if enabled, usually in the router). Use Static mode to manually set an IP address.
- **IPv4 Address –** IP address issued to the switch. Used for accessing the interface. Default: 192.168.20.254
- **Subnet Mask –** Identifies the subnet the IP address is part of. Default: 255.255.255.0
- **Default Gateway –** IP address of the Internet gateway device (usually the router).
- **DNS Server 1 –** IP address of the DNS Server. Usually the same as the Default Gateway.
- **DNS Server 2 –** (Optional) Enter a second DNS Server IP address.

IPv6 IP Settings

- **IPv6 State –** Auto Configuration, DHCPv6 Client, or Static.
- **IPv6 Address –** Displays the assigned IPv6 address and subnet mask.
- **Default Gateway –** IPv6 address of the Internet gateway device (usually the router).
- **Link Local Address –** Local routing address associated with a specific broadcast domain (VLAN).

© 2016 Araknis Networks®

Figure 14. Date and Time Settings, UPnP



Date and Time Settings

Path – Settings, System, Date and Time Settings

- **Manually Set Date and Time –** Select to manually set date and time.
  - **Date –** Enter the year, month and date (four digits for year; two digits for month, two digits for date)
  - **Time –** Enter the hour and minutes for the correct current time. Use a mobile device or satellite clock for accuracy.
- **Synchronize with PC –** Click this button to automatically sync the access point to a connected computer.
- **Automatically Get Date and Time –** Select to automatically get date and time from various web resources.
  - **NTP Server –** Select an NTP (Network Time Protocol) server for setting date and time. *Default: time.nist.gov.*
- **Time Zone –** Select the appropriate time zone from the drop-down.
- **Enable Daylight Saving –** Select to enable. DST start/end can change from year to year. Be sure to update this information.
  - **Start –** Select the month, date, day and time Daylight Saving Time starts from the drop downs.
  - **End –** Select the month, date, day and time Daylight Saving Time ends from the drop downs.

UPnP Setting

Path – Settings, System, UPnP Configuration

- **UPnP –** Allow the switch to act as a UPnP client. Enabled or Disabled.

Note – This setting will not affect OvrC Web Conect or OvrC web monitoring. Contact technical support if you need to disable OvrC functionality.

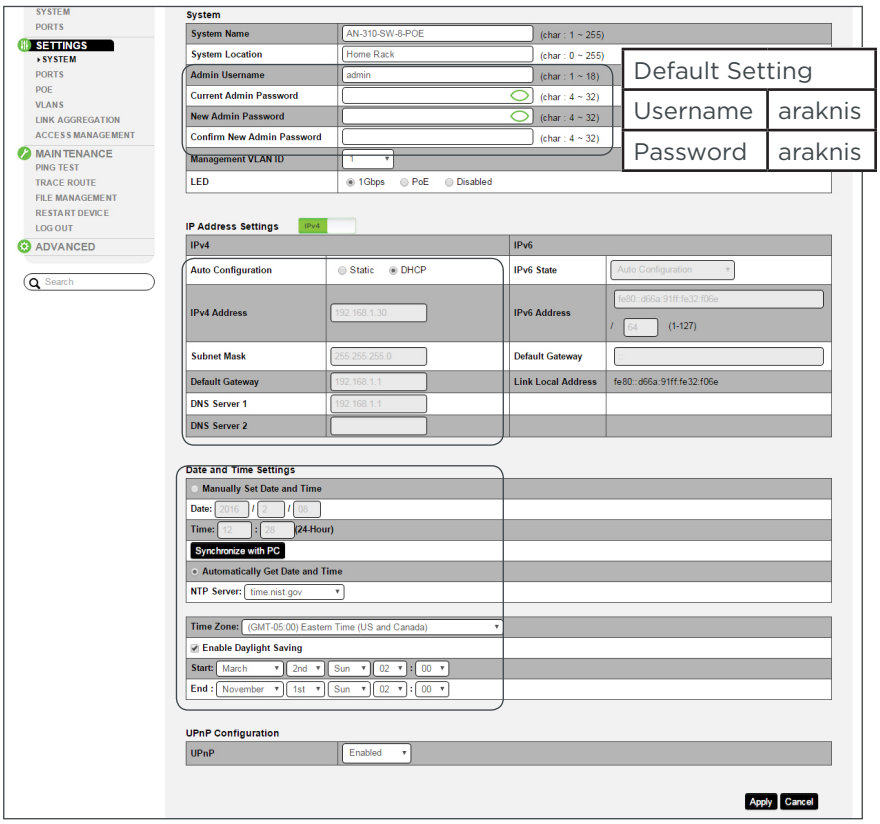
© 2016 Araknis Networks®

11 - Recommended Setup – System Settings

We recommend changing the following interface settings to provide the best security and performance. These are the minimum settings that should be changed on every install.

Path – Settings, System

Figure 15. Recommended System Settings



1. **Change Default User Name and Password**
   Enter a user name and password for the administrator account (System menu at the top of the page). This will prevent unauthorized access to the interface. (Default login: araknis; araknis) Record the new settings so you can log in after applying the changes.

2. **Configure System IP Address**
   Set an IP address for accessing the interface. We recommend a static IP so the address doesn't change. Record the address so you can access the interface later.

3. **Configure System Time and Date**
   We recommend using the Automatically Get Time and Date setting using the default server "time.nst.gov". This will ensure that scheduling features configured in the switch operate on the correct schedule.

4. **Configure other System Settings**
   Configure any other fields on the page as desired. See the previous section for all setting definitions.

5. **Save the new settings**
   Click the **Apply** button at the bottom right of the screen to save the new system settings. Enter the new user name and password when the login screen appears.

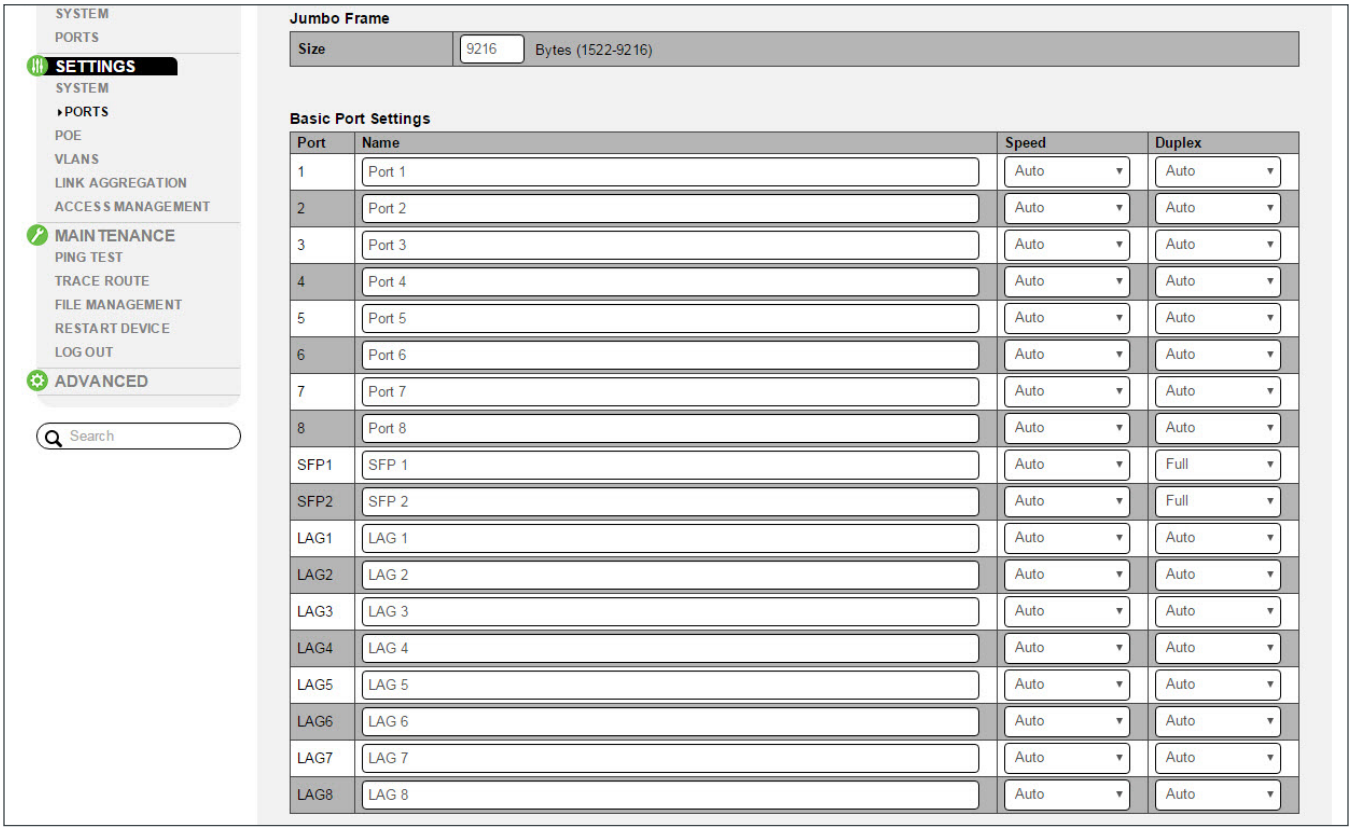
© 2016 Araknis Networks®

12 - Port Configuration Settings

Customize individual port settings and jumbo frame size.

Path – Settings, Ports

Figure 16. Jumbo Frame and Basic Port Settings



Jumbo Frame Setting

- **Size –** Sets the maximum frame size for traffic going through the switch. Received packets that exceed the maximum frame size are dropped. Range: 1518-9216 bytes.
  Default: 9216

Basic Port Settings

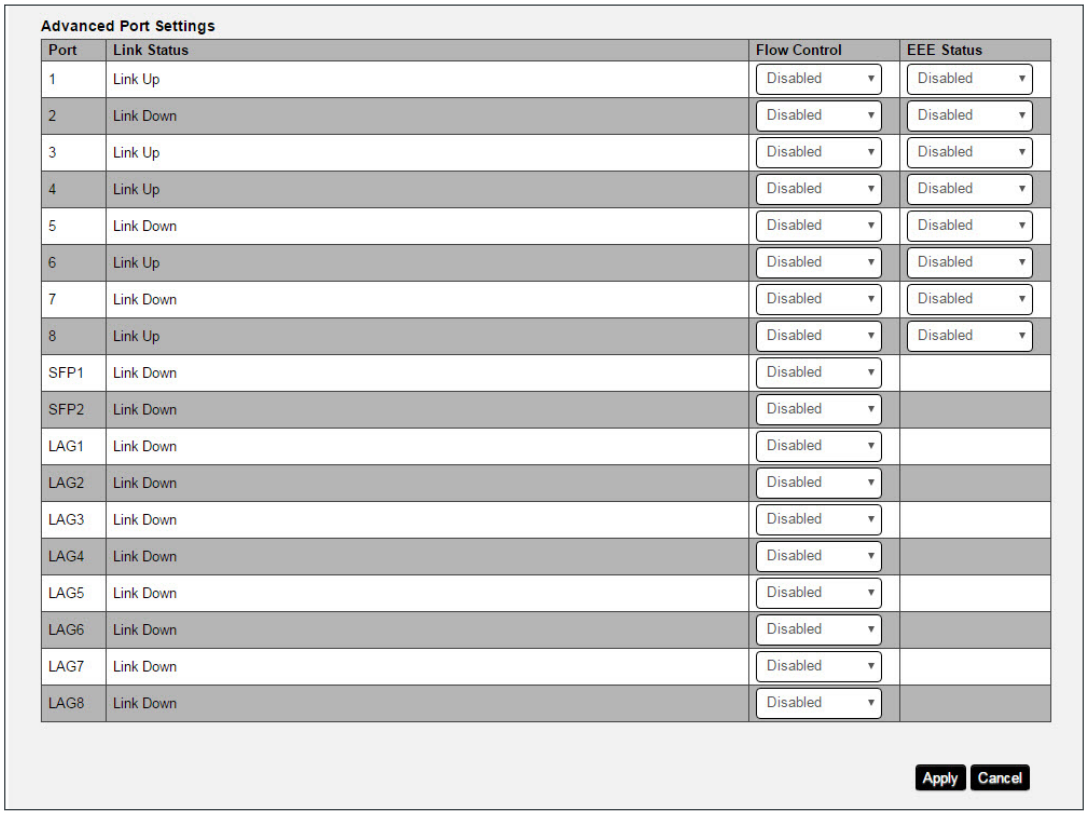
- **Port –** The number of the physical switch port.
- **Name –** The assigned name of the port.
- **Speed –** The current speed of the port based on the connected device in use. Auto, 1Gbps, 100Mbps, 10Mbps, or Disabled.
  Default: Auto
- **Duplex –** The current duplex setting with the connected device. Auto, Full or Half.
  Default: Auto

© 2016 Araknis Networks®

Advanced Port Settings

Path – Settings, Ports, Advanced Port Settings

Figure 17. Advanced Port Settings



- **Port –** The number of the physical switch port.
- **Link Status –** Current operating status of the port. Link up or Link down.
- **Flow Control –** Flow control can eliminate frame loss by "blocking" traffic from end devices or other network devices connected directly to the switch when the buffer is overloaded on a specific switch port. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation.
  Default: Disabled
- **EEE Status –** Energy Efficient Ethernet (EEE) is a standard defined by IEEE 802.3az to reduce LAN device power consumption during idle periods. With EEE enabled, compatible devices can go into LPI (Low Power Idle) mode during periods of low utilization and then turn back on when needed.
  Default: Disabled

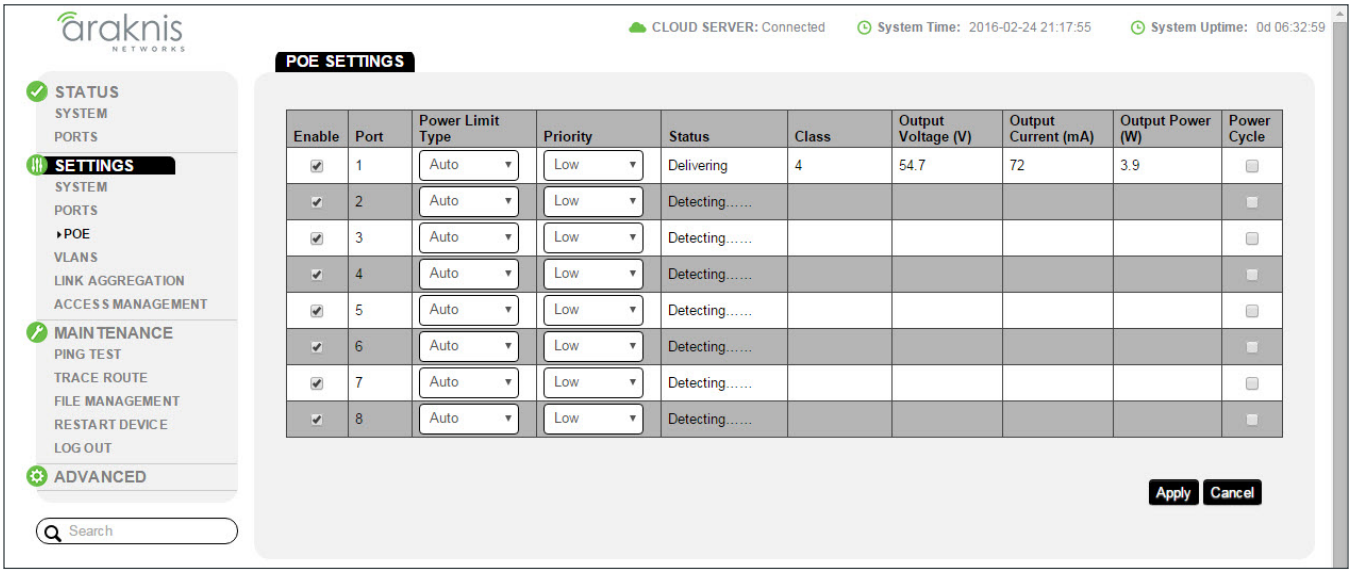
Note – EEE causes some network latency. If you experience latency problems with this mode enabled, try disabling the feature to determine if EEE is causing the issue.

© 2016 Araknis Networks®

13 - PoE Settings

The switch is designed to make PoE a plug-and-play affair for most applications. Use the PoE Settings menu to monitor, troubleshoot, and control each port.

Figure 18. PoE Settings Menu

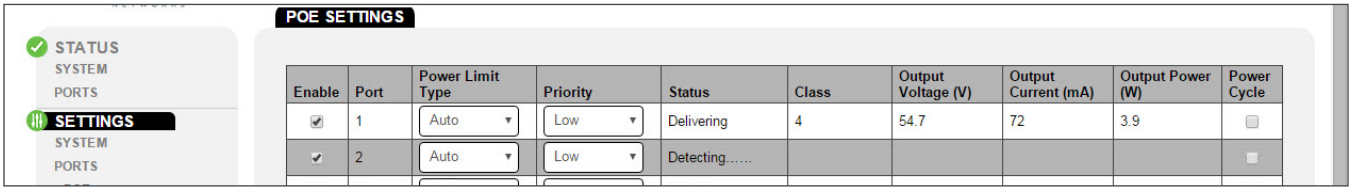


- **Enable –** Check the box to enable PoE on the specified port.
  Default: Enabled
- **Port –** The number of the physical switch port.
- **Power Limit Type –** Auto, 7W, 15.4W, or 30W.
  Default: Auto
- **Priority –** Port priority is used when remote devices require more power than the power supply can deliver. In this case, the ports with the lowest priority will be turned off starting from the port with the highest port number. Low, Medium, or High.
  Default: Low
- **Status –**
  - **Detecting –** The port is not providing PoE power and waiting for a connection that requires it. If a device is connected and status is still Detecting, then the device is not powered via PoE.
  - **Delivering –** The port is connected to a PoE device and power is being provided.
- **Class –** PoE Class of the connected device (1,2,3, or 4).
- **Output Voltage (V) –** PoE voltage being supplied to the port.
- **Output Current (mA) –** Current in milliamps being supplied to the port.
- **Output Power (W) –** Power in watts being supplied to the port.
- **Power Cycle –** Check the box and click **Apply** to power cycle PoE on one or more ports.

© 2016 Araknis Networks®

PoE Setup and Troubleshooting

Figure 19. PoE Settings Menu



Checking Status of PoE Devices

In the image above, a PoE-powered access point is connected to port 1 on the switch. The Status, Class and Output fields tell you that PoE is functioning correctly (Delivering), as well as how much power is being consumed. Update the page after changing port connections or settings on the page to refresh the table.

- **Status –** Options:
  - **Detecting –** The port is not providing PoE power. If a device is connected and status is still Detecting, see the PoE Troubleshooting section below.
  - **Delivering –** The port is connected to a PoE device and power is being provided.
- **Class –** PoE Class of the device connection.
- **Output Voltage (V) –** Voltage being supplied to the port.
- **Output Current (mA) –** Current in milliamps being supplied to the port.
- **Output Power (W) –** Power in watts being supplied to the port.

Configuring PoE Ports

Use these settings to customize PoE in situations where power is critical for certain equipment or if power must be disabled on a port.

- **Enable –** Check the box to enable PoE on the specified port.
- **Power Limit Type –** Auto, 7W, 15.4W, or 30W.
- **Priority –** Port priority is used when remote devices require more power than the power supply can deliver. In this case, the ports with the lowest priority will be turned off starting from the port with the highest port number. Low, Medium, or High.

Troubleshooting PoE Issues

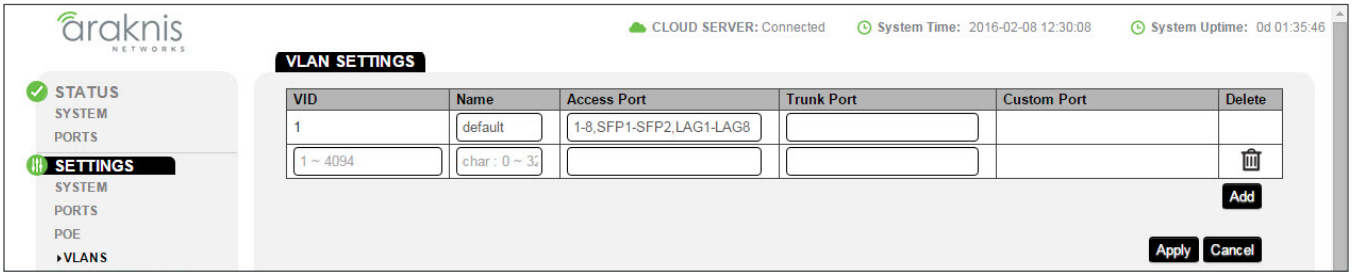
- **Power Cycle –** Check the box and click **Apply** to power cycle PoE on one or more ports.
- **Overcurrent Condition –** With default PoE settings, if the current drawn from PoE devices exceeds the total budget for the switch, PoE will be disabled on ports beginning with the highest numbered port.

© 2016 Araknis Networks®

14 - VLAN Settings (Basic Port-Based)

Use this menu to configure port-based VLANs. See the Understanding and Using VLANs white paper for more information about this feature and detailed setup examples and instructions. By default, all ports are assigned to VLAN 1 as untagged ports.

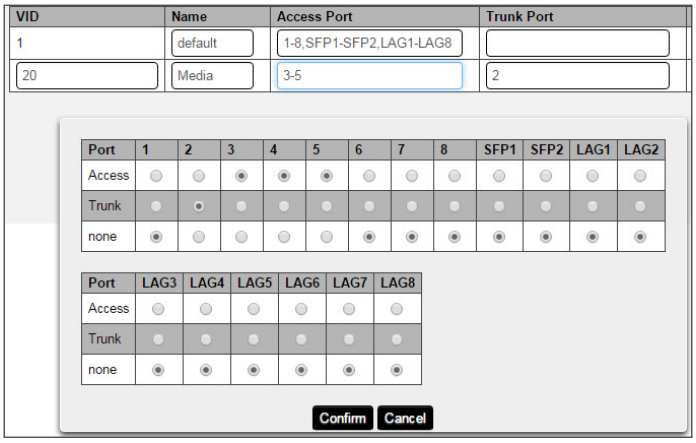
Figure 20. VLAN Settings



- **VID –** VLAN ID.
- **Name –** Use this field to enter a custom VLAN name for easy identification.
- **Access Port –** Ports and LAGs assigned to the VLAN. The switch tags untagged packets from assigned Access Ports with the specified VLAN ID. See the figure below for information about changing settings.
- **Trunk Port –** Trunk port/s assigned to the VLAN. Trunk Ports send tagged packets to other devices.
- **Custom Port –** Displays ports assigned to the VLAN that have customized settings. Customizations can be made in the Advanced VLAN configuration menus. See section “Advanced VLANs – 802.1Q VLANs” on page 61.
- **Delete –** Click the trash can icon then click **Apply** to delete a VLAN definition.

Access and Trunk Port Selection

Figure 21. Access and Trunk Port Selection



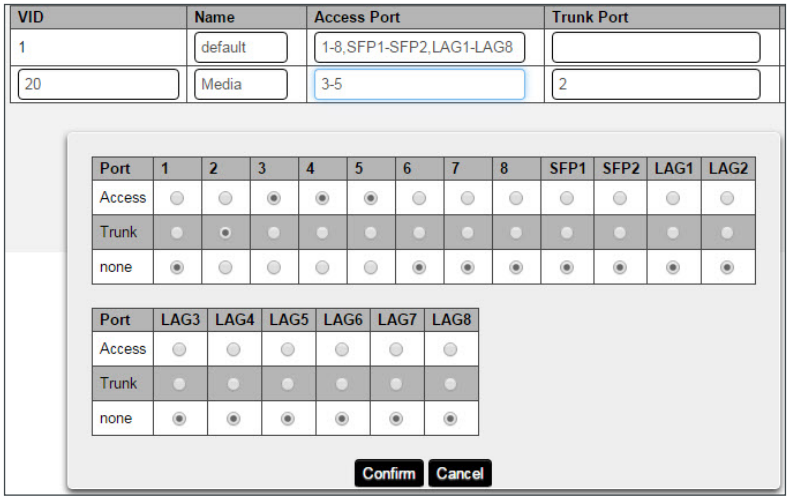
- **Access Port –** Ports and LAGs assigned to the VLAN. The switch tags untagged packets from assigned Access Ports with the specified VLAN ID.
- **Trunk Port –** Trunk port(s) assigned to the VLAN. Trunk Ports send tagged packets to other devices.
- **none –** These ports are not included in the VLAN.

© 2016 Araknis Networks

Creating a New VLAN

1. Click the **Add** button to create a new entry.
2. Enter a VLAN ID and name for the new entry.
3. Assign access and trunk ports by clicking either **Port** field to open the assignment window, then selecting the function of each port as it relates to that VLAN. You may also assign Link Aggregation Groups to VLANs in the menu.
   - **Access Port –** Ports and LAGs assigned to the VLAN. The switch tags untagged packets from assigned Access Ports with the specified VLAN ID.
   - **Trunk Port –** Trunk port/s assigned to the VLAN. Trunk Ports send tagged packets to other devices.
   - **none –** These ports are not included in the VLAN.
4. Click **Confirm** to close the window. The selections will appear in the Access and Trunk Port fields.
5. Click **Apply** to save the new settings.

Figure 22. Configuring Ports in a VLAN



In this example, for VLAN 20, Ports 3-5 are configured as Access ports and Port 2 is assigned as a Trunk port. The remaining ports are left set to none and remain on the default VLAN 1.

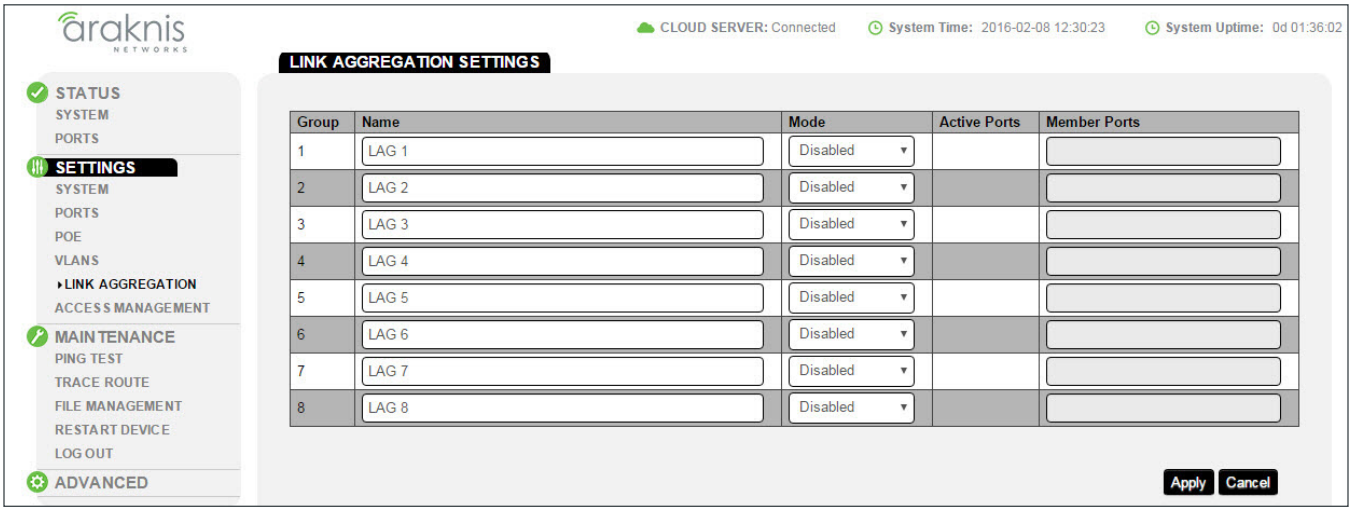
© 2016 Araknis Networks®

15 - Link Aggregation Settings

Link Aggregation is also known as Port Trunking. It allows using multiple ports in parallel to increase the link speed between two switches, increasing redundancy for higher availability.

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks must be manually configured at both ends of the link. You can configure any number of ports on the switch to use LACP as long as they are not already configured as part of a static trunk.

Figure 23. Link Aggregation Settings Menu

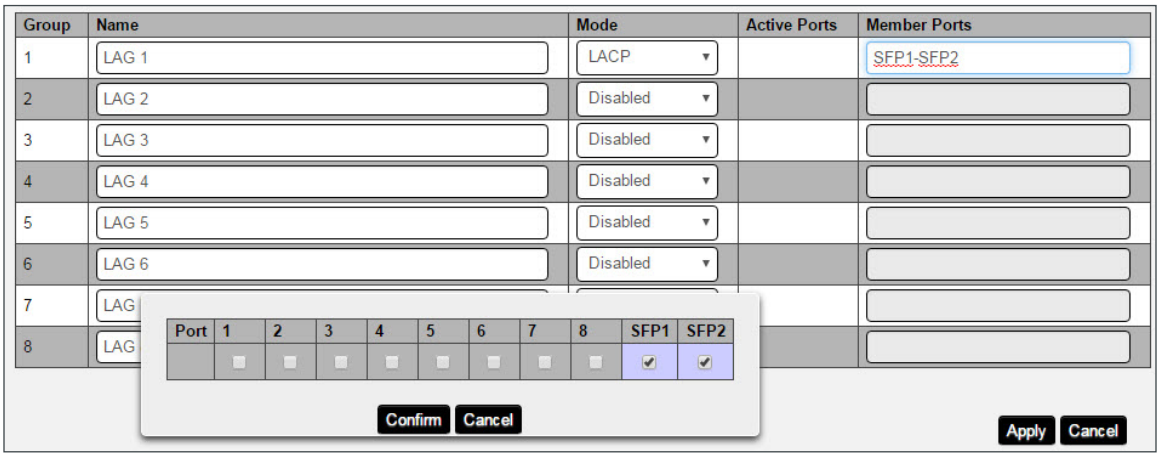


- **Group –** Number of the group configured in the rule.
- **Name –** Enter a custom name for the group being configured.
- **Mode –** Select whether the rule is disabled, static, or LACP.
  Default: Disabled
- **Active Ports –** Displays ports being actively used for LAG.
- **Member Ports –** Click to select member ports for the group.

© 2016 Araknis Networks®

Creating a New Link Aggregation Rule

1. Change the name of the group as desired.
2. Select the operating mode for the group:
   - **Disabled –** No Link Aggregation.
   - **Static –** All traffic is balanced evenly between the ports.
   - **Dynamic –** Traffic is sent based on LACP protocol.
3. Click the **Member Ports** field to open the assignment window, then select the member ports to be used for LAG.
4. Click **Confirm** to close the window. The selections will appear in the Member Port field.
5. Click **Apply** to save the new settings.



In this example, for Group 1, both SFP ports are configured as Member ports using LACP.

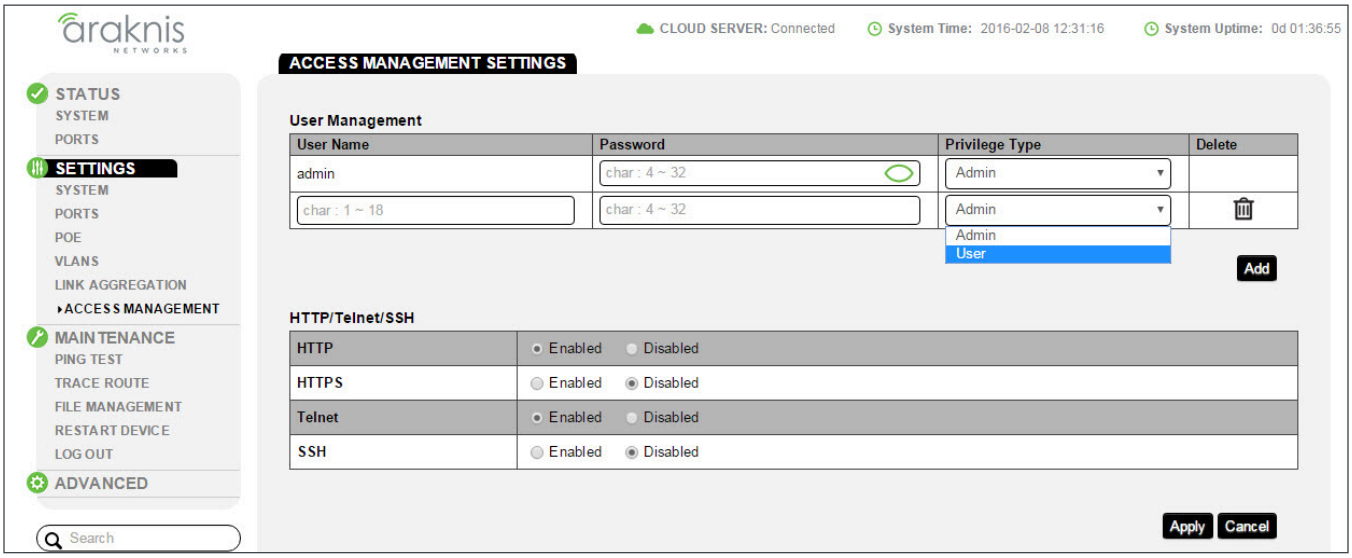
Note – LACP must be configured in equipment on both sides of the link to operate correctly.

© 2016 Araknis Networks®

16 - Access Management Settings

Configure user account permissions and what access protocols may be used for access.

Figure 24. Access Management Menu Page



User Management

- **User Name –** Enter a user name for the account. 1-18 characters. Not case sensitive.
- **Password –** Enter a password for the account. 4-32 characters. Case sensitive.
- **Privilege Type –** Select whether the account has user or admin level account functionality. Options:
  - **Admin –** Full access and control of the entire local interface.
  - **User –** Limited to viewing current settings in all menus.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry (must click Apply to save the setting). The default admin account cannot be removed.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

> **Note –** The user name of the primary account must be changed in the System Settings menu. See section “10 - System Settings” on page 23.

HTTP/Telnet/SSH

- **HTTP –** Select whether the local interface may be accessed using HTTP. This is the most common access method.
  Default: Enabled
- **HTTPS –** Select whether the interface can be accessed using HTTPS.
  Default: Disabled
- **Telnet –** Select whether the switch will accept Telnet commands.
  Default: Enabled
- **SSH –** Select whether the switch will accept SSH commands. Default: Disabled
  Default: Disabled

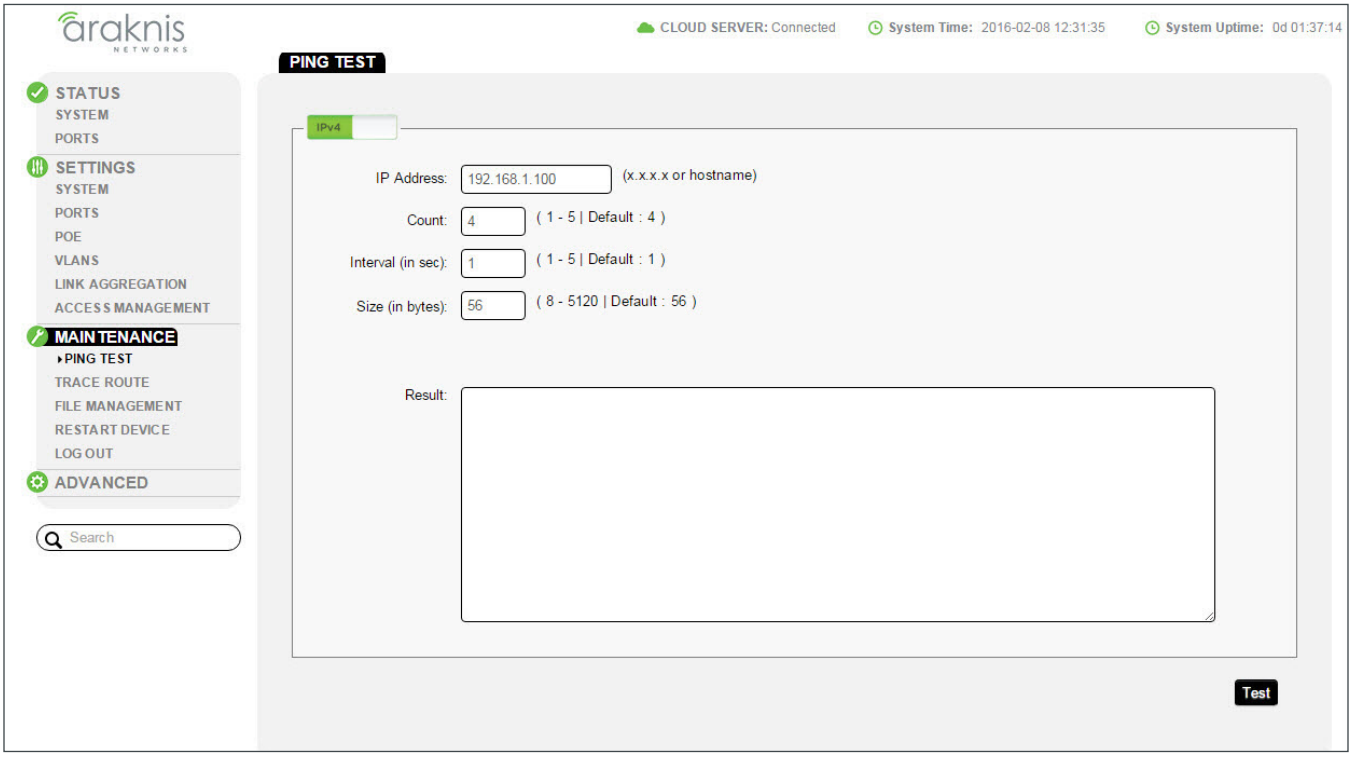
© 2016 Araknis Networks®

17 - Maintenance Menus

Ping Test

Send ICMP echo request packets to another device on the network to determine if it can be reached. Use the Ping test to determine whether a device or host is communicating correctly.

Figure 25. Ping Test Page



- **IP Address –** Enter the IP address of a device or web page to be pinged.
- **Count –** Number of ping attempts (1-5).
  Default: 4
- **Interval –** Number of seconds between pings (1-5).
  Default: 1
- **Ping Packet Size –** Enter the packet size of each ping (8-5120 bytes). Change to test MTU issues.
  Default: 56 Bytes
- **Result –** Displays results of the test in real time. Resize screen table using bottom right corner click-drag.
- **Test –** Click to start the ping test.

Running a Ping Test

1. Enter the target IP address into the IP Address field.
2. Change other parameters if desired. The default settings are a great start for troubleshooting.
3. Click **Test** and wait for the results to appear. See the next page for help understanding results.

© 2016 Araknis Networks®

Understanding Ping Test Results

Figure 26. Successful Ping Test Result

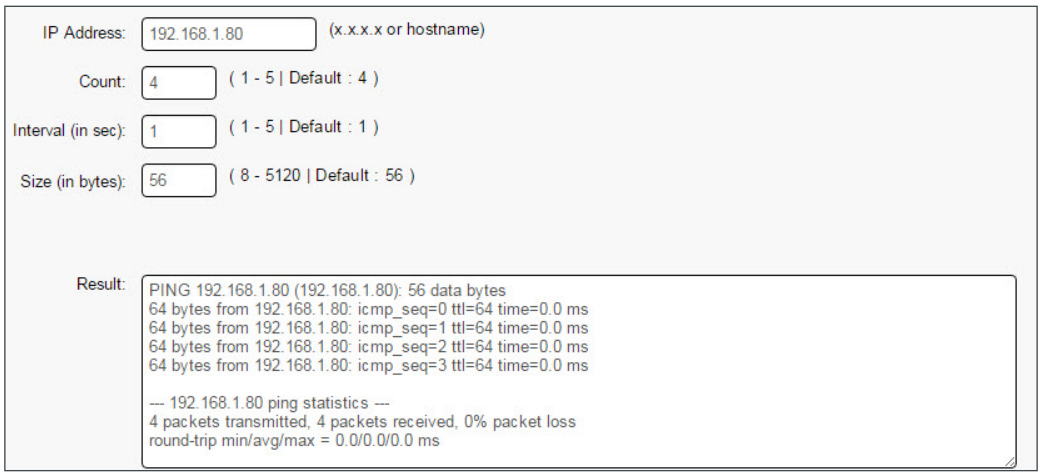
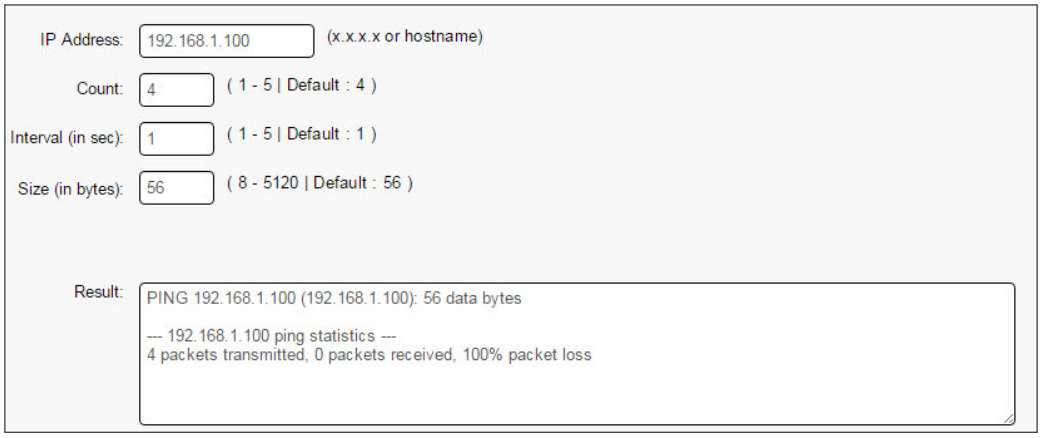


Figure 27. Failed Ping Test Result



- The first line shows the IP address pinged. If a URL was entered (example: google.com) then the IP address will be displayed also.
- If a ping is successful, the details of each packet are displayed one per line. Note how the successful ping above has four lines beginning with ***64 bytes from...*** whereas the failed ping does not.
- Ping Statistics are displayed last. Describes the number of packets (pings) transmitted, the number of packets received from the target in response, percent packet loss, and, if successful, the minimum, average, and maximum round trip timing of the packets.

Troubleshooting Using Ping Test Results

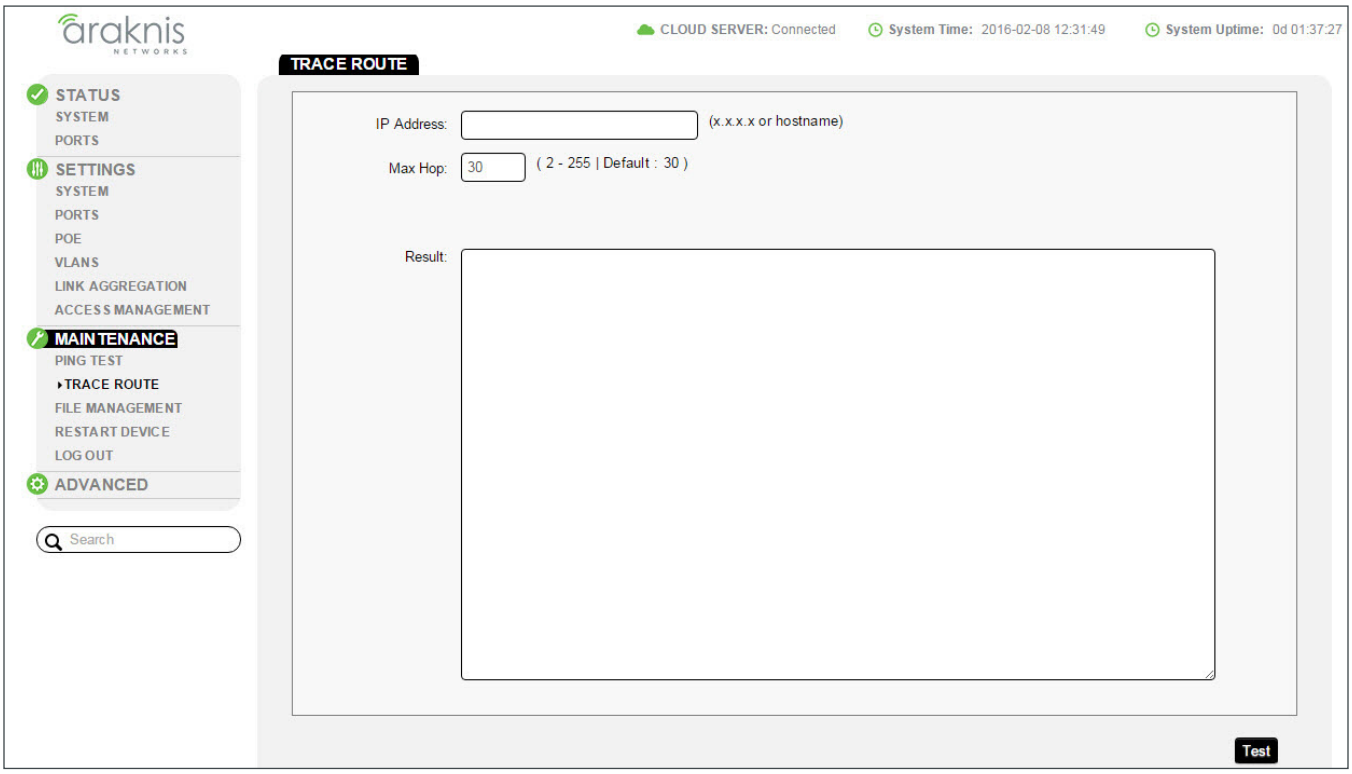
- If no packets are received, check the connections between the switch and the target device first. The target device may not be connected. If the connection is good, reset or power cycle the target device. It may have become unresponsive.
- If packets are still not received, check for a bad cable, port, or failing equipment. Try changing the connections to a known, working path.
- If everything checks out, but still no packets are received, there may be a traffic issue due to network settings like VLAN or ACL misconfiguration. Check settings related to the ports, IP addresses, and MAC addresses in use.

© 2016 Araknis Networks®

Trace Route Test

The Trace Route test uses a ping to tell you what path a packet takes to travel between the switch and the target device by counting the number of hops (hops happen when a packet is forwarded from one router to another). Trace route is primarily used to troubleshoot issues with connections over the WAN port because on the LAN there is rarely more than one router for the packet to pass through.

Figure 28. Trace Route Test Page



- **IP Address –** Enter the IP address of a device or web page to ping for the test.
- **Max Hop –** Enter the maximum number of hops to be recorded in the Ping test (2-55). *Default: 30*
- **Result –** Displays the results of the test in real time. Resize screen table using bottom right corner click-drag.
- **Test –** Click the button to start the Traceroute test.

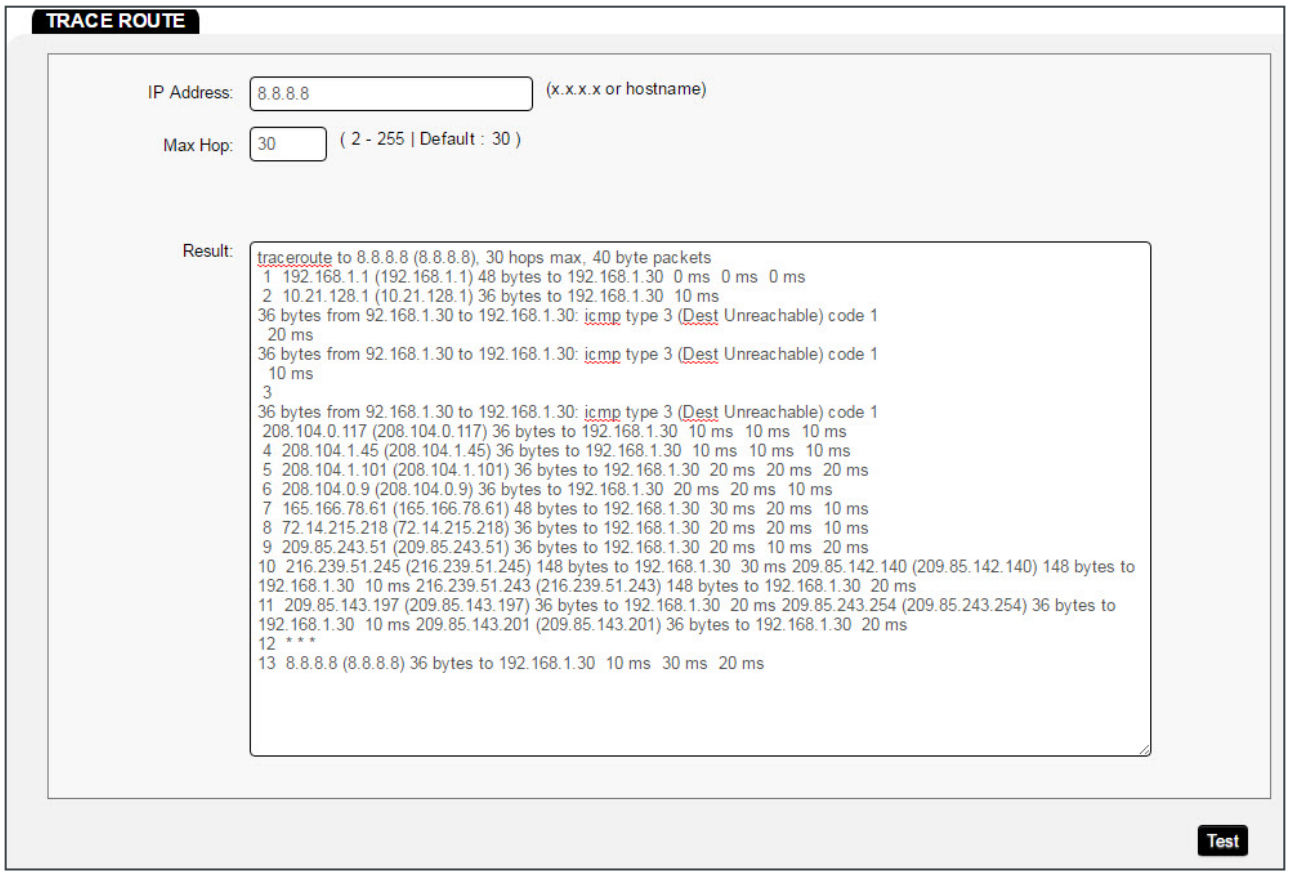
Running a Trace Route Test

1. Enter the target IP address into the IP Address field.
2. Click **Test** and wait for the results to appear. See the next page for help understanding results.

© 2016 Araknis Networks®

Understanding Trace Route Test Results

Figure 29. Trace Route Result



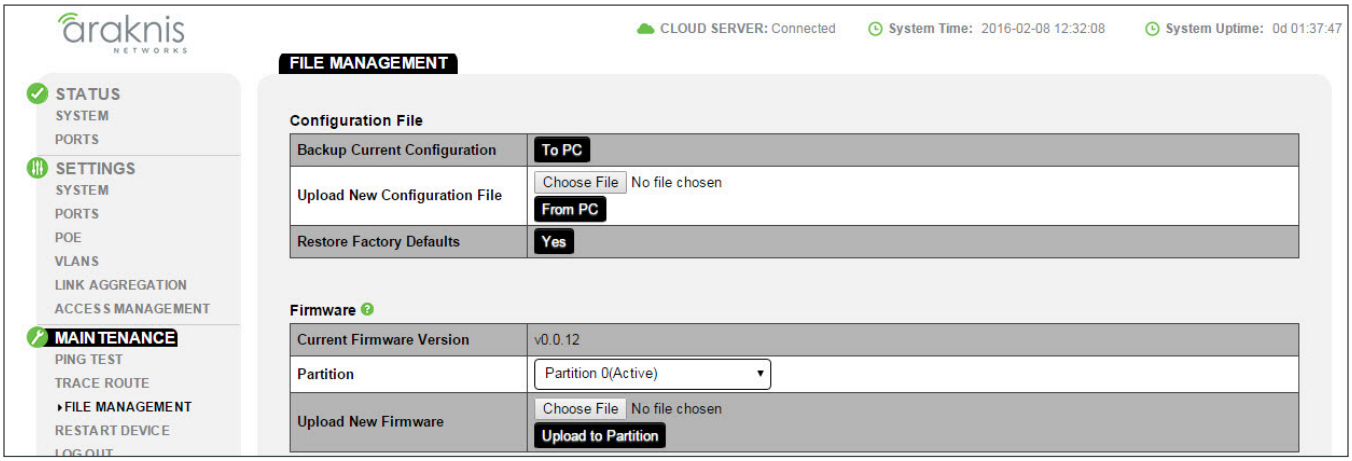
- The results window displays the parameters for the test, followed by information about each hop or hop attempt.
- Each line starting with a number indicates a hop in the path to the target IP address. Only hops between routers are shown, not between switches.
- Each hop is tested three times. In each hop entry, the send and receive IP address are shown, followed by the amount of time it took for the hop to occur on each of the three attempts.

© 2016 Araknis Networks®

File Management Settings

Save configuration files (of current switch settings) and upgrade firmware.

Figure 30. File Management Menu



Configuration File

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

- **Backup Current Configuration –** Save the current configuration settings to a compressed archive on your computer. Click the To PC button and select a location to save the file.
- **Upload New Configuration File –** Restore previously saved configuration settings. Click Choose File and select a configuration from the Open window. Then, click the From PC button to upload the configuration file.
- **Restore Factory Defaults –** Click the Yes button to restore all factory default settings.

Firmware

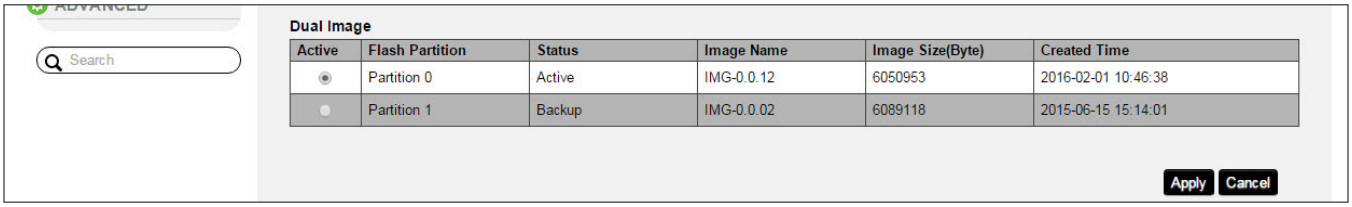
- **Current Firmware Version –** Indicates the current firmware version on the selected partition.
- **Partition –** Select the partition to change firmware for:
  - **Partition 0 –** Default partition.
  - **Partition 1 –** Backup partition. (In the event of one partition failing, the switch will reboot and use the alternate firmware.)
- **Upload New Firmware –** Upload a new firmware version to the selected partition. Click Choose File to select a file from your computer. Click Upload to Partition to load the firmware.

© 2016 Araknis Networks®

Dual Image

Select which partition the switch runs on. In the event of one partition failing, the switch will reboot and use the alternate firmware.

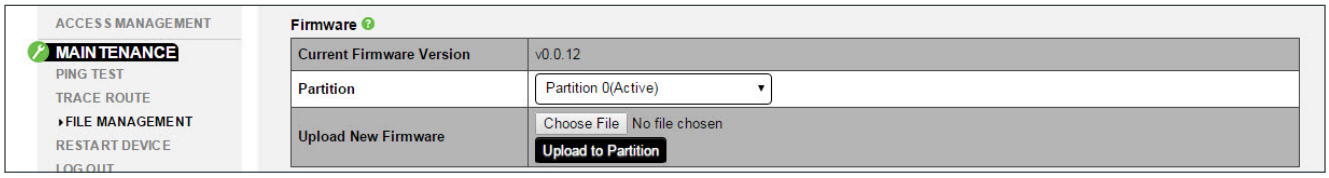
Figure 31. Dual Image Menu



- **Active –** Select the desired partition and click Apply to reboot the switch from the firmware on the selected partition.
- **Flash Partition –** Name of the partition.
- **Status –** Current partition status:
  - **Active –** The partition the switch is currently operating from.
  - **Backup –** The partition the switch is NOT currently operating from.
  - **Image Name –** Firmware version currently loaded on the partition.
  - **Image Size (Bytes) –** File size of the firmware on the partition.
  - **Created Time –** Time and date the firmware file was uploaded to the partition.

Firmware Update Instructions

1. Download the new firmware from the product support tab. Extract the firmware from the zip file to a know location on your computer.
2. Navigate to the Maintenance > File Management > Firmware menu.

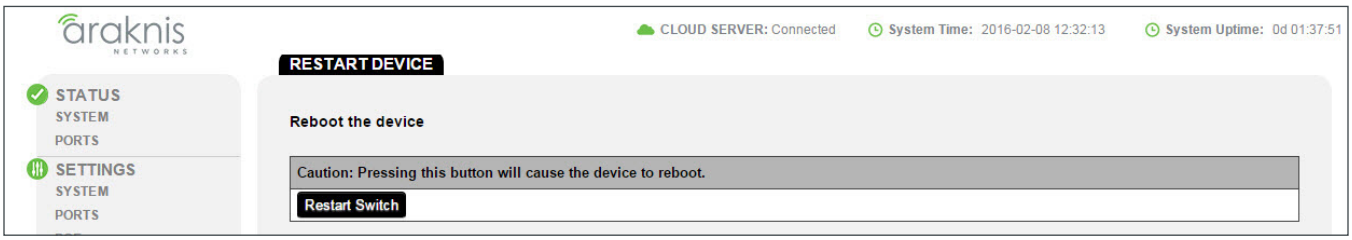


3. Click the **Choose File** button for Upload New Firmware, then find and select the new firmware and click **Open**.
4. Click Upload to Partition then follow the prompts to complete the update for the first partition.
5. After the first partition is updated, repeat the process, but before clicking **Upload to Partition**, select the alternate partition from the **Partition** drop down.
6. After the alternate partition uploads, the process is complete.

© 2016 Araknis Networks

Restart

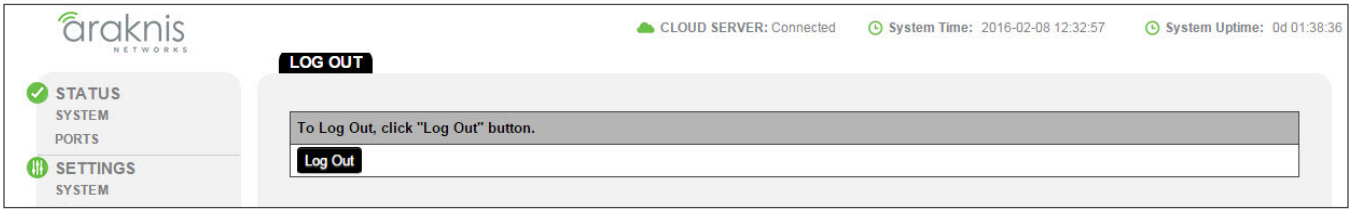
Figure 32. Restart Page



- **Restart Switch –** Click to restart the switch. No settings will be lost, but Ethernet will drop for connected devices until the restart is complete (~ 60 seconds). The login screen will reload once the restart is complete.

Log Out

Figure 33. Log Out Page



- **Log Out –** Click to log out from the current session. The login screen will reload once the logout is complete.

© 2016 Araknis Networks®

18 - Advanced Menus

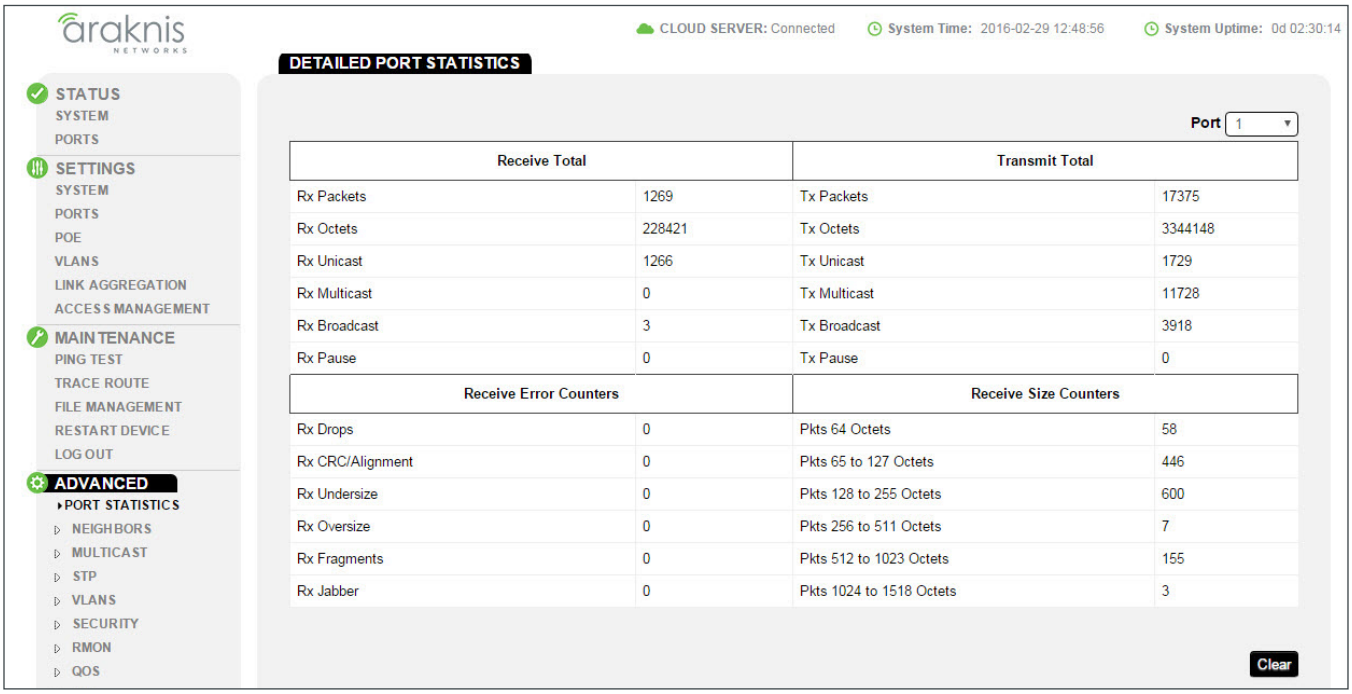
The remaining menus are meant only for advanced users. Proper setup and use of these features requires advanced networking knowledge.

© 2016 Araknis Networks®

19 - Advanced Port Statistics

Use the Detailed Port Statistics page to display detailed statistics for each switch port. This information can be used to identify potential problems with the switch (like a faulty port or an unusual traffic drop).
All values displayed are accumulated in each respective counter since the last system reboot or the last time you cleared the counters. Statistics are refreshed every 1 second by default. Use the drop-down menu at the top-right of the page to select a switch port. Click the **Clear** button to reset the statistics for the selected port.

Figure 34. Detailed Port Statistics



- **Receive/Transmit Total**
  - **Packets –** The number of all packets sent and received (good and bad).
  - **Octets –** The number of all bytes sent and received (good and bad), including Frame Check Sequence, but excluding framing bits.
  - **Unicast –** The number of unicast packets sent and received (good and bad).
  - **Multicast –** The number of multicast packets sent and received (good and bad).
  - **Broadcast –** The number of broadcast packets sent and received (good and bad).
  - **Pause –** A count of the MAC Control frames sent or received on a switch port that have an operation code indicating a PAUSE operation.
- **Receive Error Counters**
  - **Rx Undersize –** Total number of frames received that were less than 64 octets long excluding framing bits, but including FCS octets.
  - **Rx Oversize –** Total number of frames received that were longer than the configured maximum frame size for the particular switch port excluding framing bits, but including FCS octets.
  - **Rx Fragments –** Total number of frames received that were less than 64 octets in size excluding framing bits, but including FCS octets and had either an FCS or alignment error.

Continues on next page

© 2016 Araknis Networks®

Advanced Port Statistics, Continued

- **Rx Jabber –** Total number of received frames that were longer than the configured maximum frame size for the particular switch port excluding framing bits, but including FCS octets, and had either an FCS or alignment error.
- **Rx Drops –** The number of ingress packets that were dropped not due to errors in those packets. This might be a result of a congested link and switch port buffer overload.
- **Rx CRC/Alignment –** The number of frames received with CRC or alignment errors.

- **Receive Size Counters –** The number of packets sent and received (good and bad) divided into categories based on packet frame sizes.
- **Receive/Transmit Queue Counters –** The number of packets sent and received divided into categories based on QoS output queue.

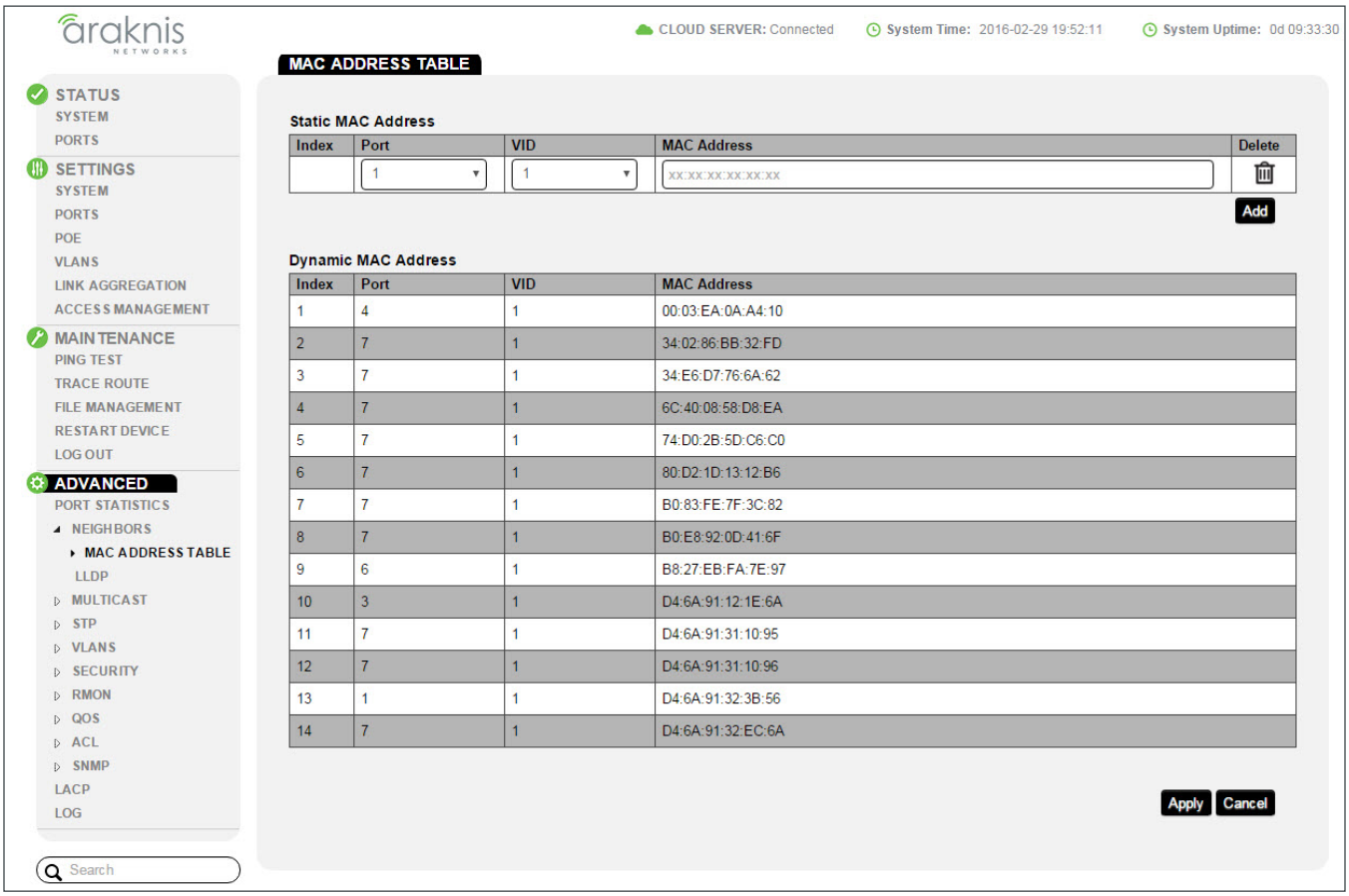
© 2016 Araknis Networks®

20 - Neighbors – MAC Address Table

See MAC addresses connected to ports on the switch and add static entries. Static entries are useful for:

- Speeding up recovery for critical devices after a reboot or power cycle (the switch is not required to poll the port for connected static MACs)
- Allowing virtual machines to be recognized on a port by MAC address

Figure 35. Neighbors MAC Address Table



Static and Dynamic MAC Address

- **Index –** Identifier number for the MAC entry.
- **Port –** Physical port or trunk on the switch.
- **VID –** The VLAN ID associated with the entry.
- **MAC Address –** Physical address associated with this interface.
- **Port Members –** The ports associated with this entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

© 2016 Araknis Networks®

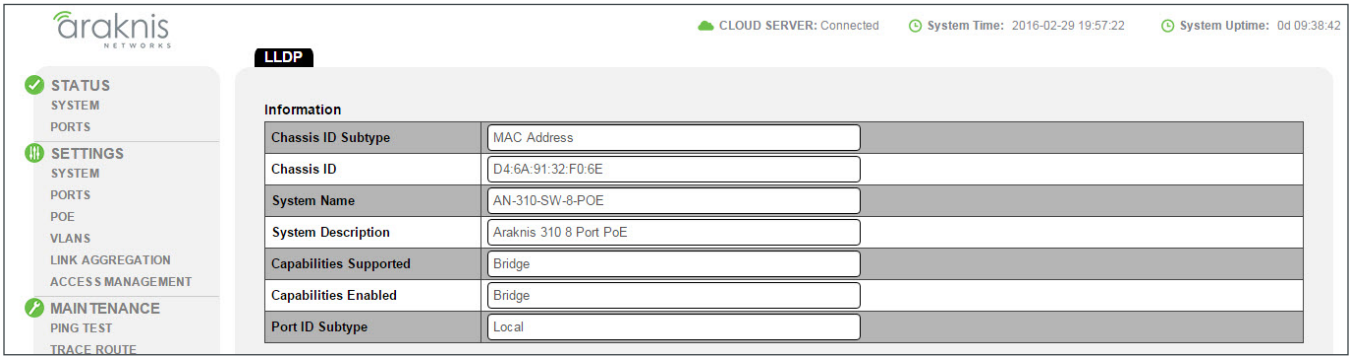
21 - Neighbors – LLDP

Link Layer Discovery Protocol (LLDP) is used to discover basic information about other devices in the same broadcast domain (i.e. VLAN). Advertised information is defined in the IEEE 802.1AB standard, and can include device details such as their identity (eg. make/model), capabilities (eg. routing/switching), and configuration settings.

Information Table

Araknis switch parameters shared using LLDP.

Figure 36. LLDP Information



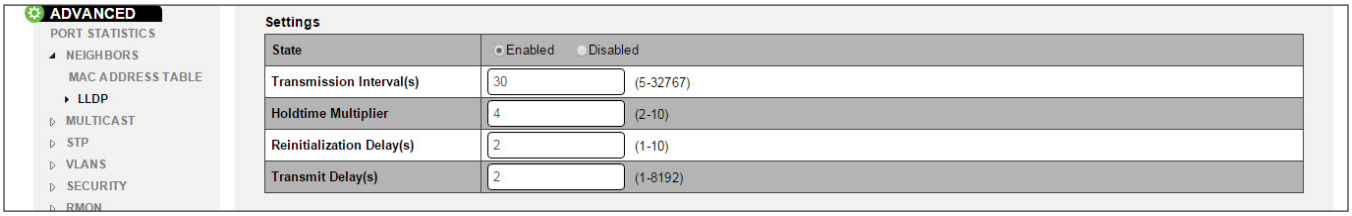
- **Chassis ID Subtype –** Method used for device identification.
- **Chassis ID –** MAC Address of the switch.
- **System Name –** System name of the switch (configured in the System Settings menu).
- **System Description –** System make and model.
- **Capabilities Supported –** Displays the capabilities of the switch; bridge only.
- **Capabilities Enabled –** Displays the currently enabled capabilities of the switch; bridge only.
- **Port ID Subtype –** Identifier subtype for the switch. Always displays ***Local***.

© 2016 Araknis Networks®

Settings

Customize settings for LLDP transmission.

Figure 37. LLDP Settings

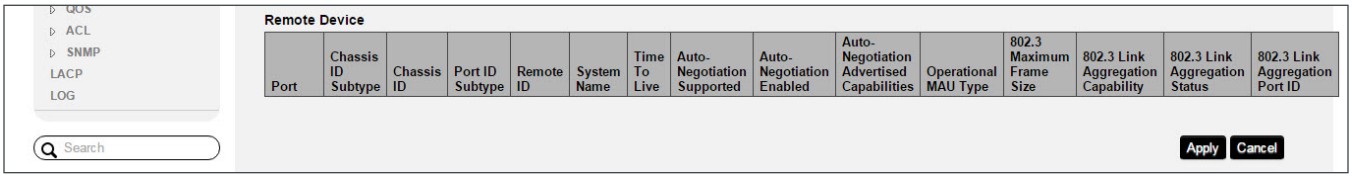


- **State–** Select whether LLDP is enabled or disabled.
- **Transmission Interval(s) –** How often LLDP information is transmitted. Range: 5-32767 seconds.
  Default: 30 seconds
- **Holdtime Multiplier –** Multiplied by the transmission interval value to generate the TTL time transmitted to neighbors. Range: 2-10.
  Default: 4
- **Reinitialization Delay(s) –** Amount of time to wait before initializing LLDP on a port. Range: 1-10 seconds.
  Default: 2
- **Transmit Delay(s) –** Minimum amount of time to wait before sending updated LLDP information after a configuration change. Range: 1-8192 seconds.
  Default: 2

Remote Device Table

This table displays LLDP information shared by connected equipment with LLDP features.

Figure 38. LLDP Remote Device Menu



- **Port –** Connected port for the device on the switch.
- **Chassis ID Subtype –** Type of information used for subtype. Typically MAC address.
- **Chassis ID Port ID Subtype –** Identification value. Typically MAC address.
- **Remote ID System Name –** Displays the configured system name of the connected device.
- **Time To Live –** TTL value for the received LLDP information.
- **Auto-Negotiation Supported/Enabled/Advertised Capabilities –** Interface auto-negotiation capabilities of the connected port.
- **Operational MAU Type –** Current Medium Attachment Unit type of the connected port.
- **802.3 Maximum Frame Size –** Maximum support Energy Efficient Ethernet frame size of the connected port.
- **802.3 Link Aggregation Capability/Status/Port ID –** Link aggregation parameters of the connected port.

© 2016 Araknis Networks

22 - Multicast – IGMP Snooping

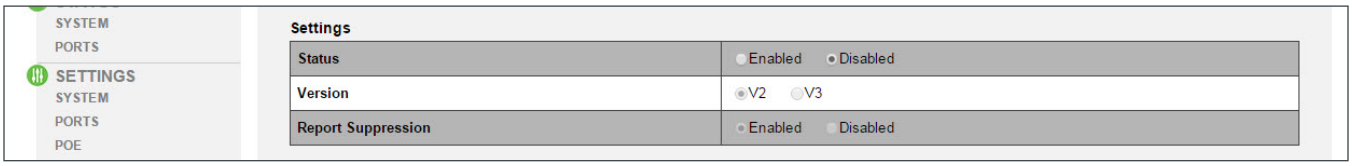
Internet Group Management Protocol (IGMP) can be used to filter multicast traffic on the switch. IGMP Snooping passively monitors exchanges between connected clients and an IGMP-enabled multicast server to discover and connect clients that want to join a multicast group.

Use the IGMP Snooping page to display IGMP snooping statistics and port status, configure global and port specific IGMP settings, and information on source-specific groups.

Settings

Configure global settings for IGMP Snooping.

Figure 39. IGMP Snooping Settings

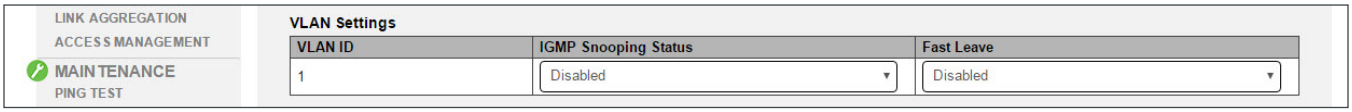


- **Status –** Enable or disable IGMP Snooping. When enabled, the switch monitors network traffic passing through it to determine which connected clients want to receive multicast traffic.
  Default: Disabled
- **Version –** Select IGMPv2 or v3.
- **Report Repression –** Enable to prevent the router from seeing the IGMP messaging that occurs at the client level. This alleviates load on the router, because the switch acts as a proxy for client level messages (like leave requests).
  Default: Enabled

VLAN Settings

Configure IGMP Snooping settings for individual VLANs.

Figure 40. IGMP Snooping VLAN Settings



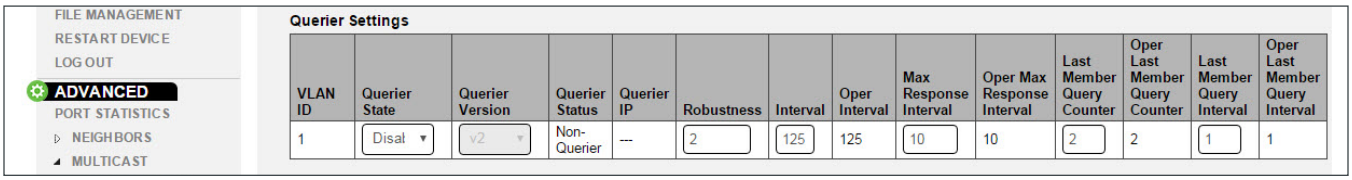
- **VLAN ID –** VLAN identifier.
- **IGMP Snooping Status –** Enable or disable IGMP Snooping for the VLAN.
- **Fast Leave –** Enable to allow subscribed multicast clients to leave without a response message.

© 2016 Araknis Networks®

Querier Settings

IGMP Query can be used to ask connected clients if they want to receive a specific multicast service. Then the ports containing clients requesting to join the service are identified, and multicast data is sent to only those ports. It then broadcasts the service request to any neighboring multicast switch to ensure that it will continue to receive the multicast service from a server connected to that switch.

Figure 41. IGMP Snooping Querier Settings



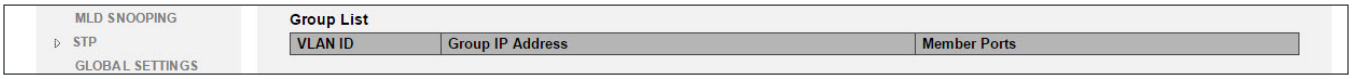
- **VLAN ID –** VLAN identifier.
- **Querier State –** Enable to make the switch the querier for the VLAN. Typically used when there is no multicast router acting as the querier.
  Default: Disabled
- **Querier Version –** Select IGMPv2 or v3 IGMP Snooping support (regardless of what clients support).
- **Querier Status –** Displays whether the switch is currently acting as the querier for the VLAN.
- **Querier IP –** IP address of the switch acting as querier for the VLAN.
- **Robustness –** Variable for resending querier messages. A higher value means that packets will be resent more often, useful for congested networks.
  Default: 2
- **Interval –** How often the switch sends IGMP host querier messages.
  Default: 125 seconds
- **Oper Interval –** Current reported IGMP host querier message interval.
- **Max Response Interval –** Maximum response time advertised in IGMP queries. This value must be lower than the query interval.
  Default: 10 seconds
- **Oper Max Response Interval –** Current reported maximum response time.
- **Last Member Query Counter –** Number of times the switch sends an IGMP query, separated by the last member query response interval, in response to a host leave message from the last known active host on the subnet. It is recommended to leave this setting at 2 in order to avoid multicast issues.
  Default: 2
- **Oper Last Member Query Counter –** Current reported Last Member Query Counter value.
- **Last Member Query Interval –** Time to wait after receiving a host leave message from the last known active host on the subnet. If no reports are received in the interval, the group state is deleted. Use this value to tune how quickly the software stops transmitting on the subnet.
  Default: 1 second
- **Oper Last Member Query Interval –** Current reported Last Member Query Interval.

© 2016 Araknis Networks®

Group List

See current group subscriptions by VLAN.

Figure 42. IGMP Snooping Group List Settings

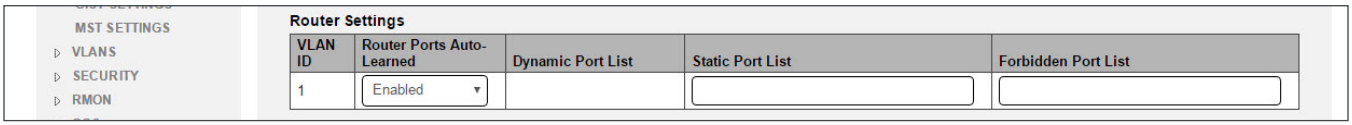


- **VLAN ID –** VLAN identifier.
- **Group IP Address –** IP address for the multicast.
- **Member Ports –** Switch ports that are part of the group.

Router Settings

Configure IGMP router ports on the switch.

Figure 43. IGMP Snooping Router Settings

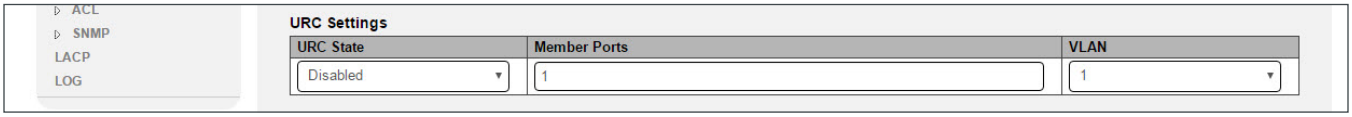


- **VLAN ID –** VLAN identifier.
- **Router Ports Auto-Learned –** Enable to allow auto learning of router port use.
  Default: Enabled
- **Dynamic Port List –** Lists auto-learned ports if Router Ports Auto-Learned is enabled.
- **Static Port List –** Manually select ports that are connected to the multicast querier.
- **Forbidden Port List –** Manually select ports to be excluded from joining multicast groups on that VLAN.

URC Settings

Use this menu to configure multicasting devices for URC brand control systems. This feature was developed by Araknis to ease setup for these systems.

Figure 44. IGMP Snooping URC Settings



- **Group –** Enable or disable URC settings.
- **Member Ports –** Select which ports on the switch should connect to the URC multicast.
- **VLAN –** Select the VLAN the URC devices are on.

© 2016 Araknis Networks®

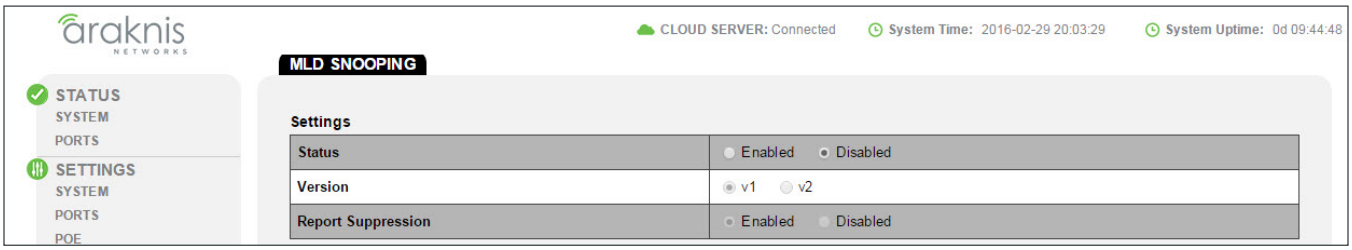
23 - Multicast – MLD Snooping

Configure settings for Multicast Listener Discovery. MLD is used by IPv6 multicast routers to detect multicast listeners.

Settings

Configure global settings for MLD Snooping.

Figure 45. MLD Snooping Menu

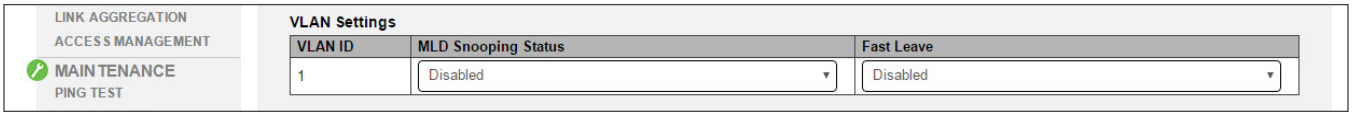


- **Status –** Enable or disable IGMP Snooping. When enabled, the switch monitors network traffic passing through it to determine which connected clients want to receive multicast traffic.
  Default: Disabled
- **Version –** Select MLDv1 or v2.
- **Report Repression –** Enable to prevent the router from seeing the IGMP messaging that occurs at the client level. This alleviates load on the router, because the switch acts as a proxy for client level messages (like leave requests).
  Default: Enabled

VLAN Settings

Configure MLD Snooping settings for individual VLANs.

Figure 46. MLD Snooping VLAN Settings

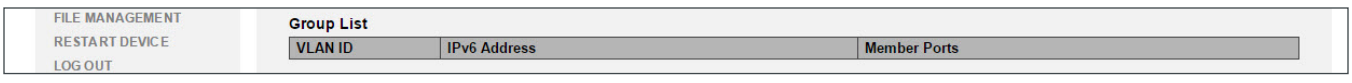


- **VLAN ID –** VLAN identifier.
- **IGMP Snooping Status –** Enable or disable MLD Snooping for the VLAN.
- **Fast Leave –** Enable to allow subscribed multicast clients to leave without a response message.

Group List

See current group subscriptions by VLAN.

Figure 47. MLD Snooping Group List



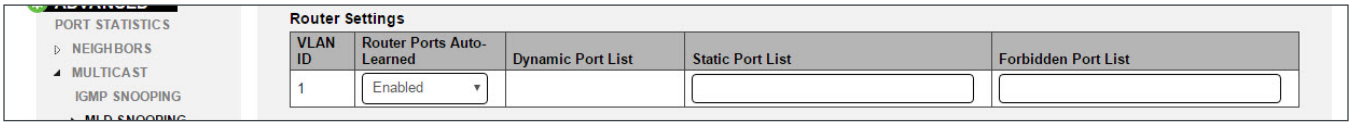
- **VLAN ID –** VLAN identifier.
- **IPv6 Address –** IP address for the multicast.
- **Member Ports –** Switch ports that are part of the group.

© 2016 Araknis Networks®

Router Settings

Configure MLD router ports on the switch.

Figure 48. MLD Snooping Router Settings



- **VLAN ID –** VLAN identifier.
- **Router Ports Auto-Learned –** Enable to allow auto learning of router port use.
  Default: Enabled
- **Dynamic Port List –** Lists auto-learned ports if Router Ports Auto-Learned is enabled.
- **Static Port List –** Manually select ports that are connected to the multicast querier.
- **Forbidden Port List –** Manually select ports to be excluded from joining multicast groups on that VLAN.

© 2016 Araknis Networks®

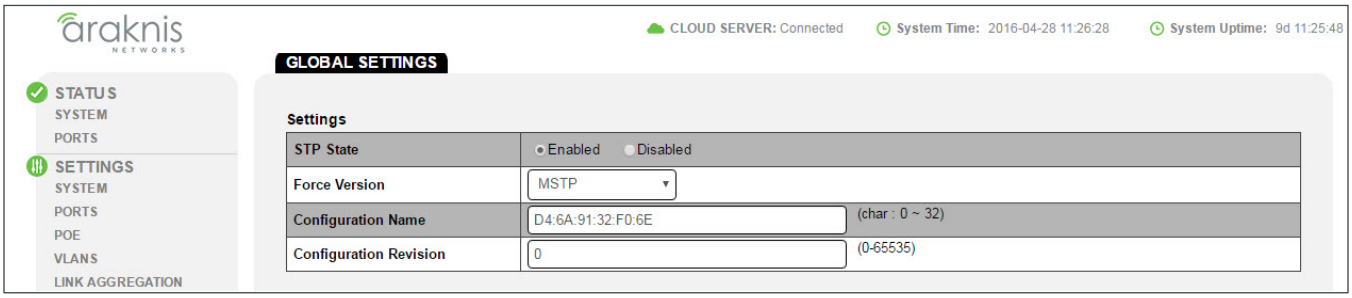
24 - STP – Overview

The Spanning Tree Protocol (STP) is a Layer 2 protocol primarily used to detect and eliminate network loops on redundant connections. Proper STP configuration ensures that only one route exists between any two end devices, with backup routes automatically taking over if a primary route goes down.

STP – Global Settings

Use this page to enable STP, select which protocol is used, and configure settings for the switch used to elect the root bridge device.

Figure 49. Global STP Settings Menu



Settings

- **STP State –** Select whether Spanning Tree Protocol is Enabled or Disabled.
- **Force Version –** Select the spanning tree protocol to enforce:
  - **STP –** Spanning Tree Protocol (IEEE 802.1D). Uses a distributed algorithm to select a switch to serve as the root of the spanning tree network. It selects a root port on each switch (except for the root device), which has the lowest path cost forwarding a packet to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost path, STP enables all root ports and designated ports, and disables all other ports to prevent loops. Network packets are then only forwarded between root ports and designated ports.

    Once the network is stable, all switches listen for Hello BPDUs (Bridge Protocol Data Units) sent by the Root Bridge. If a switch does not get a Hello BPDU after a certain period (Maximum Age), the switch assumes that the link to the Root Bridge is down. Then, the switch initiates negotiations with other switches in the network to recalculate the Spanning Tree Algorithm, determine the new root bridge device, and make the network stable again.

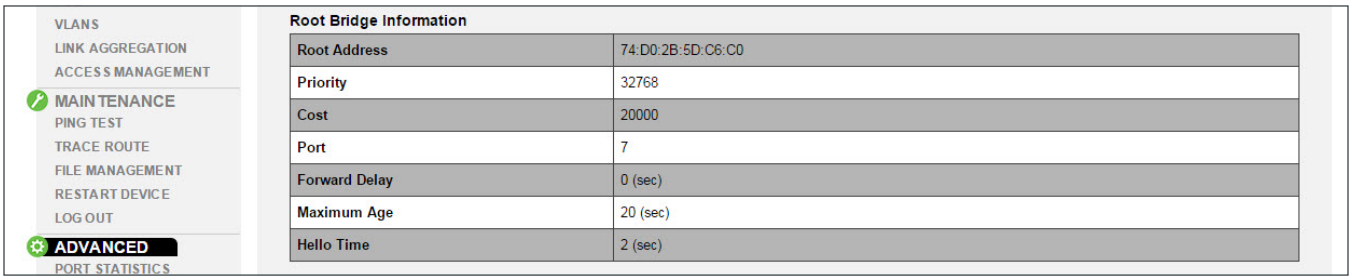
  - **RSTP –** Rapid Spanning Tree Protocol (IEEE 802.1w). Enhancement to legacy STP. RSTP is also included in MSTP. RSTP performs faster reconfiguration when topology change is detected (1 to 3 seconds for RSTP, compared to 30 seconds or more for STP). RSTP only supports one spanning tree instance on any link in a network. We recommend using RSTP over STP as long as the network equipment supports it.
  - **MSTP –** Multiple Spanning Tree Protocol (IEEE 802.1s). Designed to maintain multiple spanning trees instances based on VLANs in the network. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). Use this mode when there multiple spanning tree regions with their own regional root bridge devices.
- **Configuration Name –** (MSTP mode only) Name the MSTP configuration.
  Default: MAC address of the switch
- **Configuration Revision –** (MSTP mode only) Set a configuration revision for MSTP. The revision number must be the same for switches in the same region. Use a different revision for each region.

© 2016 Araknis Networks®

Root Bridge Information

Displays the STP parameters of the current elected root bridge device for the entire spanning tree.

Figure 50. Global STP Root Bridge Information



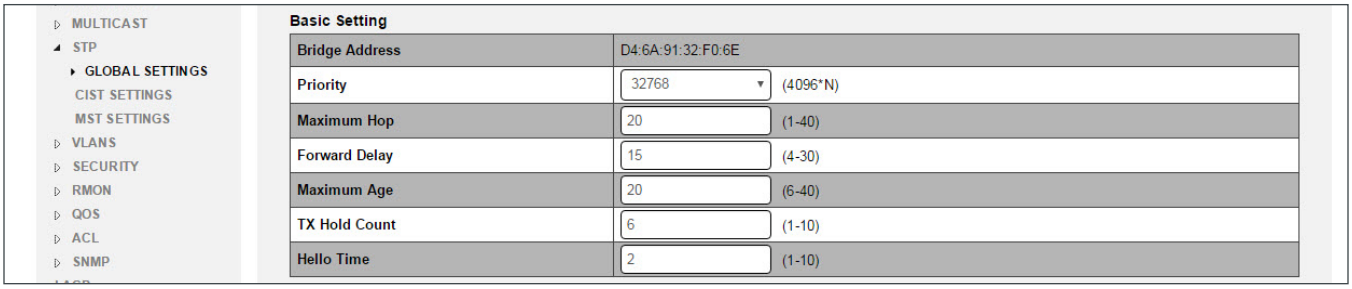
- **Root Address –** MAC address of the root bridge.
- **Priority –** Displays the value used to prioritize what switch is elected as the root bridge device. Smaller values indicate higher priority; larger values, lower priority. If all switches are left to default priority, the bridge device with the lowest numbered MAC address will be elected.
- **Cost –** Displays shortest path to the root bridge device.
- **Port –** Switch port linking to the root bridge device.
- **Forward Delay –** Amount of seconds before the root bridge port builds its bridge table after the Max Age limit has passed.
- **Maximum Age –** Amount of seconds after receiving a BPDU before the root bridge port returns to the listening state.
- **Hello Time –** Amount of seconds between BPDUs sent by the root bridge.

© 2016 Araknis Networks®

Basic Setting

Configure root bridge settings for the switch. This information will be used to decide if the switch should be the root bridge device.

Figure 51. Global STP Basic Settings



- **Bridge Address –** MAC address of the switch.
- **Priority –** Select the value used to prioritize whether the switch is elected as the root bridge. Smaller values indicate higher priority; larger values, lower priority. If all switches are left to default priority, the bridge device with the lowest numbered MAC address will be elected. If you want a particular switch to be guaranteed as the root bridge device, set its Priority value lower than other switches. Range: 0-61440 (multiples of 4096)
  Default: 32768
- **Maximum Hop –** Maximum number of link hops a BPDU will travel from the root bridge, as long as the maximum age of the BPDU has not passed. Range: 1-40
  Default: 20
- **Forward Delay –** Amount of seconds before the root bridge port rebuilds its bridge table after the Max Age limit has passed. Range: 4-30 seconds
  Default: 15 seconds
- **Maximum Age –** Amount of seconds after receiving a BPDU before the root bridge port returns to the listening state. Range: 6-40 seconds
  Default: 20 seconds
- **TX Hold Count –** Limit for the number of BPDUs can be sent during a Hello Time period. Range: 1-10
  Default: 6
- **Hello Time –** Amount of seconds between BPDUs sent by the root bridge. Range: 1-10 seconds
  Default: 2 seconds

© 2016 Araknis Networks®

25 - STP (Spanning Tree Protocol) Overview

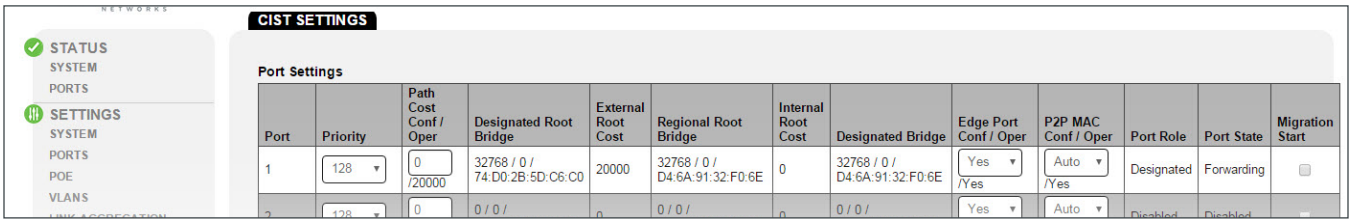
Spanning Tree Protocol is used to prevent loops in networks where packets might have multiple possible routes. Backup routes between equipment can also be maintained and used only when the primary fails. The switch supports IEEE 802.1d STP, 802.1s RSTP (Rapid Spanning Tree Protocol), and 802.1w MSTP (Multiple Spanning Tree Protocol).

STP – CIST Settings

Use this menu to view and customize port-based Common and Internal Spanning Tree (CIST) settings.

Port Settings

Figure 52. STP CIST Port Settings Menu



- **Port –** Switch port identifier.
- **Priority –** Set CIST priority for each port on the switch. Smaller values indicate higher priority; larger values, lower priority. If all ports have the same path cost, this value will be used to determine the best path to the root bridge. Range: 0-240 (multiples of 16)
  Default: 128
- **Path Cost Conf / Oper –** (Configured/Operating) Enter a value larger than zero to modify the path cost. The currently calculated (Oper) path cost is displayed below. If the entered value is zero, the Oper path cost is based on the port speed, which in this case is 1 Gbps.
- **Designated Root Bridge –** Displays the designated root bridge device's priority, forward delay, and MAC address.
- **External Root Cost –** Displays the cost to reach the root bridge across links connecting the boundary ports outside the MSTP region. When a BPDU is received on an internal port, this cost is not changed. When a BPDU is received on a boundary port, this cost is adjusted based on the receiving boundary port cost.
- **Regional Root Bridge –** Displays the regional root bridge device's priority, forward delay, and MAC address.
- **Internal Root Cost –** Displays the cost to reach the regional root bridge inside the MSTP region. When a BPDU is received on an internal port, this cost is adjusted based on the receiving boundary port cost. This information is not shared or counted outside the region.
- **Designated Bridge –** Displays the designated bridge device's priority, forward delay, and MAC address.
- **Edge Port Conf / Oper –** (Configured/Operating) Configure a switch port as an edge port for a region and see the current edge status of the port.

Continues on the next page

© 2016 Araknis Networks®

STP CIST Settings, Continued

- **P2P MAC Conf / Oper –** (Configured/Operating) Options:
  - **Auto (default) –** Allow P2P ports into full duplex mode.
  - **Yes –** Force P2P ports into full duplex mode.
  - **No –** No P2P status.
- **Port Role –** Displays what role the port is currently playing. Options:
  - **Disabled –** Port is not in use.
  - **Root –** The port with the lowest cost that links the switch to the root bridge device.
  - **Non-Designated –** (STP only) Port is blocking and not listening.
  - **Alternate –** (RSTP) Port links between bridges but is not the designated port, so it is not used unless the designated port loses connection.
  - **Designated –** Port is designated as the elected link between bridges in the spanning tree.
- **Port State –** Displays what state the port is currently in. Options:
  - **Disabled –** Port is not in use.
  - **Blocking –** Port is not forwarding frames or reading MAC addresses because it would cause a loop, but is listening for BPDUs. This state is reached once a different port is designated.
  - **Listening –** A designated or root port moves into this state if it stops blocking due to a change in the spanning tree. BPDUs are received from the connected segment and analyzed to determine the ideal topology. No other frames are forwarded while a port is in this state.
  - **Learning –** Once the listening process is complete, the port begins updated the MAC address table and gets ready to start forwarding frames as normal.
  - **Forwarding –** The port is an active link in the spanning tree forwarding frames as normal.
- **Migration Start –** (RSTP Mode only) Click the box and click Apply to force the port to use the newest configuration.

© 2016 Araknis Networks®

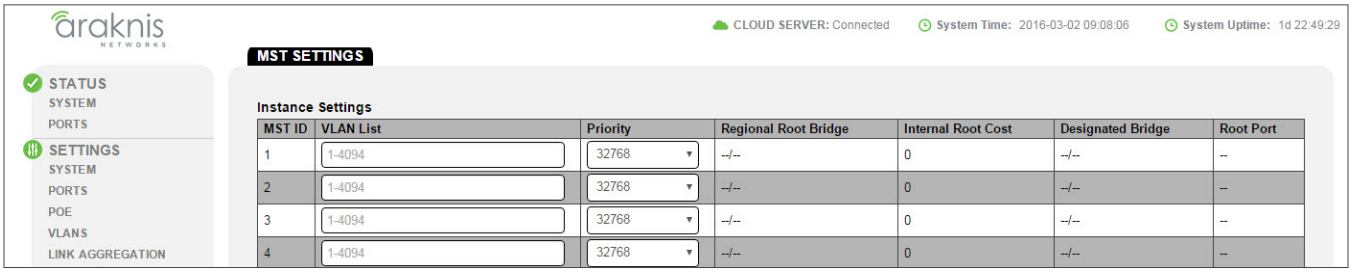
STP – MST Settings

Multiple Spanning Tree Protocol (MSTP) is used to map multiple VLANs to one spanning tree topology. Since there are rarely as many unique topologies as there are VLANs in a network, using MST saves switch CPU power by reducing the number of spanning tree instances required to handle all VLANs on the device. Each MST instance acts as its own RSTP node within the network's CIST.

Instance Settings

Select which VLANs will be included in each MSTI.

Figure 53. STP MST Instance Settings Menu



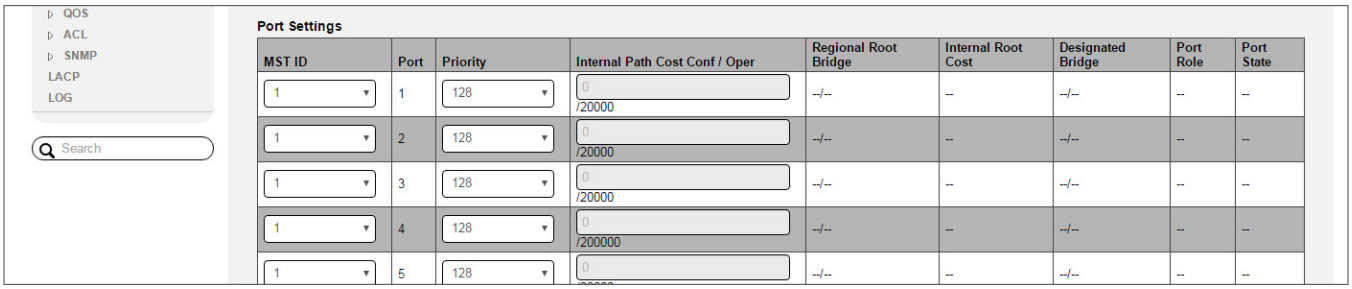
- **MST ID –** MST instance identifier.
- **VLAN List –** Enter the VLAN IDs to be associated with the topology. Enter individual or ranges of values, for example: "20, 30-32" entered would associate VLANs 20, 30, 31, and 32.
- **Priority –** Value used to prioritize what MST ID is elected as the path back to the root bridge device. If all switches are left to default priority, the root bridge with the lowest numbered MAC address will be elected. Smaller values indicate higher priority; larger values, lower priority. Range: 0-61440 (multiples of 4096)
  Default: 32768
- **Regional Root Bridge –** Displays the MAC address and priority for the regional root bridge.
- **Internal Root Cost –** Displays the cost to reach the regional root bridge inside the MSTP region. When a BPDU is received on an internal port, this cost is adjusted based on the receiving boundary port cost. This information is not shared or counted outside the region.
- **Designated Bridge –** Displays the MAC address and priority for the current designated bridge.
- **Root Port –** Switch port connecting the switch to that MST's root bridge device.

© 2016 Araknis Networks®

Port Settings

Configure MSTP settings for each port.

Figure 54. STP MST Port Settings Menu



- **MST ID –** Select the MST ID to configure.
- **Port –** Switch port being configured.
- **Priority –** Value used to prioritize the port. If all ports are left to default priority, then priority is elected based on link speed of the port. Smaller values indicate higher priority; larger values, lower priority. Range: 0-240 (multiples of 16)
  Default: 128
- **Internal Path Cost Conf / Oper –** (Configured/Operating) Set the configured internal path cost and see the current operational internal path cost.
- **Regional Root Bridge –** Displays the MAC address and priority for the regional root bridge.
- **Internal Root Cost –** Displays the cost to reach the regional root bridge inside the MSTP region. When a BPDU is received on an internal port, this cost is adjusted based on the receiving boundary port cost. This information is not shared or counted outside the region.
- **Designated Bridge –** Displays the MAC address and priority for the designated bridge.
- **Port Role –** Displays what role the port is currently playing. Options:
  - **Root –** The port links the switch to the root bridge device.
  - **Designated –** Ports in use within the MSTP region.
  - **Disabled –** Port is not in use.
- **Port State –** Displays what state the port is currently in. Options:
  - **Root –** The port links the switch to the root bridge device.
  - **Disabled –** Port is not in use.

© 2016 Araknis Networks®

26 - Advanced VLANs – Overview

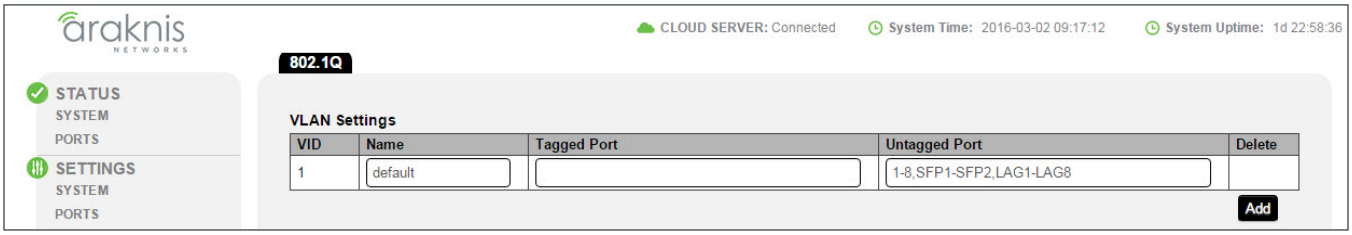
The advanced VLAN pages contain settings for customizing VLANs beyond basic port-based settings.

Advanced VLANs – 802.1Q VLANs

VLAN Settings

Manually configure VLAN tagging for each port.

Figure 55. 802.1Q VLAN Settings Menu

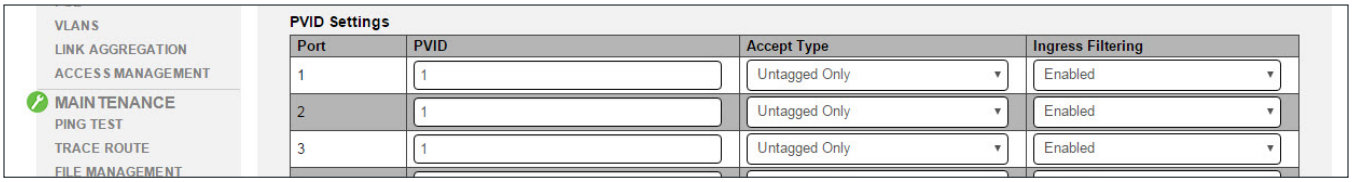


- **VID –** VLAN ID.
- **Name –** Use this field to enter a custom VLAN name for easy identification.
- **Tagged Port –** Tagged ports and LAGs for the VLAN. Click the field to configure.
- **Untagged Port –** Untagged ports and LAGs for the VLAN. Click the field to configure.
  Default: All ports untagged
- **Delete –** Click the trash can icon then click **Apply** to delete a VLAN entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

PVID Settings

Use Port VLAN ID to configure tagging on packets coming to a port.

Figure 56. 802.1Q PVID Settings Menu



- **Port –** Switch port identifier.
- **PVID –** Enter the VLAN ID(s) to be associated with the port.
- **Accept Type –** Select which packets are tagged with the PVID. Options:
  - **Untagged Only –** Only untagged packets are tagged.
  - **Tagged Only –** Only tagged packets are stripped and retagged.
  - **ALL –** All packets are tagged/stripped and retagged.
- **Ingress Filtering –** Enable or disable.

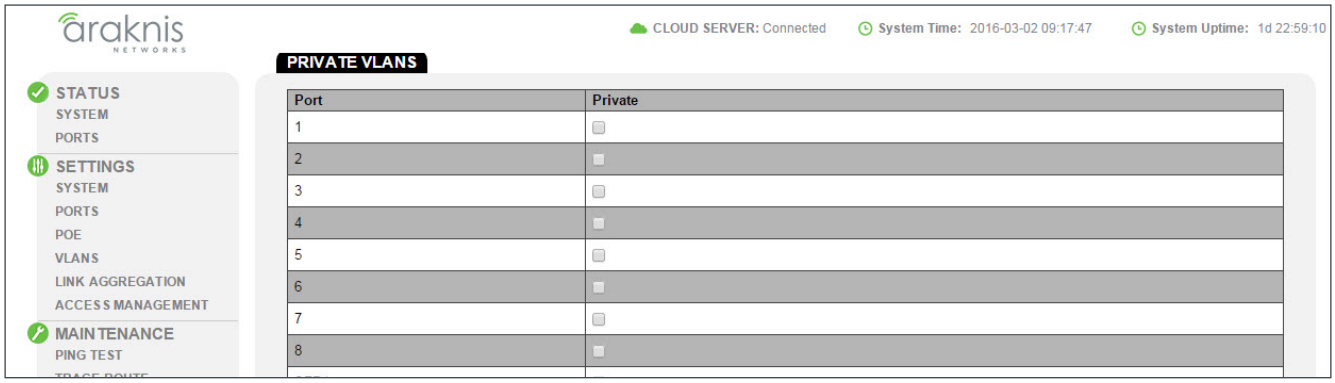
© 2016 Araknis Networks®

Advanced VLANs – Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Traffic on ports assigned to a private VLAN can only be forwarded to and from uplink ports.

> **Note –** The Private VLANs feature is only found in 310 series switches.

Figure 57. Private VLANs Menu



- **Port –** Switch port identifier.
- **Private –** Check the box to set a port to private status.
  Default: Not checked

© 2016 Araknis Networks®

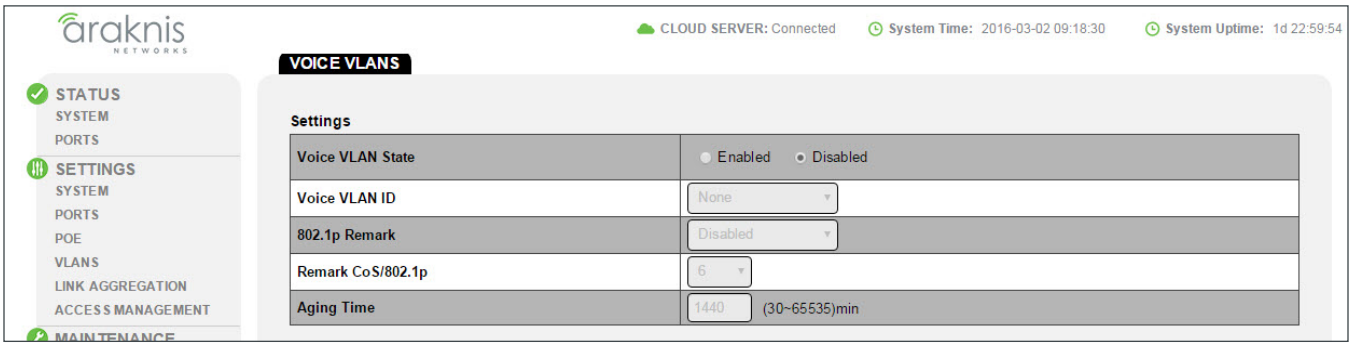
Advanced VLANs – Voice VLANs

Cofigure VLANs for VOIP phone systems with built-in VLAN tagging abilities. The interface includes presets for quickly configuring many popular brands. The switch will examine tagged packets from phones and place them in the correct VLAN automatically. QoS prioritization can also be applied to help ensure audio quality on VoIP calls.

General Settings

> **Note –** In order to configure a new voice VLAN, you must first create a new VLAN. The default VLAN cannot be used. See:
>
> - Section “14 - VLAN Settings (Basic Port-Based)” on page 31, or
> - Section “Advanced VLANs – 802.1Q VLANs” on page 61

Figure 58. Voice VLANs Settings



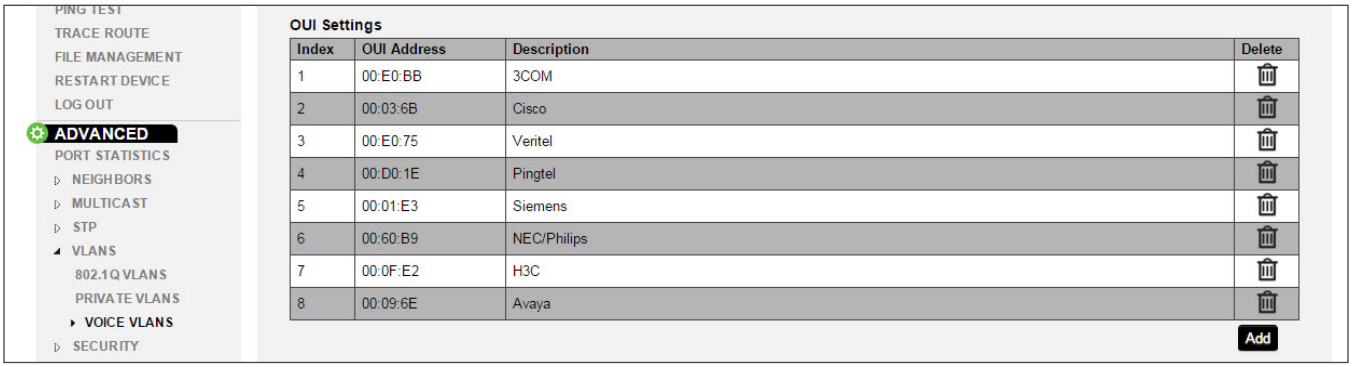
- **Voice VLAN State –** Click to enable or disable the Voice VLAN feature.
  Default: Disabled
- **Voice VLAN ID –** Select an existing VLAN ID for use as a Voice VLAN.
- **802.1p Remark –** Enable or disable 802.1p Remarks in packets to prioritize voice packets.
  Default: Disabled
- **Remark CoS/802.1p –** Select what priority level to give voice packets if remarking is enabled. Higher values receive higher priority. Range: 0-7
  Default: 6
- **Aging Time –** Range: 30~65535 minutes
  Default: 1440 minutes

© 2016 Araknis Networks®

OUI Settings

The Organizationally Unique Identifier (OUI) is the first half of a device MAC address, and is unique for every phone manufacturer. The OUI is used to automatically detect packets from the phone and send them to the Voice VLAN. The included values are very popular, and new values may be added.

Figure 59. Voice VLANS OUI Settings

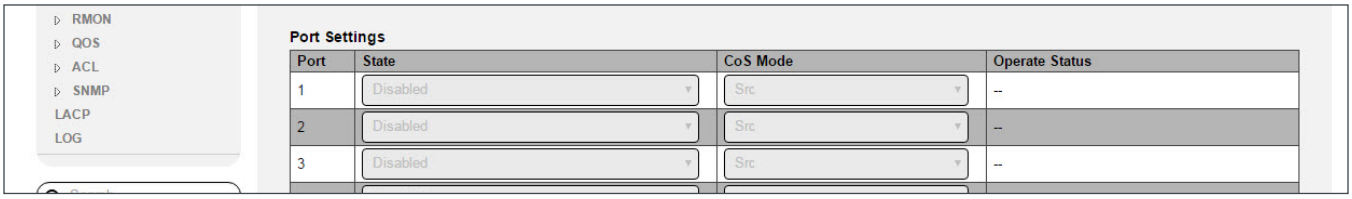


- **Index –** Identifier for the OUI.
- **OUI Address –** Portion of the MAC address used to identify different brands of IP phones.
- **Description –** Phone system name.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

Port Settings

Configure port-based Voice VLAN settings.

Figure 60. Voice VLANS Port Settings



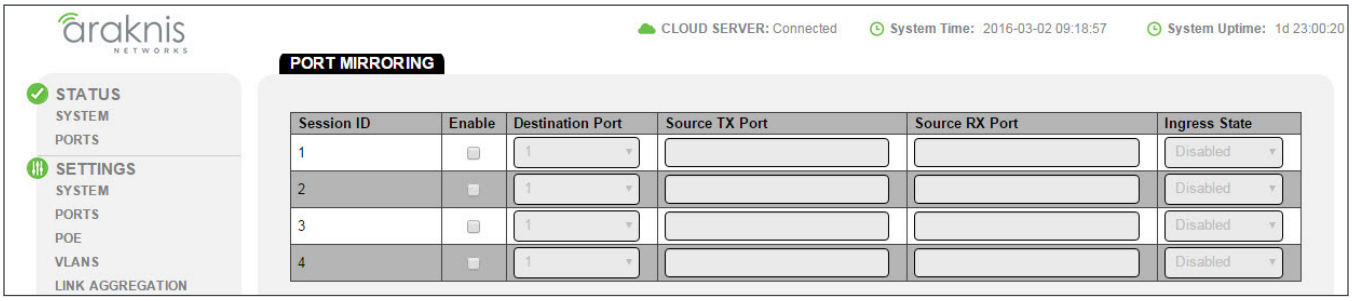
- **Port –** Switch port identifier.
- **State –** Enable or disable Voice VLAN tag examination on the port.
- **CoS Mode –** Select the Class of Service (CoS) mode. Options:
  - **Src –** Only packets from the source MAC address are given QoS prioritization on the Voice VLAN.
  - **All –** All packets on the Voice VLAN are given QoS prioritization.
- **Operate Status –** Displays the current operating status of the Voice VLAN feature on the port.

© 2016 Araknis Networks®

27 - Security – Port Mirroring

Port mirroring is used to send a copy of packets received on one switch port to a network monitoring device/software on another switch port. This is commonly used for network appliances that require monitoring of network traffic. Network engineers or administrators use port mirroring to analyze and diagnose errors on a network.

Figure 61. Port Mirroring Page



- **Session ID –** Session identifier.
- **Enable –** Check to enable a port mirroring session.
- **Destination Port –** Port that packets will be mirrored to.
- **Source TX Port –** Port that sent the original packets.
- **Source RX Port –** Port originally receiving the packets.
- **Ingress State –** Enable or disable.

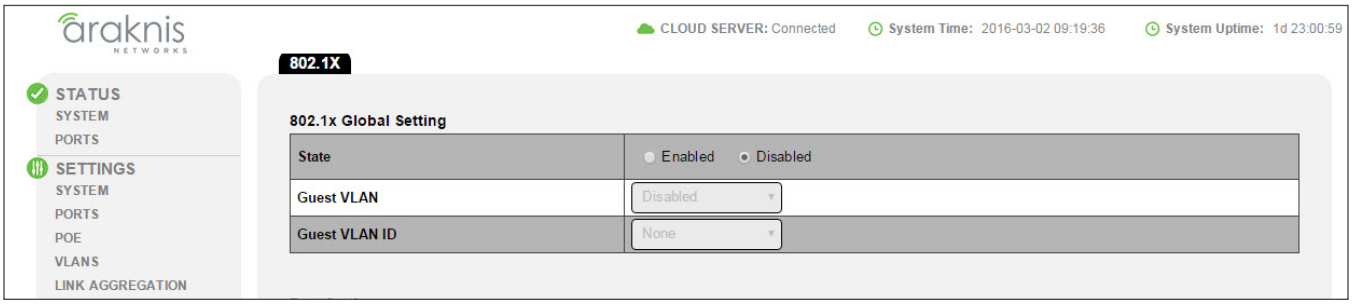
28 - Security – 802.1x

802.1x allows port-based client authentication with the use of a RADIUS server.

802.1x Global Setting

Configure global 802.1x settings.

Figure 62. 802.1x Global Settings Menu



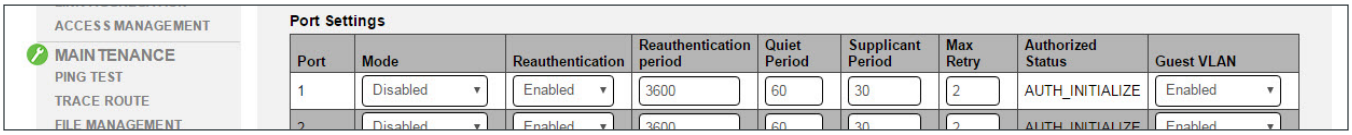
- **State –** Enable or disable the 802.1x feature.
- **Guest VLAN –** Enable or disable guest VLAN use for 802.1x. If enabled, all authorized clients will be connected to the VLAN.
- **GUEST VLAN ID –** Select a VLAN ID for use if Guest VLAN is Enabled.

© 2016 Araknis Networks®

Port Settings

Configure 802.1x settings for each switch port.

Figure 63. 802.1x Port Settings Menu



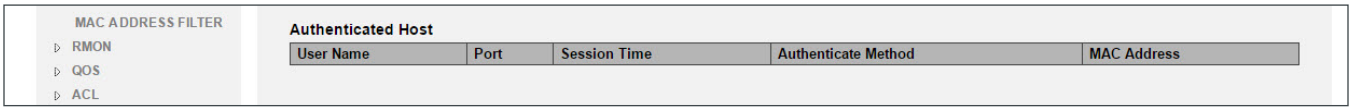
- **Port –** Switch port identifier.
- **Mode –** Options:
  - **Disabled –** 802.1x is disabled through the port.
  - **Auto –** Port allows only packets used for authentication and network discovery until the client is authenticated, then allows uninterrupted traffic.
  - **ForceUnAuthorized –** The port will remain unauthorized state and ignore all attempts to authenticate a client.
  - **ForceAuthorized –** The port always behaves as if an authenticated client is connected.
- **Reauthentication –** Enable or disable reauthentication by the switch. If enabled, a client that failed to authenticate will not be allowed to try again until the next period based on the Period Setting.
  Default: Enabled
- **Reauthentication period –** Set the reauthentication period.
  Default: 3600 seconds
- **Quiet Period –** Set the quiet period.
  Default: 60
- **Supplicant Period –** Set the Supplicant period.
  Default: 30
- **Max Retry –** Set the Max Retry value.
  Default: 2
- **Authorized Status –** Displays the current authorization status of the port.
- **Guest VLAN –** Enable or disable guest VLAN use for the port.
  Default: Enabled
  Default:

© 2016 Araknis Networks®

Authenticated Host

See currently connected authenticated hosts connected using 802.1x.

Figure 64. 802.1x Authenticated Host Table



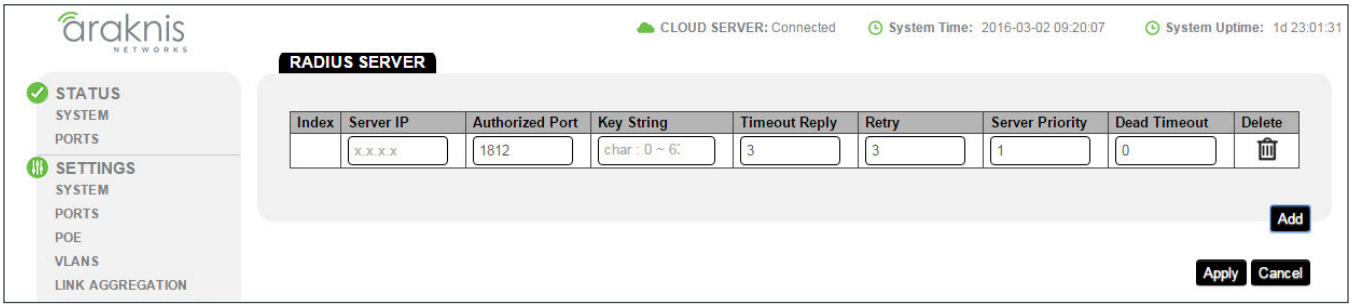
- **User Name –** Name of the user configured in the RADIUS server.
- **Port –** Switch port the user is authenticated on.
- **Session Time –** Amount of time since the user was authenticated for the current session.
- **Authenticate Method –** Method used to authenticate the user.
- **MAC Address –** MAC address of the connected client port.

© 2016 Araknis Networks®

29 - Security – Radius Server

The Remote Authentication Dial-In User Service (RADIUS) protocol provides central management for users connecting to use network services. Use this menu to configure settings for the server.

Figure 65. Radius Server Menu



- **Index –** RADIUS Server entry identifier.
- **Server IP –** IP address of the RADIUS server.
- **Authorized Port –** Port for clients communicating with the server.
- **Key String –** Enter the authentication key used between the switch and the server.
- **Timeout Reply –** How many seconds to wait for a reply from the server before trying again.
  Default: 3 seconds.
- **Retry –** Number of times to attempt connection to the server.
  Default: 3
- **Server Priority –** Enter the RADIUS server the priority for the switch. The server with the highest priority will be queried first. Lower values give higher priority.
  Default: 1
- **Dead Timeout –** Amount of time before the switch stops attempting to connect.
  Default: 0
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.

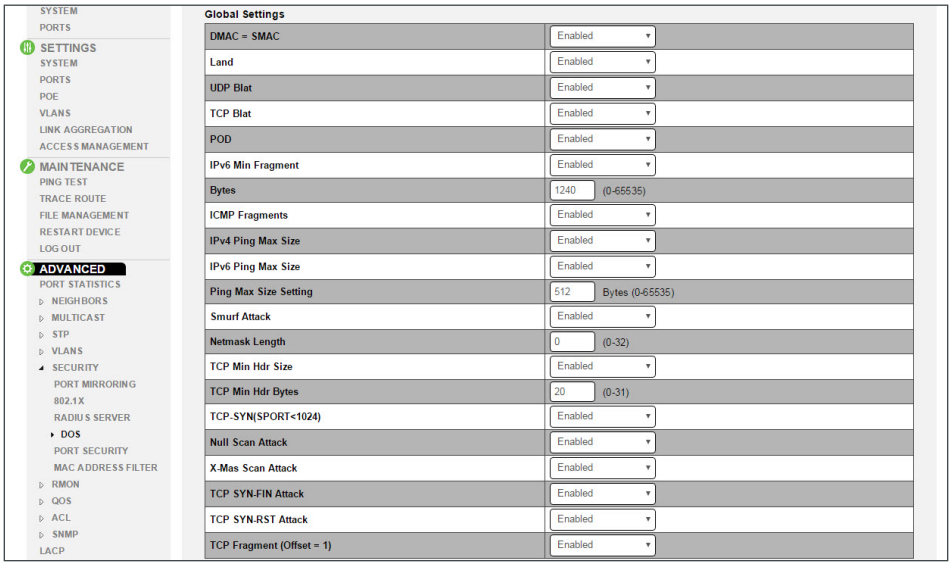
© 2016 Araknis Networks®

30 - Security – DOS

Use Denial of Service (DOS) settings to protect from DoS attacks. The switch will block traffic that meets the configured conditions.

Global Settings

Figure 66. Global DOS Settings Menu



- **DMAC = SMAC –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **Land –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **UDP Blat –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **TCP Blat –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **POD –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **IPv6 Min Fragment –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **Bytes –** Specify the minimum IPv6 fragment size to filter. Range: 0-65535 Bytes
  Default: 1240 Bytes
- **ICMP Fragments –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **IPv4 Ping Max Size –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **IPv6 Ping Max Size –** Enable or Disable filtering of this type of attack.
  Default: Enabled

Continues on next page

© 2016 Araknis Networks®

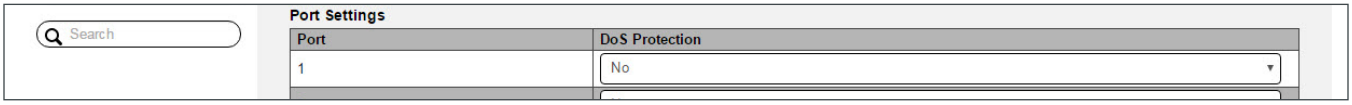
Global DOS Security Settings, Continued

- **Ping Max Size Setting –** Specify the maximum IPv6 fragment size to filter. Range: 0-65535 Bytes
  Default: 512 Bytes
- **Smurf Attack –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **Netmask Length –** Specify the netmask length to filter. Range: 0-32
- **TCP Min Hdr Size –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **TCP Min Hdr Bytes –** Specify the minimum number of TCP Min Hdr Bytes to filter. Range: 0-31 Bytes
  Default: 20 Bytes
- **TCP-SYN(SPORT<1024) –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **Null Scan Attack –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **X-Mas Scan Attack –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **TCP SYN-FIN Attack –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **TCP SYN-RST Attack –** Enable or Disable filtering of this type of attack.
  Default: Enabled
- **TCP Fragment (Offset = 1) –** Enable or Disable filtering of this type of attack.
  Default: Enabled

Port Settings

Configure port-based DOS security settings.

Figure 67. DOS Port Settings Table



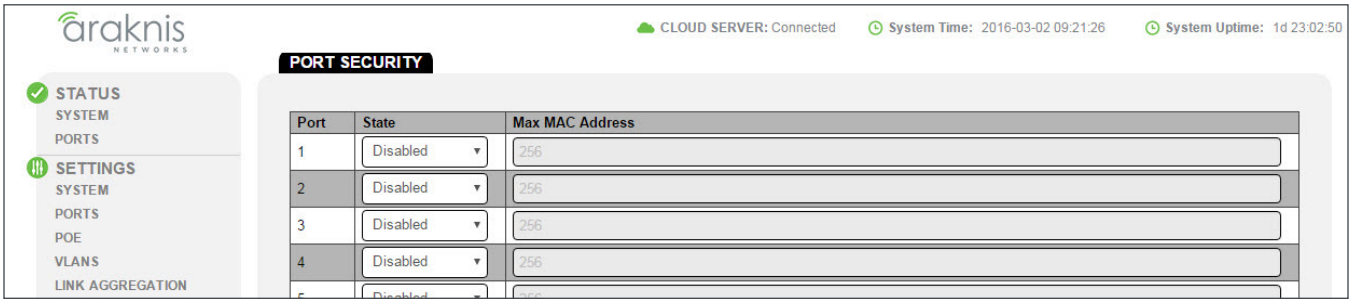
- **Port –** Switch port identifier.
- **DoS Protection –** Select Yes to enable DoS protection for the port, or No disable protection for the port. If enabled, the switch will block any types of traffic that filtering is enabled for in the DOS Global Settings menu.

© 2016 Araknis Networks®

31 - Security – Port Security

Limit the number of connected devices on a given port by limiting the total number of MAC addresses that may be identified on that port.

Figure 68. Port Security Table

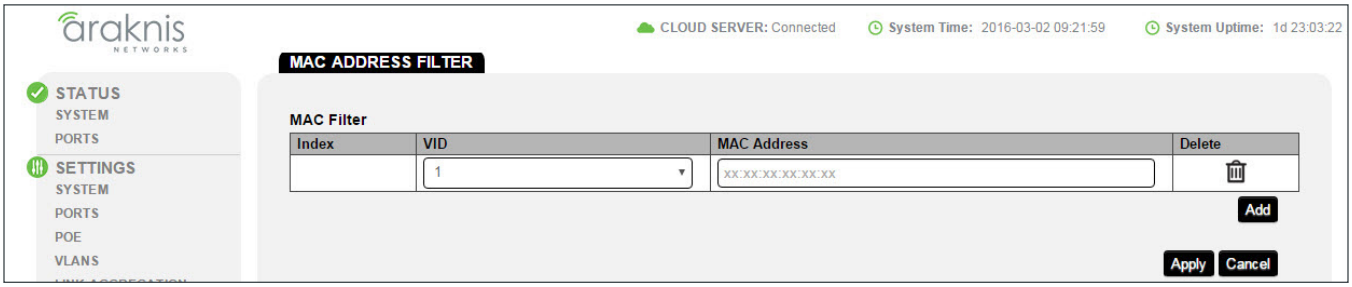


- **Port –** Switch port identifier.
- **State –** Enable or disable security for the port.
- **Max MAC Address –** Enter the total number of MAC addresses that may be identified on the port.

32 - Security – MAC Address Filter

Bind MAC addresses to VLANs regardless of which port they are connected on.

Figure 69. MAC Address Filter Table



- **Index –** MAC Filter rule identifier.
- **VID –** Select the VLAN ID for the MAC address to be bound to.
- **MAC Address –** Enter the MAC address to be filtered.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.

© 2016 Araknis Networks®

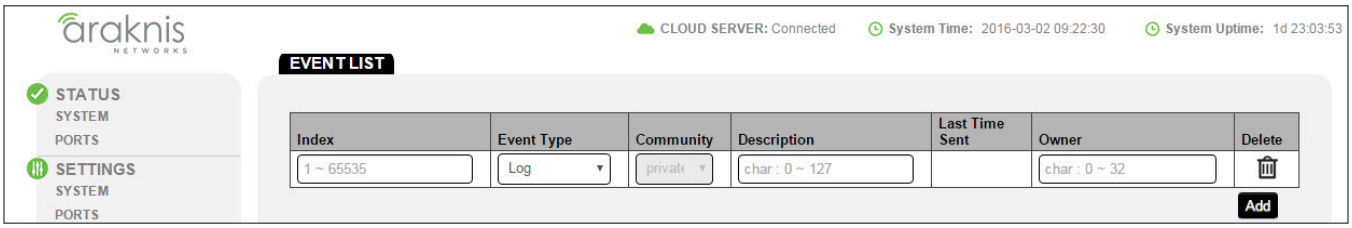
33 - RMON Overview

Remote Network Monitoring (RMON) allows the switch to monitor network traffic and send alarms if specified limits are reached or passed. Configure what events to monitor and how to react. Events may be logged and/or sent to other network clients using SNMP.

RMON – Event List

Define event types to execute when RMON alarms are triggered.

Figure 70. Event List

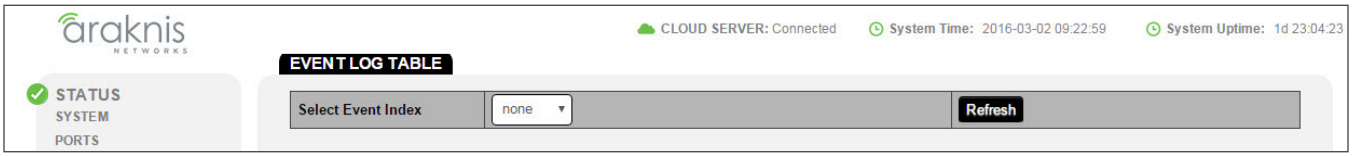


- **Index –** Enter a value to identify the event entry. Range: 1-65535
- **Event Type –** Select the desired action from the drop down:
  - **Log –** Add an entry to the event log when the alarm goes off.
  - **SNMP Trap –** Send a message to the remote log server when the alarm goes off.
  - **Log and Trap –** Log and send a message (above) when the alarm goes off.
- **Community –** If using **SNMP Trap** or **Log and Trap** event type, select whether the SNMP community is Public or Private.
- **Description –** Enter a description for the event type.
- **Last Time Sent –** Last occurrence of an event of the specified type being sent.
- **Owner –** Enter a name for the owner of the event.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.

RMON – Event Log Table

View RMON event logs.

Figure 71. Event Log Table



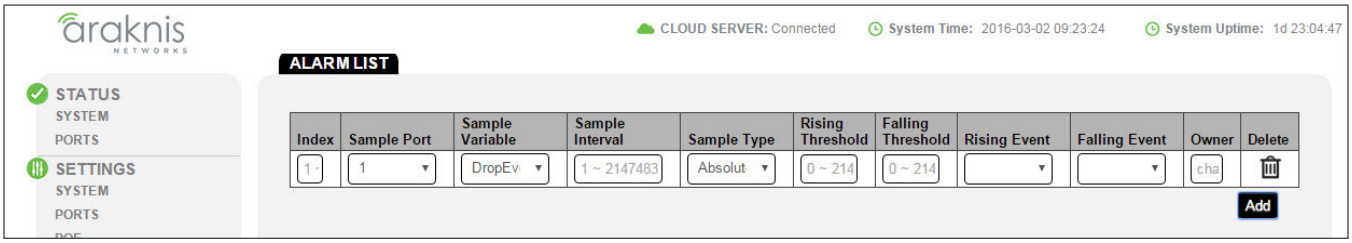
- **Select Event Index –** Select an Event identifier from the drop down. There must be configured entries in the RMON Event List to use the drop down.
- **Refresh –** Click to refresh the list and see the newest events.

© 2016 Araknis Networks

RMON – Alarm List

Configure alarms for RMON events.

Figure 72. Alarm List



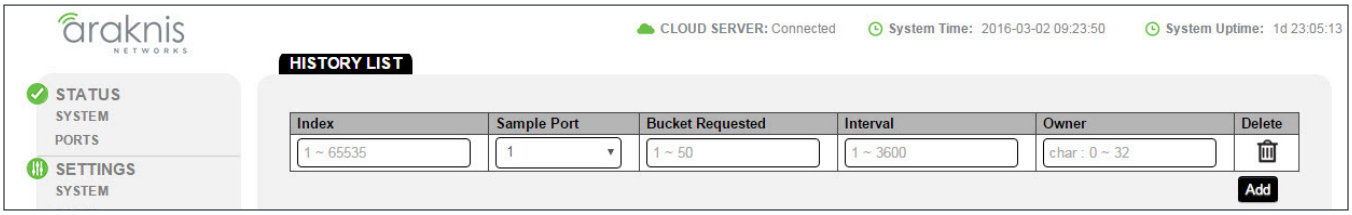
- **Index –** Enter an identifier for the Alarm List entry.
- **Sample Port –** Select the port to monitor from the drop down.
- **Sample Variable –** Select the event type to monitor for. Options: DropEvents, Octets, Pkts, BroadcastPkts, MulticastPkts, CRCAlignErrors, UnderSizePkts, OverSizePkts, Fragments, Jabbers, Collisions, PktsOctets, Pkts65-127Octets, Pkts128to255Octets, Pkts256to511Octets, Pkts512to1023Octets, Pkts1024to1518Octets.
- **Sample Interval –** Enter the alarm interval time.
- **Sample Type –** Select the sampling method:
  - **Absolute –** Compares values of thresholds vs. captured at the end of each sample interval. Use this option if the monitored value can increase or decrease at any time.
  - **Delta –** Detects change over time by subtracting the most recent sampled value from the current Use the option if the monitored value always increases over time.
- **Rising Threshold –** Upper threshold of the monitored value. Use this in conjunction with Falling Threshold to be alerted when the monitored value leaves the desired operating range.
- **Falling Threshold –** Lower threshold of the monitored value. Use this in conjunction with Rising Threshold to be alerted when the monitored value leaves the desired operating range.
- **Rising Event –** Select an event to execute from the drop down when the monitored value exceeds the Rising Threshold.
- **Falling Event –** Select an event to execute from the drop down when the monitored value exceeds the Falling Threshold.
- **Owner –** Enter a name to identify when the switch sends an alarm.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.

© 2016 Araknis Networks®

RMON – History List

Configure the events to record to the RMON history log on each port.

Figure 73. History List

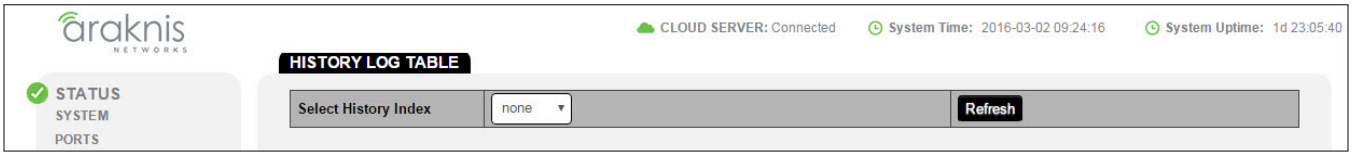


- **Index –** History Log identifier
- **Sample Port –** Select the port to monitor.
- **Bucket Requested –** Enter the number of samples to save in each entry.
- **Interval –** Enter the interval for recording samples on the port.
- **Owner –** Enter the name of the requester.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.

RMON – History Log Table

View selected history logs.

Figure 74. History Log Table



- **Select History Index –** Select a History Log type to monitor from the drop down. In order to view logs, you must first configure an entry in the RMON History List.
- **Refresh –** Click to refresh the log and see the newest results.

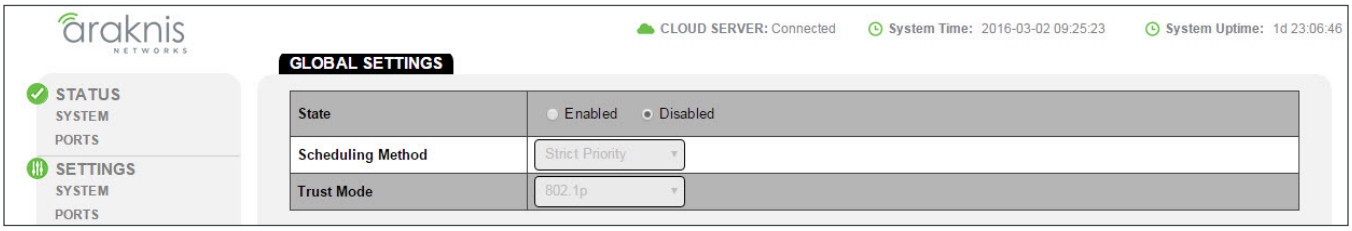
© 2016 Araknis Networks®

34 - QoS – Overview

Quality of Service (QoS) is used to organize and prioritize packet flow and bandwidth use on the LAN based on traffic type, source, or destination in order to help guarantee network performance for critical services.

QoS – Global Settings

Figure 75. Global Settings

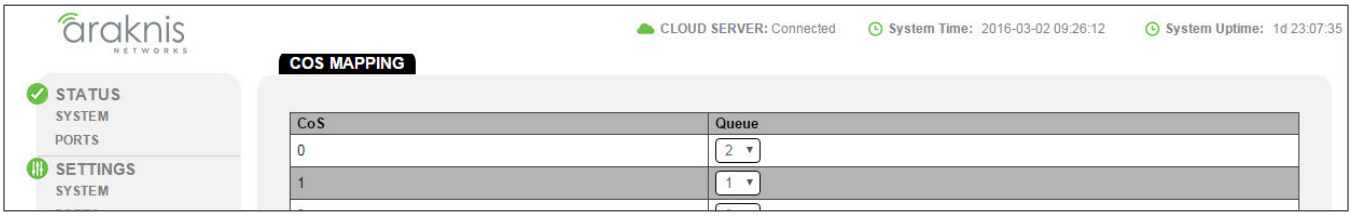


- **State –** Enabled or Disabled.
- **Scheduling Method –** Select the desired mode for scheduling traffic from the drop down:
  - **Strict Priority –** Traffic is scheduled specifically based on queue priority.
  - **WRR –** Use the Weighted Round Robin algorithm to prioritize traffic queues.
- **Trust Mode –** Select the desired mode of operation from the drop down:
  - **802.1p –** Traffic is prioritized based on its 802.1p priority tag.
  - **DSCP –** Traffic is prioritized based on its DSCP priority tag.
  - **802.1p + DSCP –** Traffic is prioritized based on both 802.1p and DSCP priority tags.

QoS – COS Mapping

Assign traffic of different CoS priority levels to the desired queue.

Figure 76. COS Mapping Table



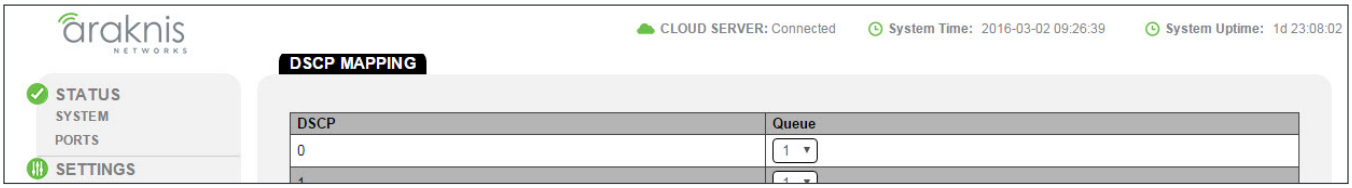
- **CoS –** CoS Priority level identifier.
- **Queue –** Select a queue from the drop down for the given priority level. The default values are standard for most applications.

© 2016 Araknis Networks®

QoS – DSCP Mapping

Assign traffic of different Differentiated Services Code Point (DSCP) priority levels to the desired queue.

Figure 77. DSCP Mapping Table

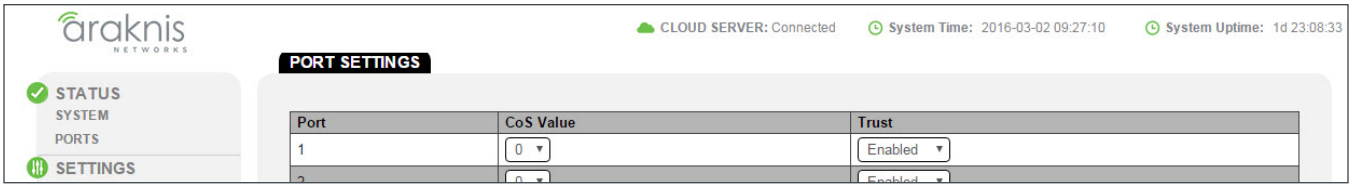


- **DSCP –** DSCP Priority level identifier
- **Queue –** Select a queue from the drop down for the given priority level. The default values are standard for most applications.

QoS – Port Settings

Assign all traffic from specified ports to be tagged with a certain CoS value.

Figure 78. QoS Port Settings Table

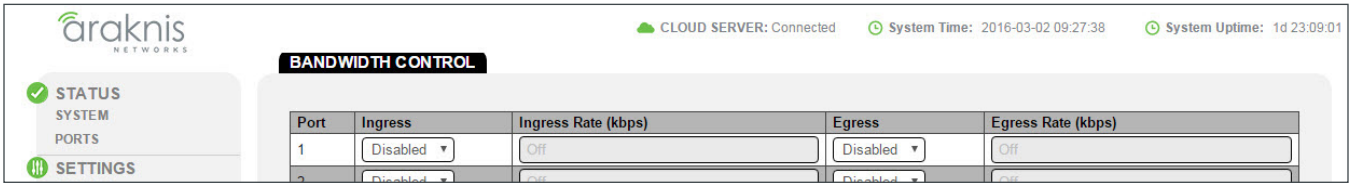


- **Port –** Switch Port identifier.
- **CoS Value –** Select a CoS value from the drop down for all packets on the specified port.
- **Trust –** Enable or disable.

QoS – Bandwidth Control

Limit the total amount of traffic allowed to come into or out of switch ports.

Figure 79. Bandwidth Control Table



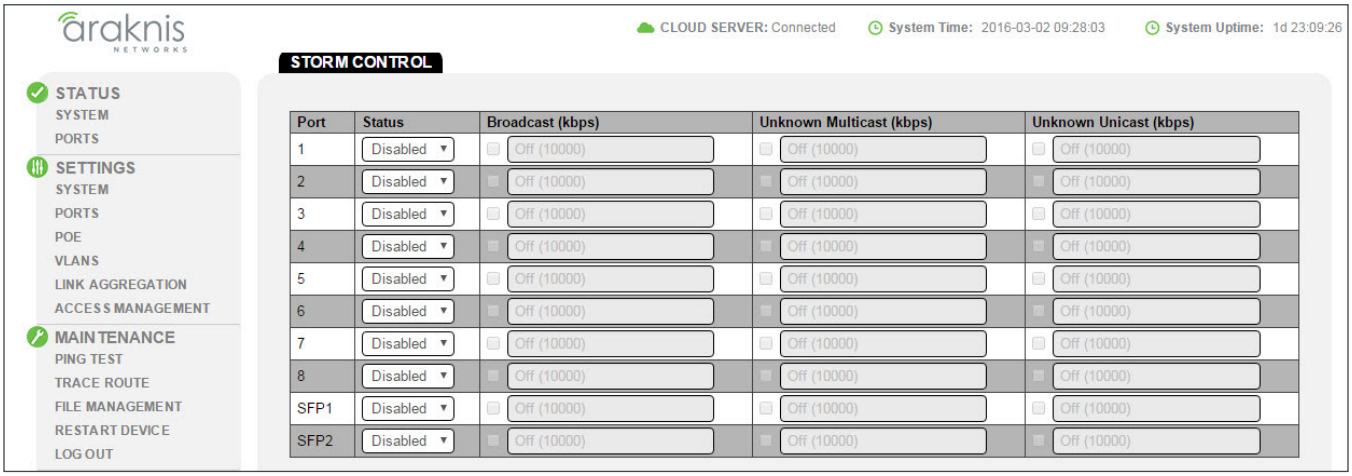
- **Port –** Switch Port identifier.
- **Ingress –** Enable or disable incoming bandwidth control for the port.
- **Ingress Rate (kbps) –** Enter the maximum data rate in kbps (multiples of 16) for incoming traffic on the port.
- **Egress –** Enable or disable outgoing bandwidth control for the port.
- **Egress Rate (kbps) –** Enter the maximum data rate in kbps (multiples of 16) for outgoing traffic on the port.

© 2016 Araknis Networks®

QoS – Storm Control

Use Storm Control to limit the amount of broadcast, unknown multicast, and unknown unicast packets coming into ports on the switch. Excessive frames are discarded when the specified limit is passed.

Figure 80. Storm Control Table



- **Port –** Switch Port identifier.
- **Status –** Enable or Disable Storm Control for the specified port.
- **Broadcast (kbps) –** Check the box to enable Broadcast storm control, then enter the maximum allowed traffic rate of that type in kbps.
- **Unknown Multicast (kbps) –** Check the box to enable Unknown Multicast storm control, then enter the maximum allowed traffic rate of that type in kbps.
- **Unknown Unicast (kbps) –** Check the box to enable Unknown Unicast storm control, then enter the maximum allowed traffic rate of that type in kbps.

© 2016 Araknis Networks®

35 - ACL – Overview

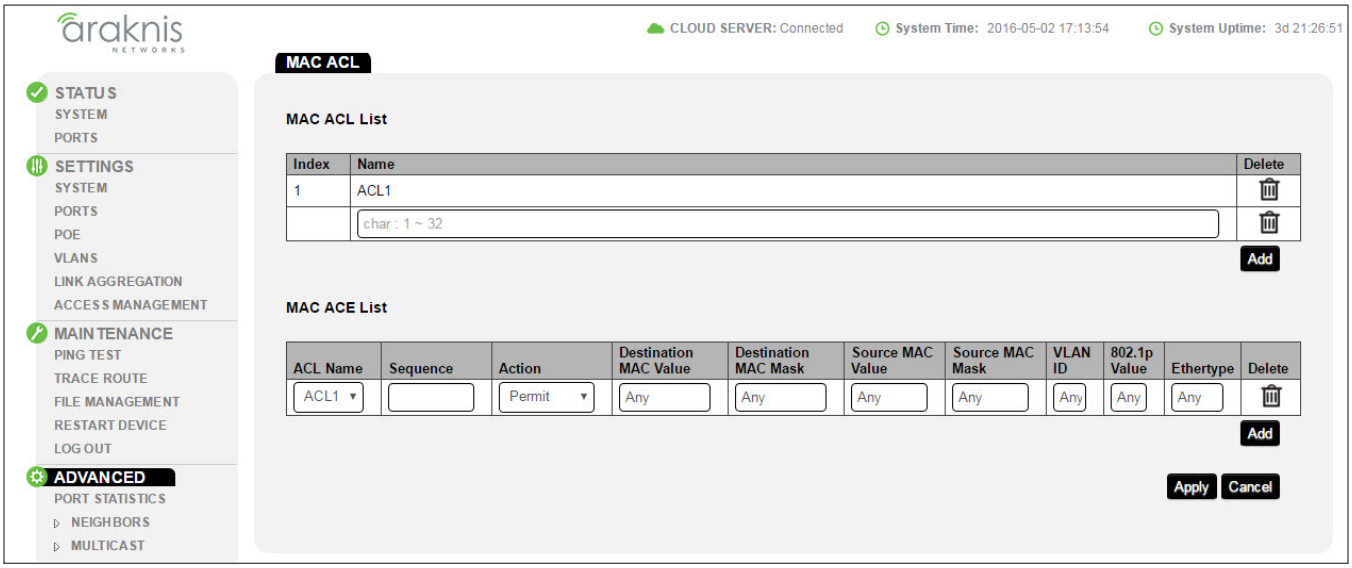
Access Control Lists (ACLs) are used for preventing access between or to devices on the network, primarily for many clients to one or vice versa. MAC-based ACLs can only control incoming traffic and IPv4/IPv6 -based ACLs can control both incoming and outgoing traffic.

Note – The ACL feature is only found in 310 series switches.

ACL – MAC ACL

Create MAC address-based rules for controlling incoming access to a device on any connected port.

Figure 81. MAC ACL List



MAC ACL List

Manage MAC ACLs.

- **Index –** List identifier.
- **Name –** Enter a name to describe the members or reason for the ACL list.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.

MAC ACE List

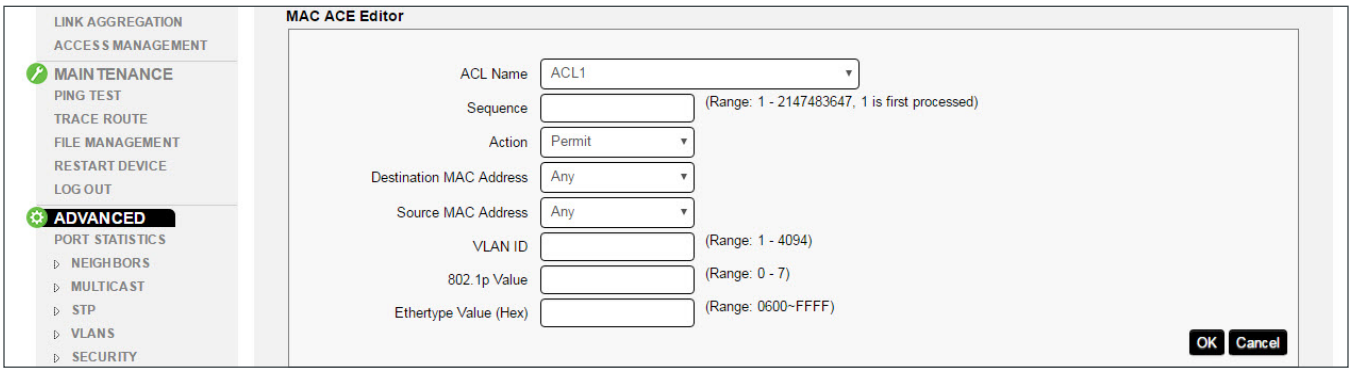
Define Access Control Entries (ACEs) associated with each ACL list.

- **Click any entry field to open the MAC ACE List Editor (see next page).**
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings. You must create an ACL List entry before adding a new ACE List entry.

© 2016 Araknis Networks®

MAC ACE List Editor

Figure 82. MAC ACL ACE List Editor



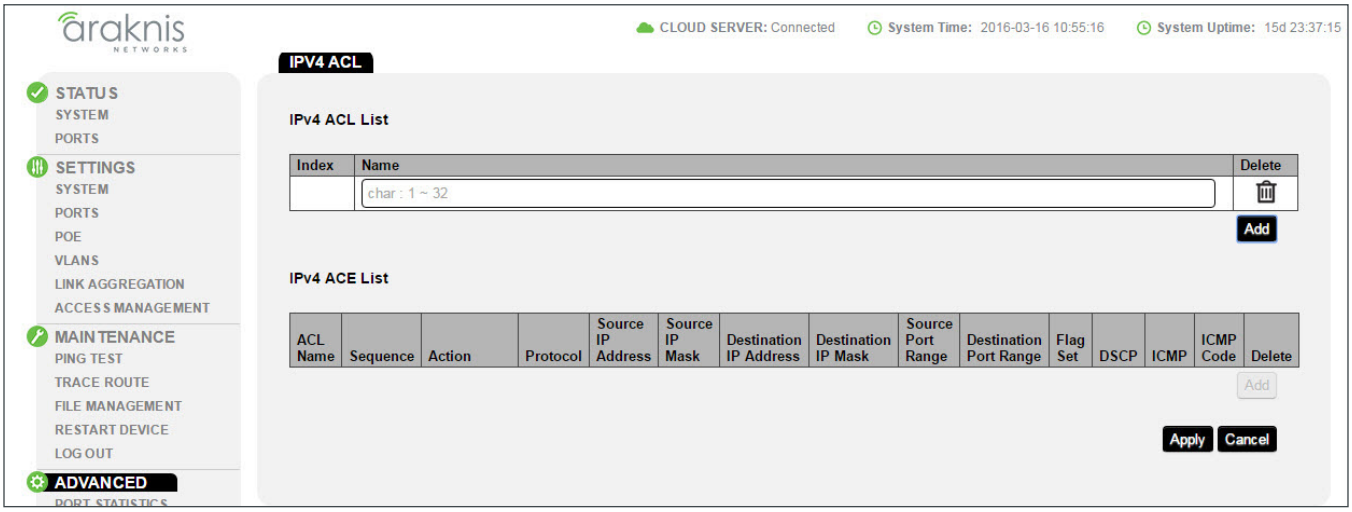
- **ACL Name –** Select the ACL to associate the ACE with.
- **Sequence –** Enter a value for the sequence in relation to other ACLs. The smallest value is processed first.
- **Action –** Select whether to Permit or Deny traffic that meets the set criteria.
- **Destination MAC Address –** Destination MAC address to monitor for. Options: Any or User Defined.
- **Destination MAC Mask –** Destination MAC mask to monitor for. Use this field to filter multiple addresses within a range. Only visible when monitoring a User Defined address.
- **Source MAC Value –** Source MAC address to monitor for. Options: Any or User Defined.
- **Source MAC Mask –** Source MAC mask to monitor for. Use this field to filter multiple addresses within a range. Only visible when monitoring a User Defined address.
- **VLAN ID –** Enter the VLAN ID to monitor for.
- **802.1p Value –** Enter the 802.1p value to monitor for.
- **Ethertype –** Leave blank. Entering a value will restrict traffic using certain protocols.
- **OK –** Click to accept the new settings and return to the MAC ACL ACE List.
- **Cancel –** Click to reject the new settings and return to the MAC ACL ACE List.

© 2016 Araknis Networks®

ACL – IPV4 ACL

Create rules for controlling incoming and outgoing traffic to any device on a connected port based on its IPv4 address.

Figure 83. IPv4 ACL Menu Page



IPv4 ACL List

- **Index –** List identifier.
- **Name –** Enter a name to describe the members or reason for the ACL list.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

IPv4 ACE List

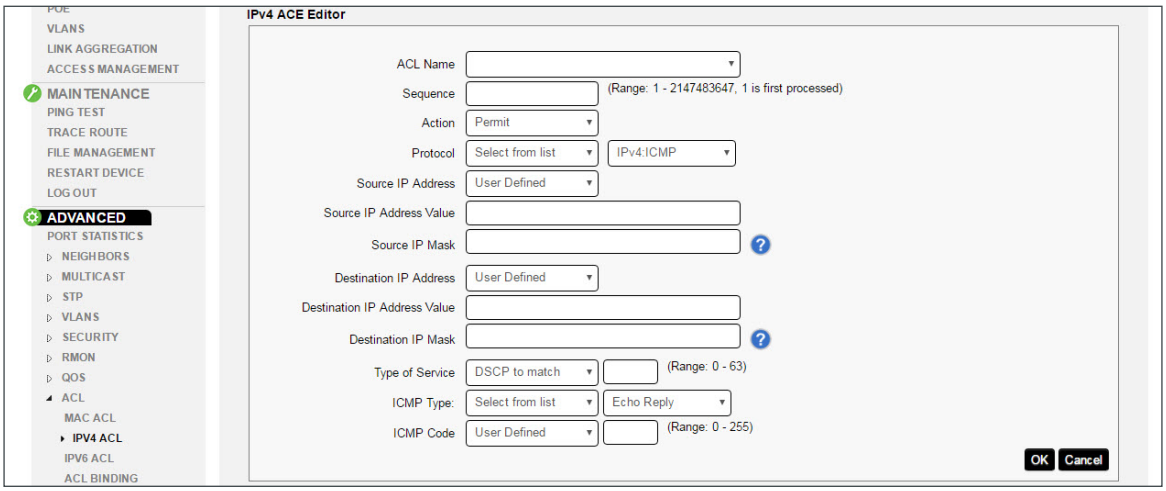
Define Access Control Entries (ACEs) associated with each ACL list.

- **Click any entry field to open the IPv4 ACE List Editor (see next page).**
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings. You must create an ACL List entry before adding a new ACE List entry.

© 2016 Araknis Networks®

IPv4 ACE List Editor

Figure 84. IPv4 ACL ACE Editor



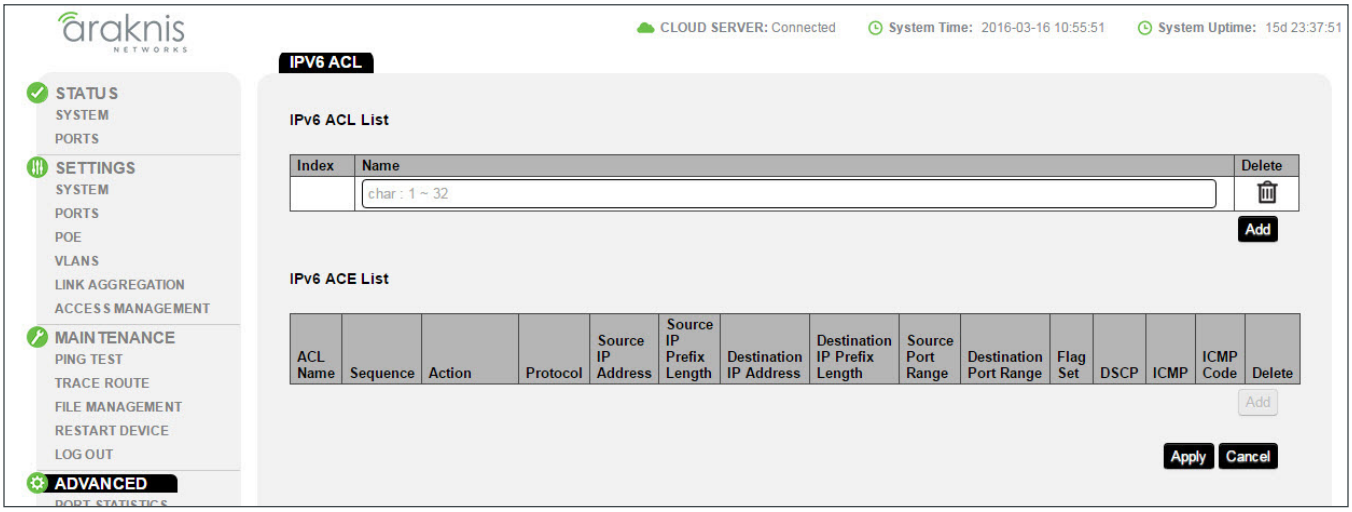
- **ACL Name –** Select the ACL to associate the ACE with.
- **Sequence –** Enter a value for the sequence in relation to other ACLs. The smallest value is processed first.
- **Action –** Select whether to Permit or Deny traffic that meets the set criteria.
- **Protocol –** Select whether traffic using a certain protocol is controlled. Options:
  - **Any –** No Protocol monitoring.
  - **Select from list –** Select the protocol to control from the drop down. Options: IPv4:ICMP, IPinIP, TCP, EGP, UDP, HMP, RDP, IPv6, IPv6:Rout, IPv6Frag, RSVP, IPv6:ICMP, OSPF, PIM, or L2TP.
  - **Protocol ID –** Enter the identifier for the protocol.
- **Source/Destination IP Address –** Select whether to monitor Any or a User Defined address.
- **Source/Destination IP Address Value –** Enter the address to monitor. Only visible when monitoring a User Defined address.
- **Source/Destination IP Mask –** Subnet mask to monitor. Use this field to filter multiple addresses within a range. Only visible when monitoring a User Defined address.
- **Source/Destination Port/Port Range –** Enter a port or ports to monitor.
- **Type of Service –** Select Any or DSCP to match (then enter range).
- **ICMP Type –** Select the IMCP type to monitor:
  - **Any –** No ICMP monitoring.
  - **Select from list –** Select the ICMP type to monitor. Options: EchoReply, Destination Unreachable, Source Quench, Echo Request, Router Advertisement, Router Solicitation, Time Exceeded, Timestamp, Timestamp Reply, or Traceroute.
  - **Protocol ID –** Enter the identifier for the protocol
- **ICMP Code**
  - **Any –** No ICMP code monitoring.
  - **User Defined –** Enter the code value to be monitored.
- **OK –** Click to accept the new settings and return to the IPv4 ACL ACE List.
- **Cancel –** Click to reject the new settings and return to the IPv4 ACL ACE List.

© 2016 Araknis Networks

ACL – IPV6 ACL

Create rules for controlling incoming and outgoing traffic to any device on a connected port based on its IPv6 address.

Figure 85. IPv6 ACL Menu Page



IPv6 ACL List

- **Index –** List identifier.
- **Name –** Enter a name to describe the members or reason for the ACL list.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

IPv6 ACE List

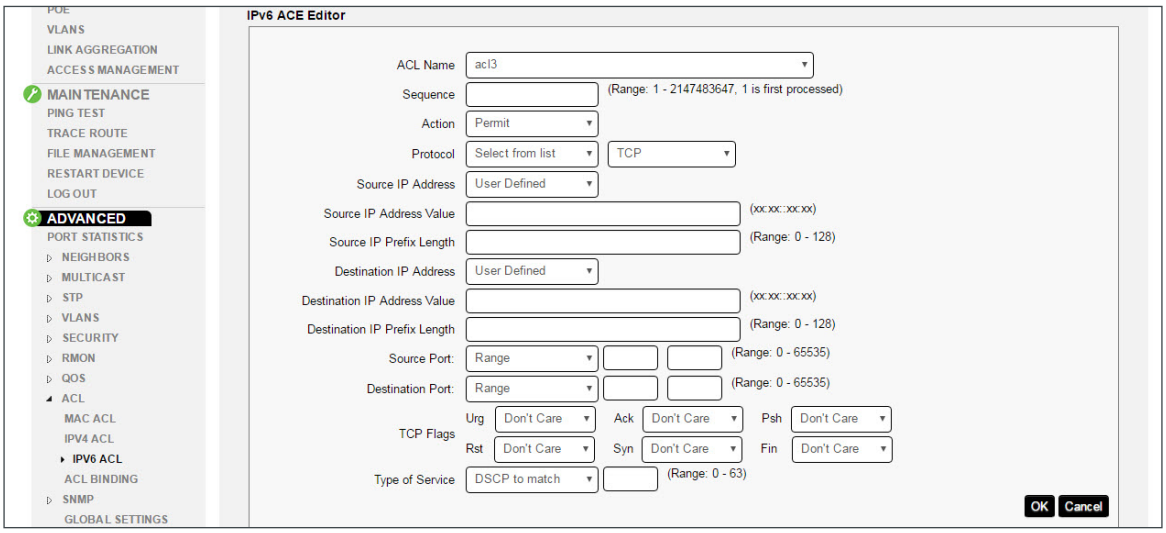
Define Access Control Entries (ACEs) associated with each ACL list.

- **Click any entry field to open the IPv4 ACE List Editor (see next page).**
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings. You must create an ACL List entry before adding a new ACE List entry.

© 2016 Araknis Networks®

IPv6 ACE List Editor

Figure 86. IPv4 ACL ACE Editor



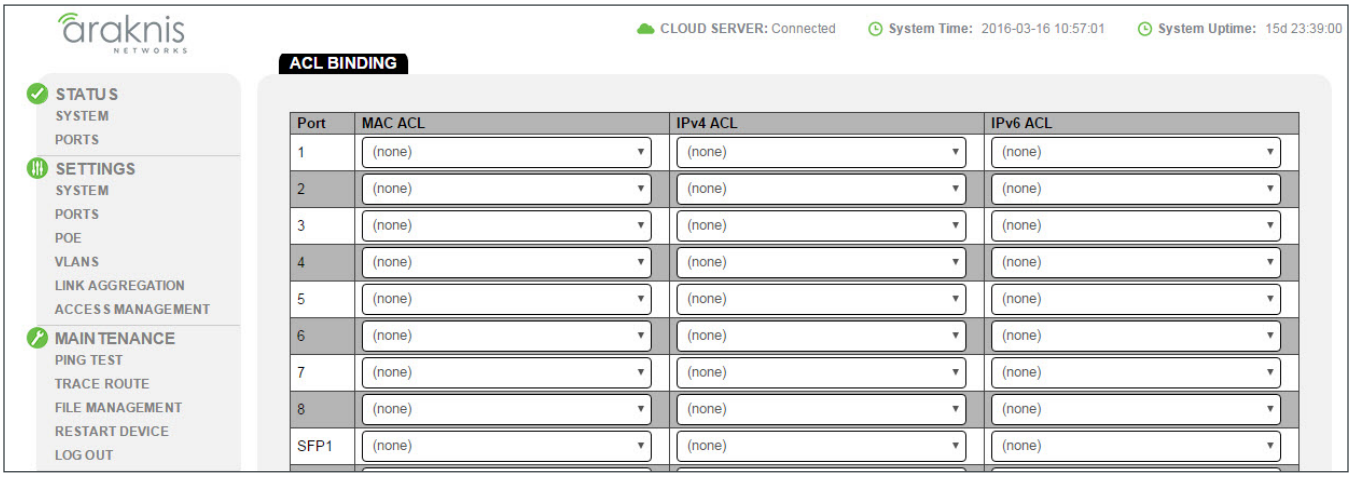
- **ACL Name –** Select the ACL to associate the ACE with.
- **Sequence –** Enter a value for the sequence in relation to other ACLs. The smallest value is processed first.
- **Action –** Select whether to Permit or Deny traffic that meets the set criteria.
- **Protocol –** Select whether traffic using a certain protocol is controlled. Options:
  - **Any –** No specific protocol monitoring.
  - **Select from list –** Select the protocol to control from the drop down. Options: TCP, UDP, IPv6:ICMP.
  - **Protocol ID –** Enter the identifier for the protocol.
- **Source/Destination IP Address –** Select whether to monitor Any or a User Defined address.
- **Source/Destination IP Address Value –** Enter the address to monitor. Only visible when monitoring a User Defined address.
- **Source/Destination IP Prefix Length –** Prefix to monitor. Use this field to filter multiple addresses within a range. Only visible when monitoring a User Defined address.
- **Source/Destination Port/Port Range –** Enter a port or ports to monitor.
- **TCP Flags –** Select options for monitoring TCP Flags when monitoring TCP Protocol.
- **Type of Service –** Select Any or DSCP to match (then enter range).
- **OK –** Click to accept the new settings and return to the IPv6 ACL ACE List.
- **Cancel –** Click to reject the new settings and return to the IPv6 ACL ACE List.

© 2016 Araknis Networks®

ACL – ACL Binding

Bind configured ACLs to switch ports to implement access control rules.

Figure 87. ACL Binding Menu Page



- **Port –** Switch Port identifier.
- **MAC/ IPv4/ IPv6 ACL –** Select an ACL entry to enable on the port. You must configure a rule in the respective ACL menu before configuring this setting.

© 2016 Araknis Networks®

36 - SNMP – Overview

The Simple Network Management Protocol (SNMP) is a Layer 7 protocol for managing and monitoring network equipment from a central SNMP manager.

Managed devices that support SNMP run their own agent software; the SNMP agent maintains a defined set of variables that are used to manage the switch. These objects are defined in a Management Information Base (MIB).

The Araknis switch includes an SNMP agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware and the traffic passing through its ports. SNMP client software can access the switch SNMP agent through SNMP community strings. These community strings are used for authentication.

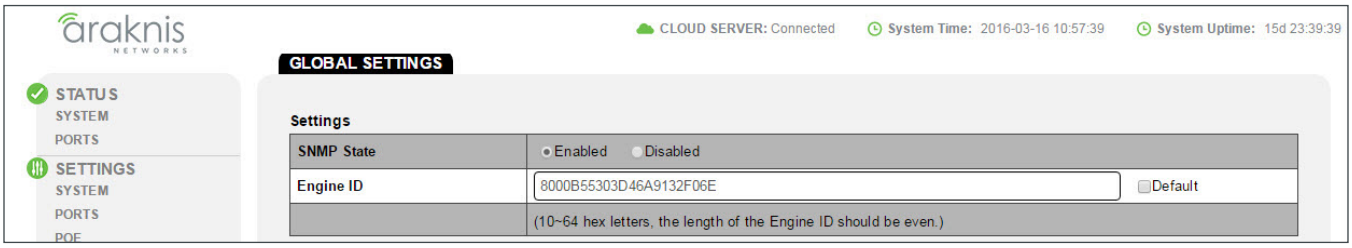
SNMPv3 provides additional security features that cover message integrity, authentication, and encryption, as well as controlling user access to specific objects in the MIB.

SNMP – Global Settings

Configure global settings for SNMP.

Settings

Figure 88. SNMP Global Settings



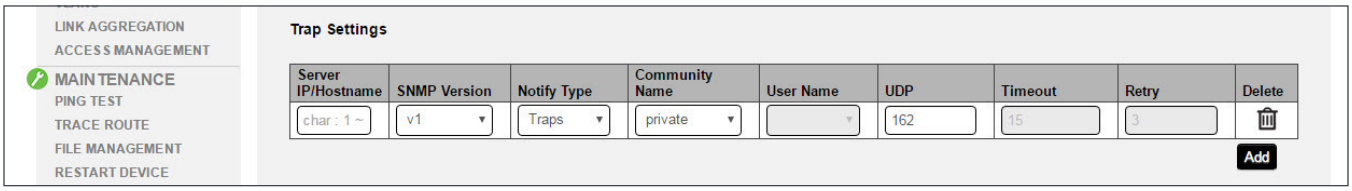
- **SNMP State –** Enabled or disable SNMP for the switch.
- **Engine ID –** Enter a unique SNMP Engine identifier. Check the box to use the default ID. The ID must be made from an even number of 10~64 hex letters. Enter this ID in other equipment when prompted to use the switch as the SNMP server.

© 2016 Araknis Networks

Trap Settings

Configure trap servers for the switch to send SNMP trap messages to.

Figure 89. SNMP Trap Settings

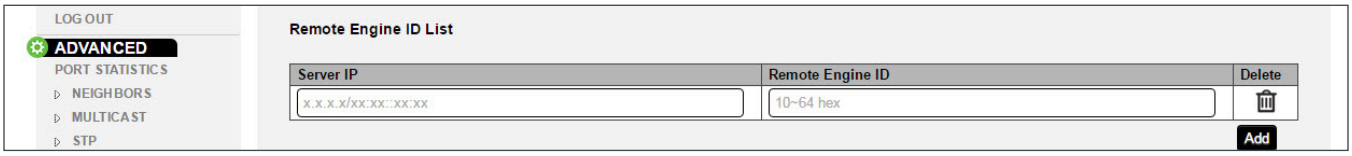


- **Server IP/Hostname –** Enter the address of the SNMP trap server.
- **SNMP Version –** Select the SNMP version used by the server. Options: v1, v2c, or v3.
- **Notify Type –** Select whether notifications are sent as Traps or as Informs.
- **Community Name –** Select whether the name is Public or Private.
- **User Name –** Select the username for logging into the server.
- **UDP –** UDP port for logging into the server.
- **Timeout –** Number of seconds to wait before declaring a timeout of connection from the server.
- **Retry –** Number of retry attempts to make after a timeout.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

Remote Engine ID List

Configure the switch to recognize SNMPv3 inform notifications from other engines.

Figure 90. SNMP Remote Engine ID List Settings



- **Server IP –** Enter an IP address for a remote SNMP server.
- **Remote Engine ID –** Enter the ID found in the Engine.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

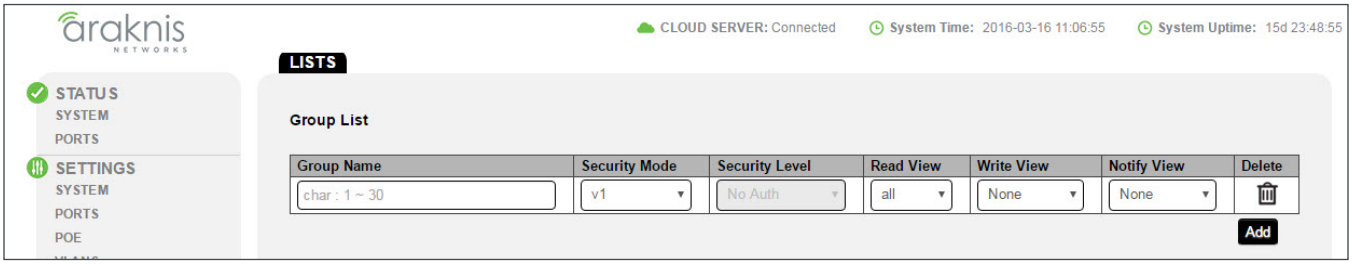
© 2016 Araknis Networks®

SNMP – Lists

Configure SNMP groups, events, community strings, and users.

Group Lists

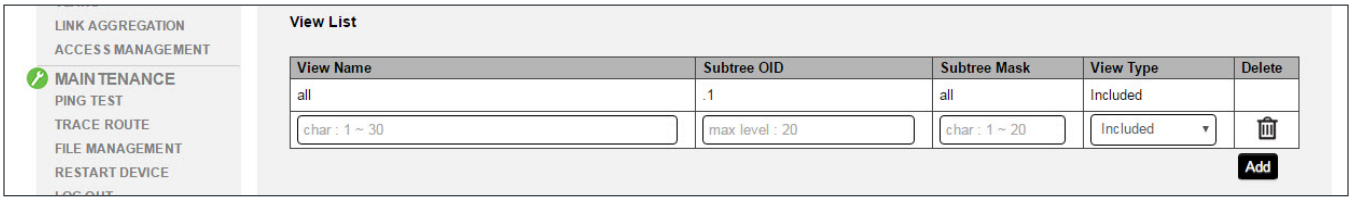
Figure 91. SNMP Group List



- **Group Name –** Enter a name to describe the group.
- **Security Mode –** Select the SNMP version for the group. Options: v1, v2c, or v3
- **Security Level –** Select the security level for users in the group. Options:
  - **NoAuth –** No authentication or privacy for group members.
  - **Auth –** SNMP messages are authenticated.
  - **Priv –** SNMP messages are encrypted.
- **Read View –** All; cannot be changed.
- **Write View –** Select None or All.
- **Notify View –** Select None or All.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

View List

Figure 92. SNMP View List

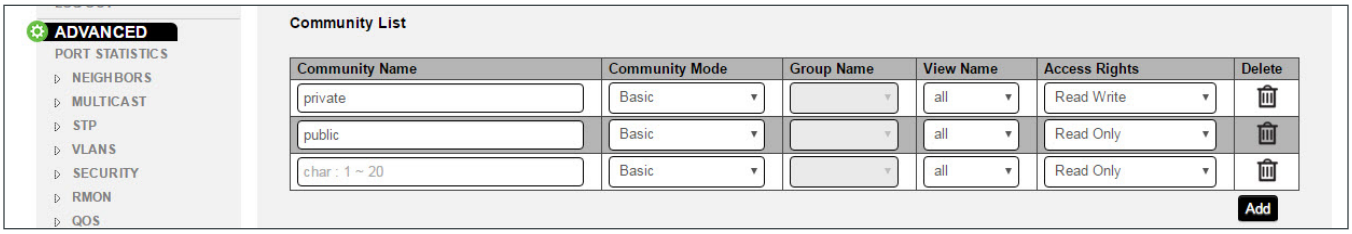


- **View Name –** Enter a name to identify the View.
- **Subtree OID –** Enter the Subtree Object Identifier (OID) value (must begin with a "**.**"). This value identifies an MIB tree that will be granted or denied access by the SNMP manager. Max level: 20
- **Subtree Mask –** Enter 0 (zero) for does not concern, or 1 for is concerned.
- **View Type –** Select Included or Excluded.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

© 2016 Araknis Networks®

SNMP Community List

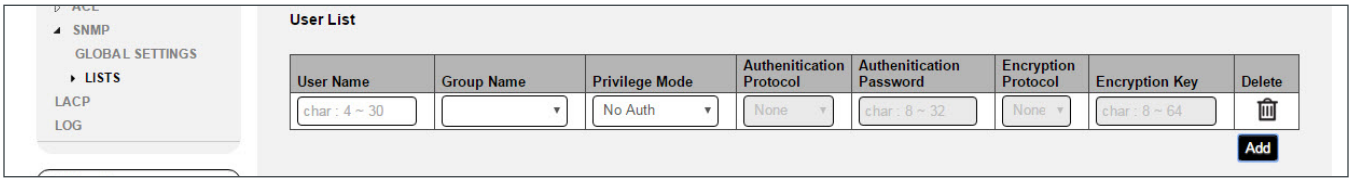
Figure 93. SNMP Community List



- **Community Name –** Enter a name to describe the community.
- **Community Mode –** Select Basic or Advanced
- **Group Name –** Select the group that community belongs to. You must configure a group before configuring this setting.
- **View Name –** Select All or a specific user. You must configure a user before configuring this setting.
- **Access Rights –** Select Read Only or
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

User List

Figure 94. SNMP User List



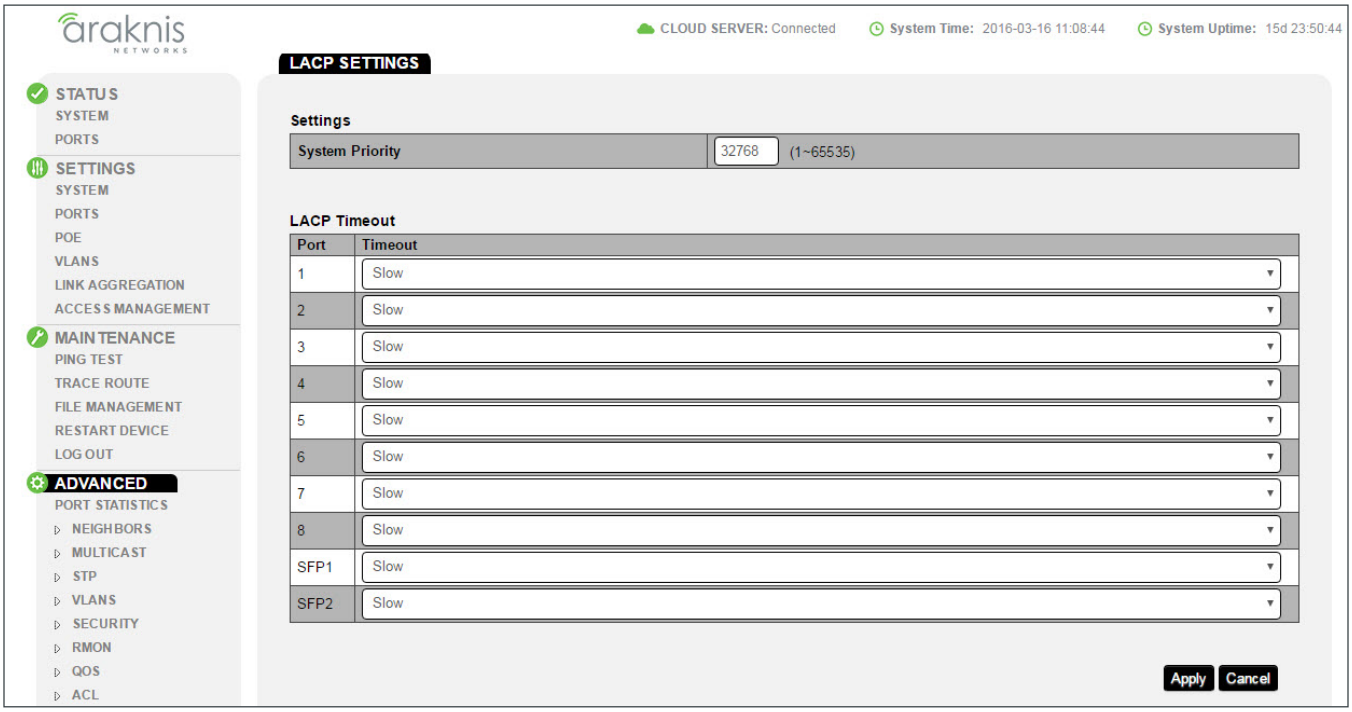
- **User Name –** Enter a name for the user.
- **Group Name –** Select which group the user is a part of. You must configure an SNMP group before configuring this setting.
- **Privilege Mode –**
  - **NoAuth –** No authentication or privacy for group members.
  - **Auth –** SNMP messages are authenticated.
  - **Priv –** SNMP messages are encrypted.
- **Authentication Protocol –** MD5 or SHA.
- **Authentication Password –** Enter the password for user authentication.
- **Encryption Protocol –** Select whether to use DES encryption with **Priv** privilege level messages.
- **Encryption Key –** Enter a key for DES encryption. Minimum 8 characters long.
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

© 2016 Araknis Networks

37 - Advanced LACP

Configure advanced parameters for LACP communication between switches connected by aggregated links.

Figure 95. Advanced LACP Settings



Settings

- **System Priority –** Enter a priority value for the switch. The device with the lowest value has priority.
  Range: 1-65535
  Default: 32768

LACP Timeout

- **Port –** Switch Port identifier.
- **Timeout –** Set the timeout speed for disabled ports to be removed from a trunk. Use the Low setting for busy trunked links.

© 2016 Araknis Networks®

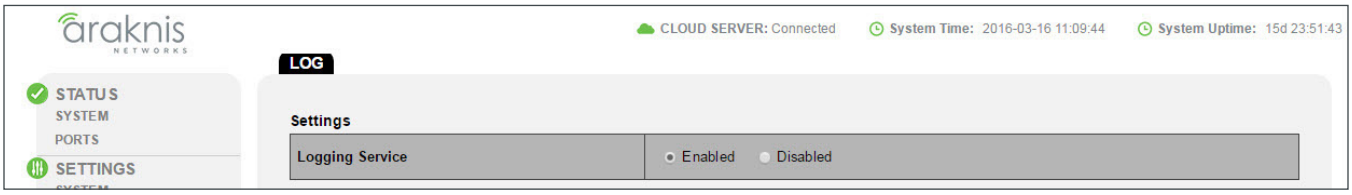
38 - Advanced Log

Configure advanced system logging. These settings affect the log on the system status page.

Settings

Turn advanced logging on or off.

Figure 96. Log Settings

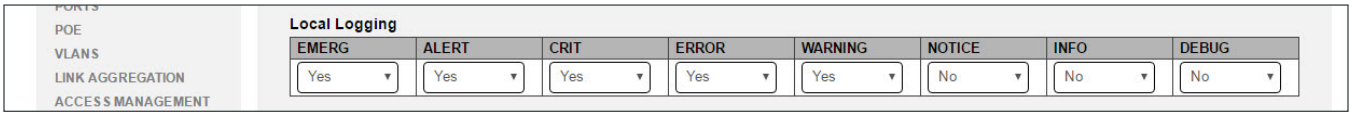


- **Logging Service –** Enabled or disable logging services.

Local Logging

Use this menu to configure whether log entries are submitted for the specified event severity. Values to the left indicate more severe events, and logs to the right indicate less severe events. Any NOTICE, INFO, or DEBUG events may be disregarded by the user.

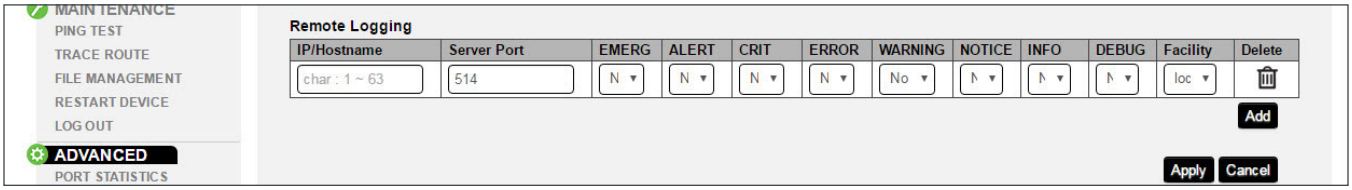
Figure 97. Local Logging



- **EMERG/ALERT/CRIT/ERROR/WARNING/NOTICE/INFO/DEBUG –** Select Yes to enable local logging for the event severity level or No to disable logging for the event severity level.

Remote Logging

Figure 98. Remote Logging



- **IP/Hostname –** Enter the IP address of the remote log server.
- **Server Port –** Enter the port configured for server communication.
- **EMERG/ALERT/CRIT/ERROR/WARNING/NOTICE/INFO/DEBUG –** Select Yes to enable remote logging for the event severity level or No to disable logging for the event severity level.
- **Facility –** Select the facility value for the remote logging event. Options: local0-local7.
  Default: local 0
- **Delete –** Click the trash can icon then click **Apply** to delete an entry.
- **Add –** Click to create a new entry. Remember to click **Apply** to save the new settings.

© 2016 Araknis Networks®

Table of Figures

Figure 1. Package Contents 7
Figure 2. Mounting Methods 10
Figure 3. Connection Diagram 11
Figure 4. EIA/TIA 568B Termination Pattern 11
Figure 5. PoE Calculation Example 12
Figure 6. OvrC Operation Diagram 13
Figure 7. Interface Layout 19
Figure 8. Apply Button 19
Figure 9. System Information and Port Status 20
Figure 10. Events Log 21
Figure 11. Port Status 22
Figure 12. System Information Settings 23
Figure 13. IP Address Settings Menu 24
Figure 14. Date and Time Settings, UPnP 25
Figure 15. Recommended System Settings 26
Figure 16. Jumbo Frame and Basic Port Settings 27
Figure 17. Advanced Port Settings 28
Figure 18. PoE Settings Menu 29
Figure 19. PoE Settings Menu 30
Figure 20. VLAN Settings 31
Figure 21. Access and Trunk Port Selection 31
Figure 22. Configuring Ports in a VLAN 32
Figure 23. Link Aggregation Settings Menu 33
Figure 24. Access Management Menu Page 35
Figure 25. Ping Test Page 36
Figure 26. Successful Ping Test Result 37
Figure 27. Failed Ping Test Result 37
Figure 28. Trace Route Test Page 38
Figure 29. Trace Route Result 39
Figure 30. File Management Menu 40
Figure 31. Dual Image Menu 41
Figure 32. Restart Page 42
Figure 33. Log Out Page 42
Figure 34. Detailed Port Statistics 44
Figure 35. Neighbors MAC Address Table 46
Figure 36. LLDP Information 47
Figure 37. LLDP Settings 48
Figure 38. LLDP Remote Device Menu 48
Figure 39. IGMP Snooping Settings 49
Figure 40. IGMP Snooping VLAN Settings 49

© 2016 Araknis Networks®

Figure 41. IGMP Snooping Querier Settings 50
Figure 42. IGMP Snooping Group List Settings 51
Figure 43. IGMP Snooping Router Settings 51
Figure 44. IGMP Snooping URC Settings 51
Figure 45. MLD Snooping Menu 52
Figure 46. MLD Snooping VLAN Settings 52
Figure 47. MLD Snooping Group List 52
Figure 48. MLD Snooping Router Settings 53
Figure 49. Global STP Settings Menu 54
Figure 50. Global STP Root Bridge Information 55
Figure 51. Global STP Basic Settings 56
Figure 52. STP CIST Port Settings Menu 57
Figure 53. STP MST Instance Settings Menu 59
Figure 54. STP MST Port Settings Menu 60
Figure 55. 802.1Q VLAN Settings Menu 61
Figure 56. 802.1Q PVID Settings Menu 61
Figure 57. Private VLANs Menu 62
Figure 58. Voice VLANs Settings 63
Figure 59. Voice VLANS OUI Settings 64
Figure 60. Voice VLANS Port Settings 64
Figure 61. Port Mirroring Page 65
Figure 62. 802.1x Global Settings Menu 65
Figure 63. 802.1x Port Settings Menu 66
Figure 64. 802.1x Authenticated Host Table 67
Figure 65. Radius Server Menu 68
Figure 66. Global DOS Settings Menu 69
Figure 67. DOS Port Settings Table 70
Figure 68. Port Security Table 71
Figure 69. MAC Address Filter Table 71
Figure 70. Event List 72
Figure 71. Event Log Table 72
Figure 72. Alarm List 73
Figure 73. History List 74
Figure 74. History Log Table 74
Figure 75. Global Settings 75
Figure 76. COS Mapping Table 75
Figure 77. DSCP Mapping Table 76
Figure 78. QoS Port Settings Table 76
Figure 79. Bandwidth Control Table 76
Figure 80. Storm Control Table 77
Figure 81. MAC ACL List 78

© 2016 Araknis Networks®

Figure 82. MAC ACL ACE List Editor 79
Figure 83. IPv4 ACL Menu Page 80
Figure 84. IPv4 ACL ACE Editor 81
Figure 85. IPv6 ACL Menu Page 82
Figure 86. IPv4 ACL ACE Editor 83
Figure 87. ACL Binding Menu Page 84
Figure 88. SNMP Global Settings 85
Figure 89. SNMP Trap Settings 86
Figure 90. SNMP Remote Engine ID List Settings 86
Figure 91. SNMP Group List 87
Figure 92. SNMP View List 87
Figure 93. SNMP Community List 88
Figure 94. SNMP User List 88
Figure 95. Advanced LACP Settings 89
Figure 96. Log Settings 90
Figure 97. Local Logging 90
Figure 98. Remote Logging 90

© 2016 Araknis Networks®

39 - AN-210-SW Specifications

		210-8P	210-16P	210-24P
Port				
10/100/1000Base RJ-45 Ports		8	16	24
1000Base SFP		2	2	2
PoE Ports		8	16	24
Physical Configuration				
Flash Memory		16MB	16MB	16MB
SDRAM		128MB	128MB	128MB
Packet Buffer		512KB	512KB	512KB
ESD & Surge				
Cable ESD		15Kv	15Kv	15Kv
Air ESD		+/- 8Kv	+/- 8Kv	+/- 8Kv
Contact ESD		+/- 6Kv	+/- 6Kv	+/- 6Kv
RJ-45 Surge		+/- 1.6Kv	+/- 1.6Kv	+/- 1.6Kv
PSU Surge		+/- 2.5Kv	+/- 2.5Kv	+/- 2.5Kv
Performance				
MAC Address Table Size		8K	8K	8K
Switching Capacity		20Gbps	36Gbps	52Gbps
Forwarding Rate		14.8Mbps	26.8Mbps	38.7Mbps
PoE Features				
802.3af/at Compliant		x	x	x
Max Power Output per Port		30W	30W	30W
PoE Power Budget		65W	130W	190W
PD Classification		x	x	x
Power Management	Enable/Disable per port	x	x	x
	Priority Setting per port	x	x	x
	Overloading Protection per port	x	x	x
	Power level setting per port	x	x	x
L2 Features				
HOL Blocking	Head-of-line blocking	x	x	x
Flow Control	802.3x, Back Pressure	x	x	x
Forwarding Mode	Store-and-forward	x	x	x
Energy Efficient Ethernet	IEEE 802.3az	x	x	x
Spanning Tree	802.1D (STP)	x	x	x
	802.1w (RSTP)	x	x	x
	802.1s (MSTP)	x	x	x
VLAN	802.1Q	x	x	x
	VLAN Group	x	x	x
	Port-based VLANs	x	x	x
	Private VLANs	-	-	-
	QinQ	-	-	-
	Protocol-based VLAN	-	-	-
	Voice VLAN	x	x	x
Link Aggregation	Static, 802.3ad LACP	x	x	x
	Max ports per group	8	8	8
	Max Group	8	8	8
Multicast Snooping	IGMP Snooping v1/v2/v3; MLD Snooping v1/v2	x	x	x
	IGMP Querier	x	x	x
	IGMP Immediate Leaxe	x	x	x
Storm Control	Broadcast/UnKnown Multi-cast/Unknown Unicast	x	x	x
Jumbo Frame Support		9k	9k	9k

© 2016 Araknis Networks®

		210-8P	210-16P	210-24P
QoS Features				
Number of priority queues		x	x	x
Rate Limiting	Ingress	x	x	x
	Egress	x	x	x
DiffServ (RFC2474)		x	x	x
Scheduling	WRR	x	x	x
	Strict	x	x	x
	Hybrid	-	-	-
CoS	802.1p	x	x	x
	IP ToS Precedence	x	x	x
	IP DSCP	x	x	x
Security				
Port Security (MAC-based)		x	x	x
802.1x		x	x	x
ACL	L2	-	-	-
	L3	-	-	-
	L4	-	-	-
IP Source Guard		-	-	-
RADIUS		x	x	x
TACACS+		-	-	-
HTTPS and SSL		x	x	x
SSH v2.0		x	x	x
MAC Filter		x	x	x
IP Filter		-	-	-
Management				
Management	CLI, Web, Telnet	x	x	x
Dual FW Images		-	-	-
FW Upgrade	TFTP upgrade	x	x	x
	HTTP upgrade	x	x	x
Management Access Filtering	SNMP/Web/Telnet	x	x	x
SNMP	v1,v2c,v3	x	x	x
SNTP		x	x	x
RMON (1,2,3 and 9 groups)		x	x	x
DHCP	Server	-	-	-
	Client	x	x	x
	Relay	-	-	-
	Option82	-	-	-
	Snooping	-	-	-
Exent log	local flash, remote serxer	x	x	x
sFlow		-	-	-
Port Mirroring	One to One, Many to One	x	x	x
Remote Ping		x	x	x
LLDP (IEEE802.1ab)		x	x	x
Cable Diagnostics		x	x	x
UPnP		x	x	x
Environmental				
Dimensions	Inches (WxHxD)	12.99 x 9.06 x 1.75	18.98 x 10.24 x 1.75	18.98 x 10.24 x 1.75
Power Supply		100-240x AC, 50/60 Hz	100-240x AC, 50/60 Hz	100-240x AC, 50/60 Hz
Maximum Power Consumption (Full PoE | No PoE)	Watts	86.50 | 13.30	162.08 | 21.31	291.81 | 23.71
Operating Temperature		0-50°C	0-50°C	0-50°C
Humidity (non-condensing)		10 - 90%	10 - 90%	10 - 90%

© 2016 Araknis Networks®

40 - AN-310-SW Specifications

SPEC		310-8P	310-16P	310-24P	310-8	310-16	310-24
Port							
10/100/1000Base RJ-45 Ports		8	16	24	8	16	24
1000Base SFP		2	2	2	2	2	2
PoE Ports		8	16	24	8	16	24
Physical Configuration							
Flash Memory		16MB	16MB	16MB	16MB	16MB	16MB
SDRAM		128MB	128MB	128MB	128MB	128MB	128MB
Packet Buffer		512KB	512KB	512KB	512KB	512KB	512KB
ESD & Surge							
Cable ESD		15Kx	15Kx	15Kx	15Kx	15Kx	15Kx
Air ESD		+/- 8Kx	+/- 8Kx	+/- 8Kx	+/- 8Kx	+/- 8Kx	+/- 8Kx
Contact ESD		+/- 6Kx	+/- 6Kx	+/- 6Kx	+/- 6Kx	+/- 6Kx	+/- 6Kx
RJ-45 Surge		+/- 1.6Kx	+/- 1.6Kx	+/- 1.6Kx	+/- 1.6Kx	+/- 1.6Kx	+/- 1.6Kx
PSU Surge		+/- 2.5Kx	+/- 2.5Kx	+/- 2.5Kx	+/- 2.5Kx	+/- 2.5Kx	+/- 2.5Kx
Performance							
MAC Address Table Size		8K	8K	8K	8K	8K	8K
Switching Capacity		20Gbps	36Gbps	52Gbps	20Gbps	36Gbps	52Gbps
Forwarding Rate		14.8Mbps	26.8Mbps	38.7Mbps	14.8Mbps	26.8Mbps	38.7Mbps
PoE Features							
802.3af/at Compliant		x	x	x	-	-	-
Max Power Output per Port		30W	30W	30W	-	-	-
PoE Power Budget		130W	250W	375W	-	-	-
PD Classification		x	x	x	-	-	-
Power Management	Enable/Disable per port	x	x	x	-	-	-
	Priority Setting per port	x	x	x	-	-	-
	Overloading Protection per port	x	x	x	-	-	-
	Power level setting per port	x	x	x	-	-	-
L2 Features							
HOL Blocking	Head-of-line blocking	x	x	x	x	x	x
Flow Control	802.3x, Back Pressure	x	x	x	x	x	x
Forwarding Mode	Store-and-forward	x	x	x	x	x	x
Energy Efficient	IEEE 802.3az	x	x	x	x	x	x
Spanning Tree	802.1D (STP)	x	x	x	x	x	x
	802.1w (RSTP)	x	x	x	x	x	x
	802.1s (MSTP)	x	x	x	x	x	x
VLAN	802.1Q	x	x	x	x	x	x
	VLAN Group	x	x	x	x	x	x
	Port-based VLANs	x	x	x	x	x	x
	Private VLANs	x	x	x	x	x	x
	QinQ	-	-	-	-	-	-
	Protocol-based VLAN	-	-	-	-	-	-
	xoice VLAN	x	x	x	x	x	x
Link Aggregation	Static, 802.3ad LACP	x	x	x	x	x	x
	Max ports per group	8	8	8	8	8	8
	Max Group	8	8	8	8	8	8
Multicast Snooping	IGMP Snooping v1/v2/v3 MLD	x	x	x	x	x	x
	IGMP Querier	x	x	x	x	x	x
	IGMP Immediate Leave	x	x	x	x	x	x
Storm Control	Broadcast/UnKnown Multi-	x	x	x	x	x	x
Jumbo Frame Support		9k	9k	9k	9k	9k	9k

© 2016 Araknis Networks®

SPEC		310-8P	310-16P	310-24P	310-8	310-16	310-24
QoS Features							
Number of priority queues		x	x	x	x	x	x
Rate Limiting	Ingress	x	x	x	x	x	x
	Egress	x	x	x	x	x	x
DiffSerx (RFC2474)		x	x	x	x	x	x
Scheduling	WRR	x	x	x	x	x	x
	Strict	x	x	x	x	x	x
	Hybrid	-	-	-	-	-	-
CoS	802.1p	x	x	x	x	x	x
	IP ToS Precedence	x	x	x	x	x	x
	IP DSCP	x	x	x	x	x	x
Security							
Port Security (MAC-based)		x	x	x	x	x	x
802.1x		x	x	x	x	x	x
ACL	L2	x	x	x	x	x	x
	L3	x	x	x	x	x	x
	L4	x	x	x	x	x	x
IP Source Guard		-	-	-	-	-	-
RADIUS		x	x	x	x	x	x
TACACS+		-	-	-	-	-	-
HTTPS and SSL		x	x	x	x	x	x
SSH x2.0		x	x	x	x	x	x
MAC Filter		x	x	x	x	x	x
IP Filter		-	-	-	-	-	-
Management							
Management	CLI, Web, Telnet	x	x	x	x	x	x
Dual FW Images		x	x	x	x	x	x
FW Upgrade	TFTP upgrade	x	x	x	x	x	x
	HTTP upgrade	x	x	x	x	x	x
Management	SNMP/Web/Telnet	x	x	x	x	x	x
SNMP	v1,v2c,v3	x	x	x	x	x	x
SNTP		x	x	x	x	x	x
RMON (1,2,3 and 9 groups)		x	x	x	x	x	x
DHCP	Server	-	-	-	-	-	-
	Client	x	x	x	x	x	x
	Relay	-	-	-	-	-	-
	Option82	-	-	-	-	-	-
	Snooping	-	-	-	-	-	-
Event log	local flash, remote server	x	x	x	x	x	x
sFlow		-	-	-	-	-	-
Port Mirroring	One to One, Many to One	x	x	x	x	x	x
Remote Ping		x	x	x	x	x	x
LLDP (IEEE802.1ab)		x	x	x	x	x	x
Cable Diagnostics		x	x	x	x	x	x
UPnP		x	x	x	x	x	x
Environmental							
Dimensions	Inches (WxHxD)	12.99 x 9.06 x 1.75	18.98 x 10.24 x 1.75	18.98 x 10.24 x 1.75	12.99 x 9.06 x 1.75	18.98 x 10.24 x 1.75	18.98 x 10.24 x 1.75
Power Supply		100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz	100-240V AC, 50/60 Hz
Maximum Power Consumption (Watts) (Full PoE | No PoE)		10.22	12.64	18.34	163.00 | 12.70	287.93 | 22.24	425.15 | 38.75
Operating Temperature		0-50°C	0-50°C	0-50°C	0-50°C	0-50°C	0-50°C
Humidity (non-condensing)		10 - 90%	10 - 90%	10 - 90%	10 - 90%	10 - 90%	10 - 90%

© 2016 Araknis Networks®

41 - Appendix – Safety and Regulatory Information

FCC Warning

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operations of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Warning

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

UL Statement

All models have been evaluated by UL. This device is intended for indoor use only. It should not be connected to an Ethernet network with outside plant routing.

The user must use the class I optical transceivers which conform to U.S. code of federal regulation, 21 CFR 1040.

This equipment is only to be connected to PoE networks without routing to outside plants.

© 2016 Araknis Networks®

42 - Warranty

2 Year Limited Warranty

Araknis Networks® products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to a designated service center with prior notification and an assigned return authorization (RA) number. Contact technical support for an RA number.

Contact Information

Web: www.araknisnetworks.com

Phone: Technical Support - (866) 838.5052

Email: techsupport@araknisnetworks.com

© 2016 Araknis Networks®

160509-1500