

Models:


AN-210-SW-F/R-8-POE
AN-210-SW-F/R-16-POE
AN-210-SW-F/R-24-POE
AN-210-SW-F-48-POE
AN-310-SW-F/R-8
AN-310-SW-F/R-16
AN-310-SW-F/R-24
AN-310-SW-F-48
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.



Table of Contents

1 - Welcome to Araknis Networks™	8
2 - Package Contents	8
3 - Series Overview	8
4 - Device Layout	9
Rear Facing Models	10
Front Facing Models	10
5 - Hardware Installation	11
Mounting	11
Rack Mount	11
Wall Mount	11
Shelf Mount	11
Rack Mounting Guidelines	12
Connections	13
Input Power Requirements	13
Network Cable Requirements	13
SFP Ports	13
Switch	13
PoE Budget Calculation Example	14
6 - OvrC Setup	15
7 - Interface Access	16
OvrC Web Connect Access	16
Direct Access Using LAN IP Address (DHCP)	17
Default IP Address Access	18
8 - Interface Overview	21
Page Layout	21
Applying or Canceling Changes	21
9 - Switch Status Pages	22
System Status Page	22
System Information	22
Port Status	22
Events Log	23
Port Status Page	24
10 - System Settings	25
System Information	25
IP Address Settings	26
IPv4 IP Settings	26
IPv6 IP Settings	26
Date and Time Settings	27
UPnP Setting	27
11 - Recommended Setup – System Settings	28
12 - Port Configuration Settings	29
Jumbo Frame Setting	29
Basic Port Settings	29
Advanced Port Settings	30



13 - PoE Settings	31
PoE Setup and Troubleshooting	32
Checking Status of PoE Devices	32
Configuring PoE Ports	32
Troubleshooting PoE Issues	32
14 - VLAN Settings (Basic Port-Based)	33
Access and Trunk Port Selection	33
Creating a New VLAN	34
15 - Link Aggregation Settings	35
Creating a New Link Aggregation Rule	36
16 - Access Management Settings	37
User Management	37
HTTP/Telnet/SSH	37
17 - Maintenance Menus	38
Ping Test	38
Running a Ping Test	38
Understanding Ping Test Results	39
Troubleshooting Using Ping Test Results	39
Trace Route Test	40
Running a Trace Route Test	40
Understanding Trace Route Test Results	41
File Management Settings	42
Configuration File	42
Firmware	42
Dual Image	43
Firmware Update Instructions	43
Restart	44
Log Out	44
18 - Advanced Menus	45
19 - Advanced Port Statistics	46
20 - Neighbors - MAC Address Table	48
Static and Dynamic MAC Address	48
21 - Neighbors - LLDP	49
Information Table	49
Settings	50
Remote Device Table	50
22 - Multicast - IGMP Snooping	51
Settings	51
VLAN Settings	51
Querier Settings	52
Group List	53
Router Settings	53
URC Settings	53



23 - Multicast - MLD Snooping	54
Settings	54
VLAN Settings	54
Group List	54
Router Settings	55
24 - STP - Overview	56
STP - Global Settings	56
Settings	56
Root Bridge Information	57
Basic Setting	58
25 - STP (Spanning Tree Protocol) Overview	59
STP - CIST Settings	59
Port Settings	59
STP - MST Settings	61
Instance Settings	61
Port Settings	62
26 - Advanced VLANs - Overview	63
Advanced VLANs - 802.1Q VLANs	63
VLAN Settings	63
PVID Settings	63
Advanced VLANs - Private VLANs	64
Advanced VLANs - Voice VLANs	65
General Settings	65
OUI Settings	66
Port Settings	66
27 - Security - Port Mirroring	67
28 - Security - 802.1x	67
802.1x Global Setting	67
Port Settings	68
Authenticated Host	69
29 - Security - Radius Server	70
30 - Security - DOS	71
Global Settings	71
Global DOS Security Settings, Continued	72
Port Settings	72
31 - Security - Port Security	73
32 - Security - MAC Address Filter	73
33 - RMON Overview	74
RMON - Event List	74
RMON - Event Log Table	74
RMON - Alarm List	75
RMON - History List	76
RMON - History Log Table	76



34 - QoS - Overview	77
QoS - Global Settings	77
QoS - COS Mapping	77
QoS - DSCP Mapping	78
QoS - Port Settings	78
QoS - Bandwidth Control	78
QoS - Storm Control	79
35 - ACL - Overview	80
ACL - MAC ACL	80
MAC ACL List	80
MAC ACE List	80
MAC ACE List Editor	81
ACL - IPV4 ACL	82
IPv4 ACL List	82
IPv4 ACE List	82
IPv4 ACE List Editor	83
ACL - IPV6 ACL	84
IPv6 ACL List	84
IPv6 ACE List	84
IPv6 ACE List Editor	85
ACL - ACL Binding	86
36 - SNMP - Overview	87
SNMP - Global Settings	87
Settings	87
Trap Settings	88
Remote Engine ID List	88
SNMP - Lists	89
Group Lists	89
View List	89
SNMP Community List	90
User List	90
37 - Advanced LACP	91
Settings	91
LACP Timeout	91
38 - Advanced Log	92
Settings	92
Local Logging	92
Remote Logging	92
39 - AN-210-SW Hardware Specifications	96
40 - AN-310-SW (Non-PoE) Hardware Specifications	97
41 - AN-310-SW-POE Hardware Specifications	98
42 - General Specifications (All 210/310 Models)	99



43 - Appendix - Safety and Regulatory Information	101
FCC Warning	101
CE Warning	101
UL Statement	101
44 - Warranty	102
2 Year Limited Warranty	102
Contact Information	102

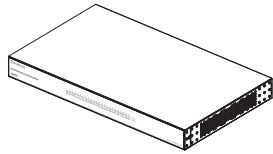


1 - Welcome to Araknis Networks™

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

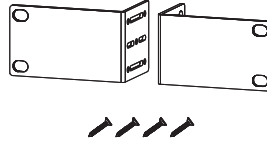
Figure 1. Package Contents



Switch (1)



Rubber Feet for Flat Surfaces (4)



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



Quick Start Guide



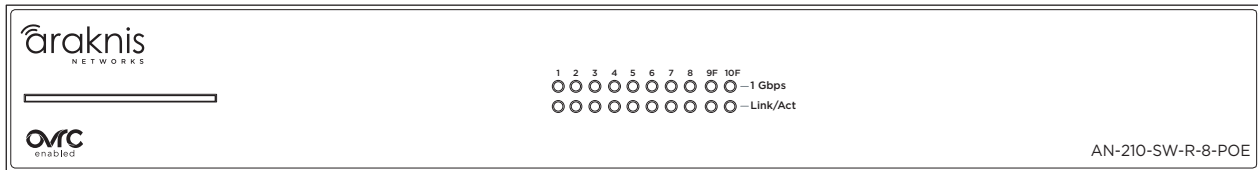
AC Power Cord

3 - Series Overview

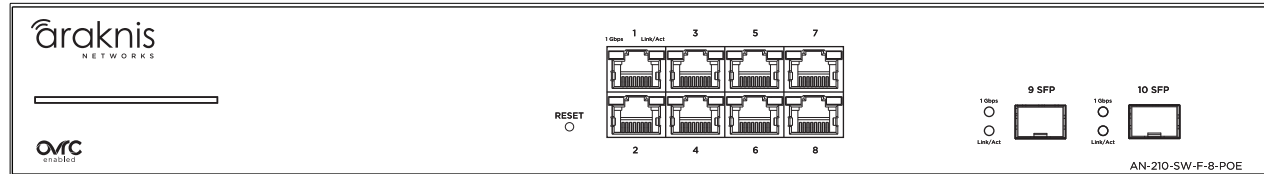
Model	Ethernet Ports	SFP Ports	PoE Budget (Watts)
AN-210-SW-F/R-8-POE	8	2	65W
AN-210-SW-F/R-16-POE	16	2	130W
AN-210-SW-F/R-24-POE	24	2	190W
AN-210-SW-F-48-POE	48	4	375W
AN-310-SW-F/R-8	8	2	-
AN-310-SW-F/R-16	16	2	-
AN-310-SW-F/R-24	24	2	-
AN-310-SW-F-48	48	4	-
AN-310-SW-F/R-8-POE	8	2	130W
AN-310-SW-F/R-16-POE	16	2	250W
AN-310-SW-F/R-24-POE	24	2	375W



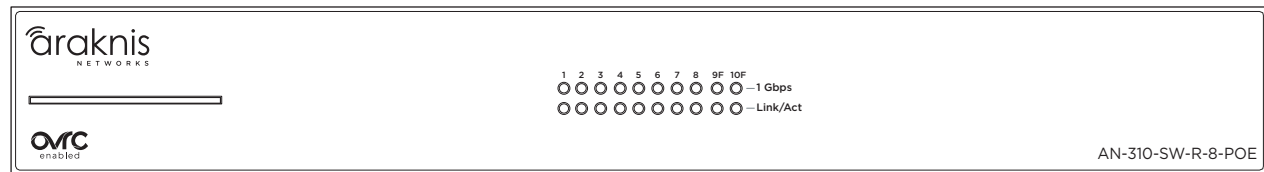
4 - Device Layout



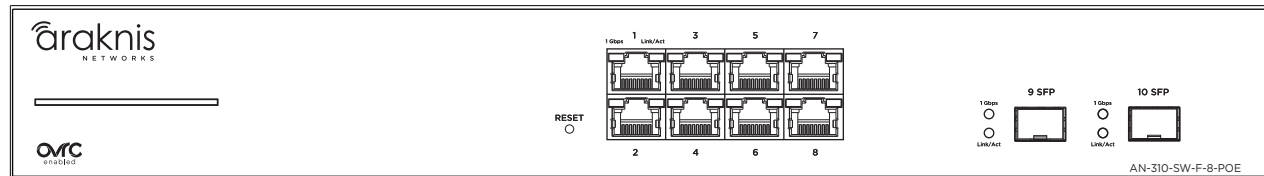
AN-210-SW-R-8-POE



AN-210-SW-F-8-POE



AN-310-SW-R-8-POE



AN-310-SW-F-8-POE

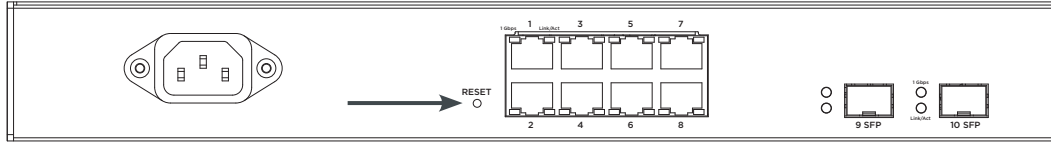
1. **Power LED** - On: system is up.
Off: system is down.
2. **1Gbps LED** - On: port connected at 1000Mbps speed.
Off: port is connected at 10/100Mbps speed.
3. **Link/Act LED** - On: port is connected to another device.
Blinking: packets are running through the port.
Off: port is not connected to a device.

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

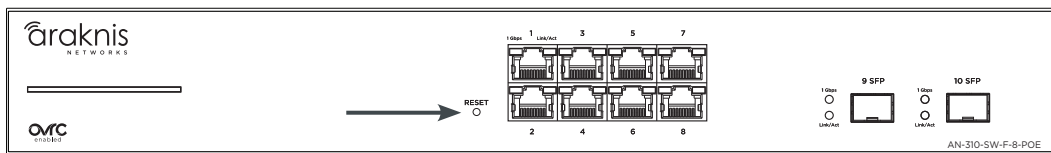
Factory Reset

Reboot or default the switch configuration settings.

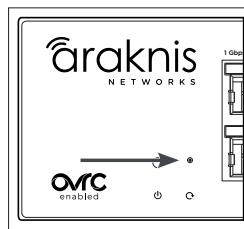
Rear Facing Models



Front Facing Models



48 Port Models



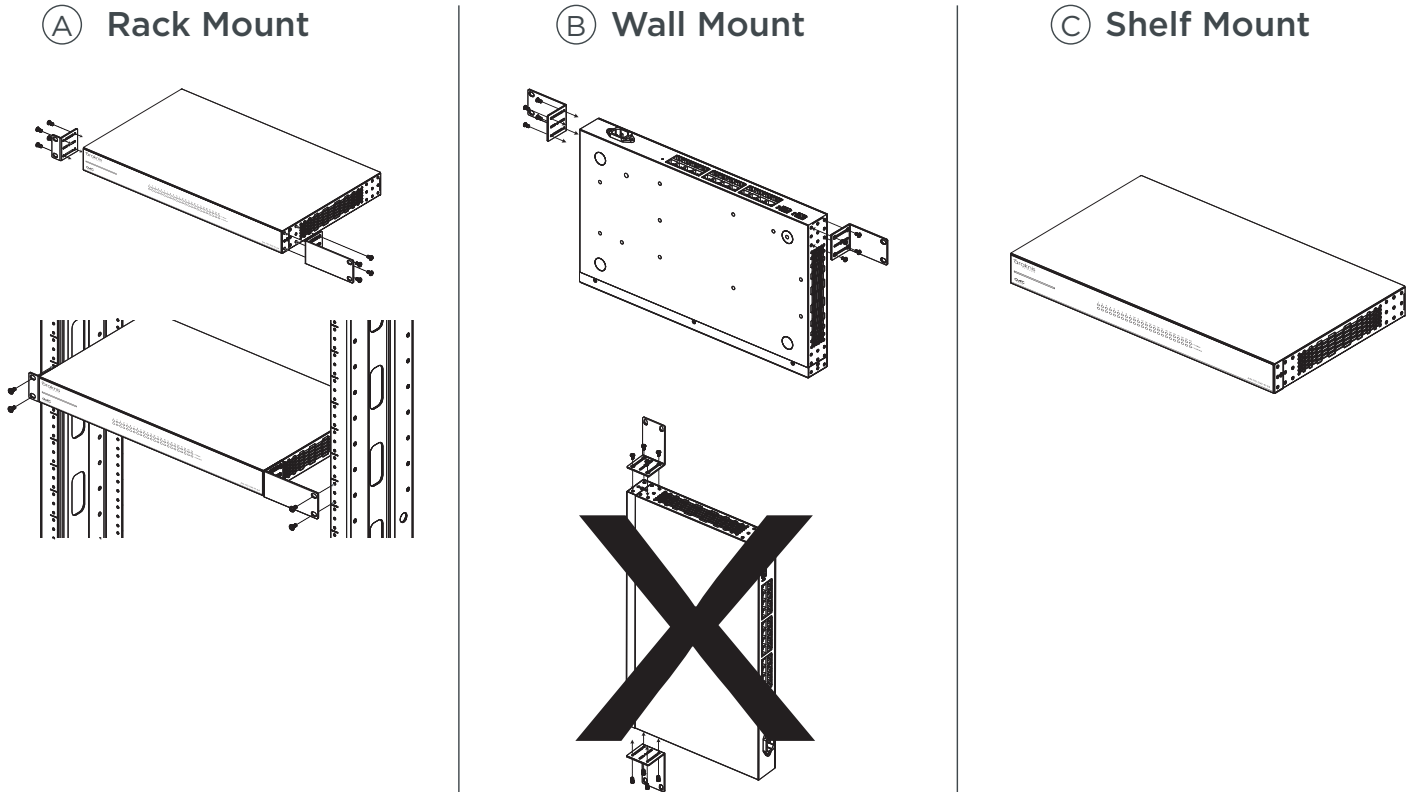
- 1. Reboot** – Press and hold the RESET button on the back of the switch for 5 seconds, then release. The switch will power cycle and the front status lights will flash.
- 2. Factory Reset** – Press and hold the RESET button for 10-15 seconds until the status LEDs flash once. The switch will power cycle and be reset to factory default settings.



5 - Hardware Installation

Mounting

Figure 2. Mounting Methods



Note - The switch must be wall mounted with the Ethernet ports facing either the floor or the ceiling. Do not mount the switch with the ports facing to the side.

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.

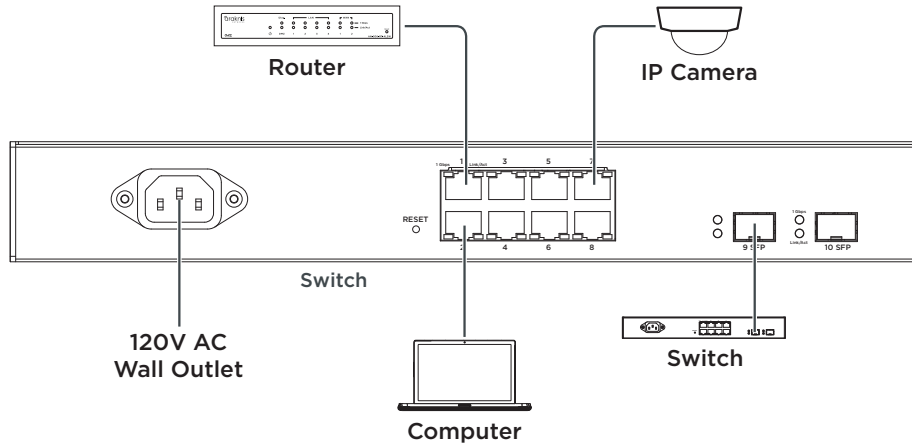
Circuit Overloading – Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing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



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.

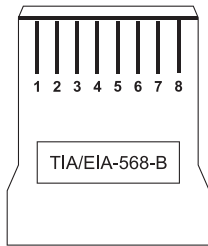
Input Power Requirements

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.



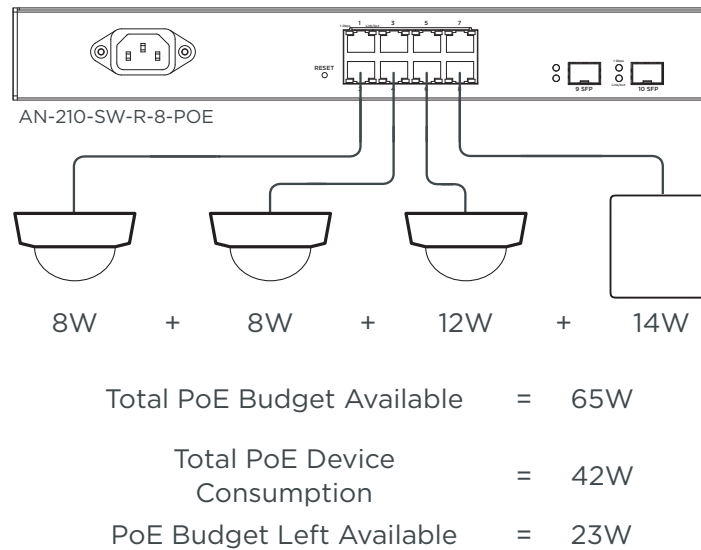
PoE Budgeting

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-210-SW-F-48-POE	375W
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

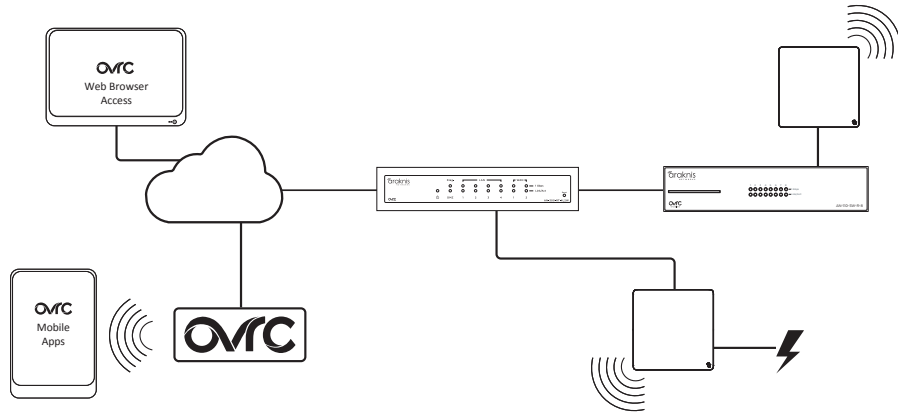


Note - Port PoE settings may be modified using the PoE Settings menu. Click to see information and instructions.

6 - OvrC Setup

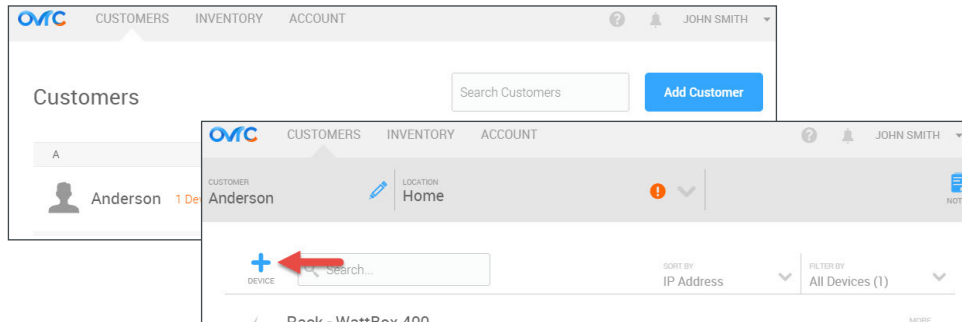
OvrC provides remote firmware upgrades, real-time notifications, and intuitive customer management, right from your computer or mobile device. Setup is plug-and-play, with no port forwarding or DDNS address required.

Figure 6. OvrC Operation Diagram

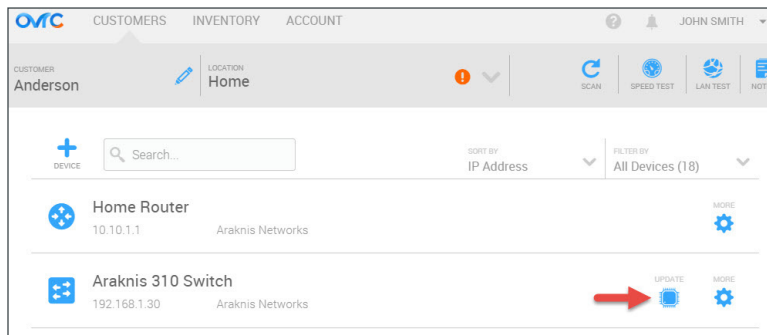


To add this device to your OvrC account:

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.





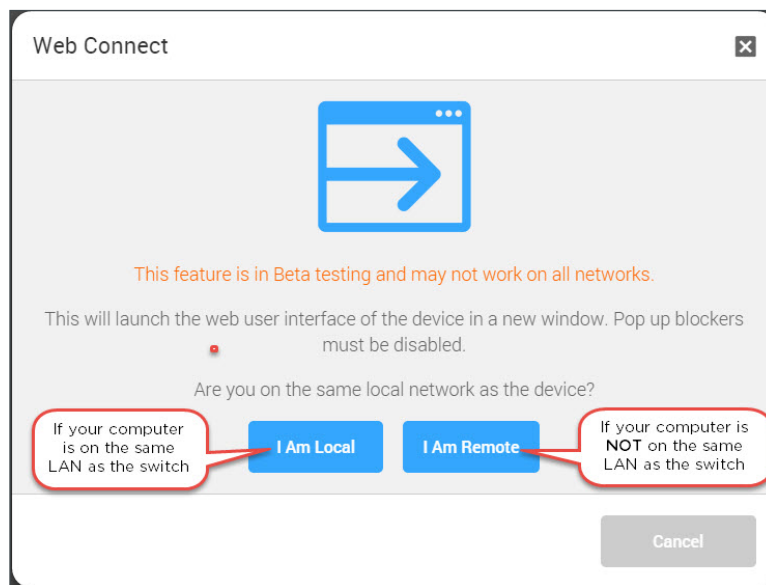
7 - Interface Access

OvrC Web Connect Access

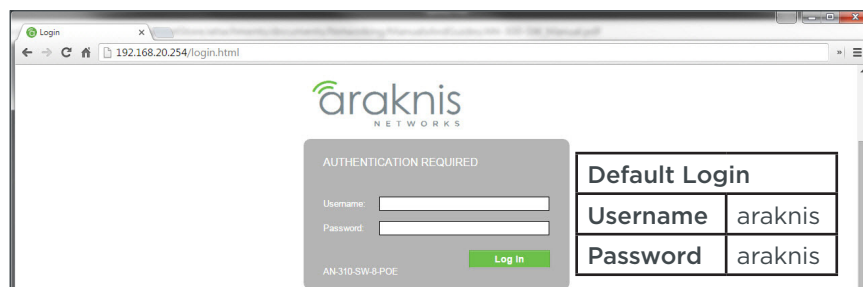
1. Log into the OvrC app and find the switch. The OvrC web interface is easier to use than mobile for Web Connect access. Popup blockers must be disabled.



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**.

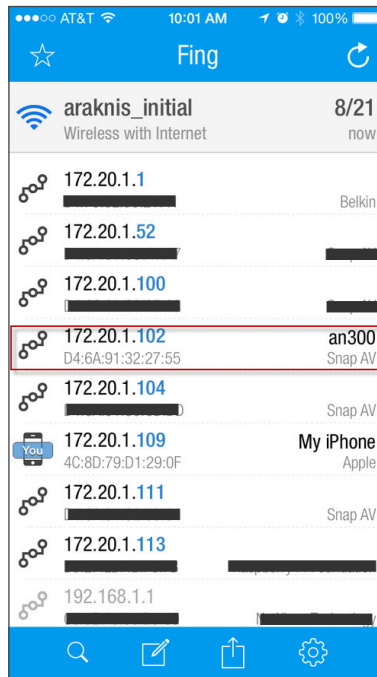


4. If you were able to log in successfully, go to the System Settings menu to begin completing the recommended setup for all users. See section "11 - Recommended Setup - System Settings" on page 26.
5. If this access method does not work for your application, see the next section for instructions to access the interface using a DHCP IP address.

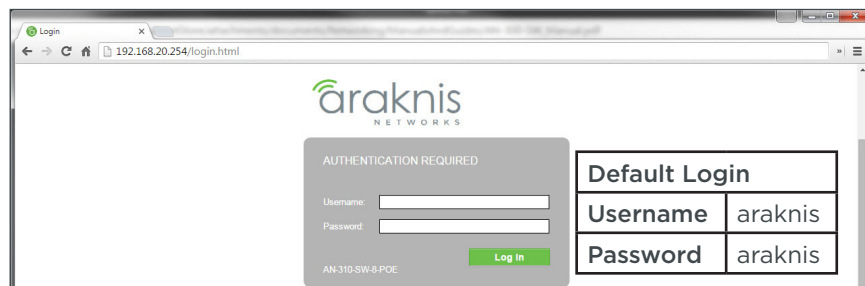


Direct Access Using LAN IP Address (DHCP)

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**.

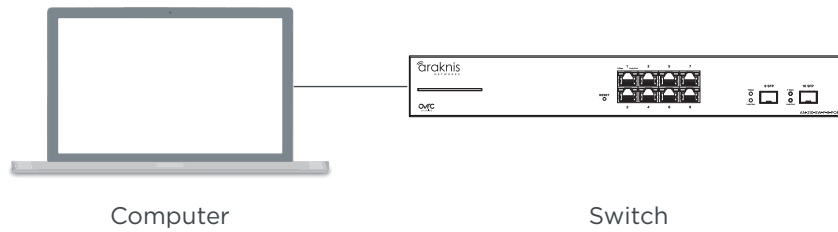


3. If you were able to log in successfully, go to the System Settings menu to begin completing the recommended setup for all users. See section "11 - Recommended Setup – System Settings" on page 26.
4. If this access method does not work for your application, see the next section for instructions to access the interface using the switch's default IP address.

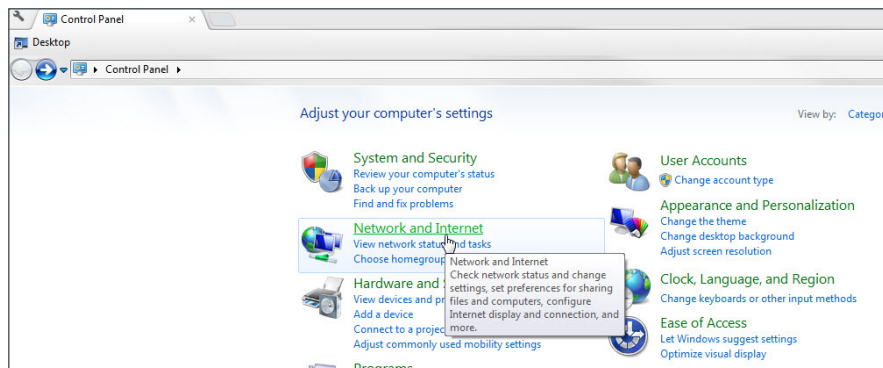
Default IP Address Access

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

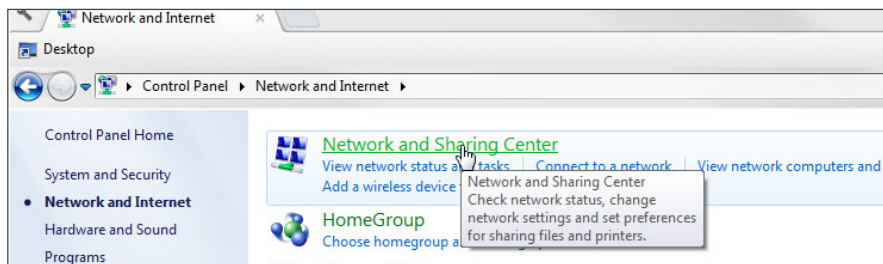
1. Connect your PC to the switch using a network patch cable.



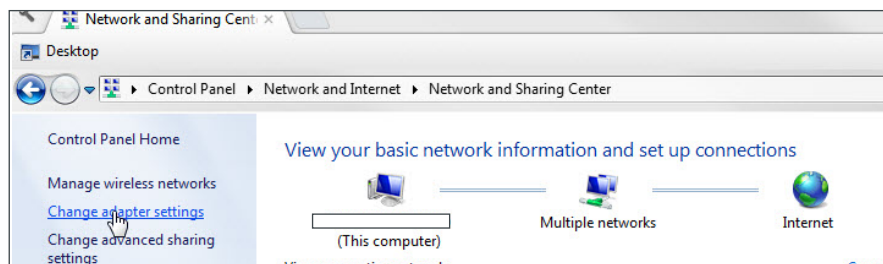
2. On your PC, open the Control Panel and left-click **Network and Internet**.



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

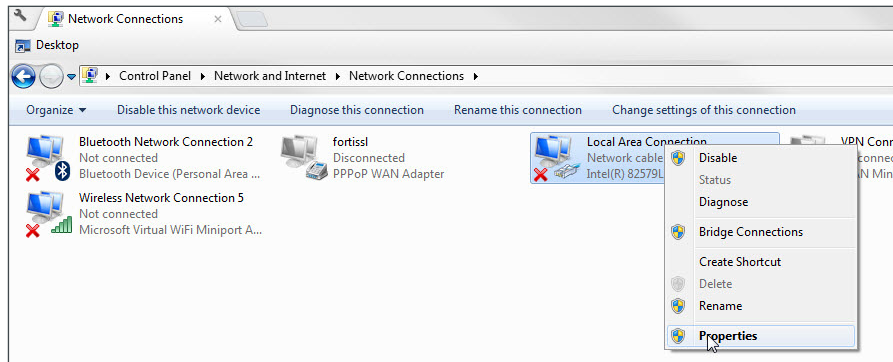


4. In the left bar, left-click **Change adapter settings**.

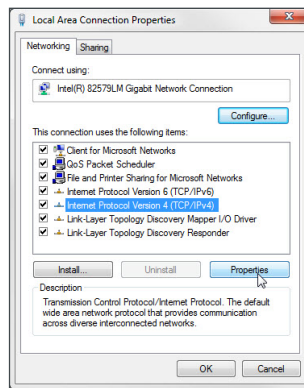




5. Right-click the icon for the wired network connection and left-click **Properties**.

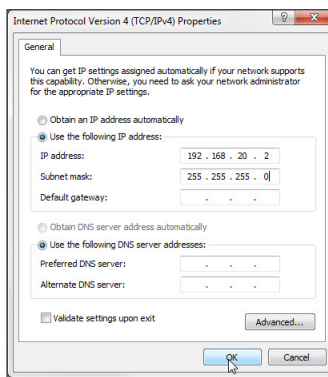


6. Left-click to highlight **Internet Protocol Version 4 (TCP/IPv4)**, then left-click **Properties**.



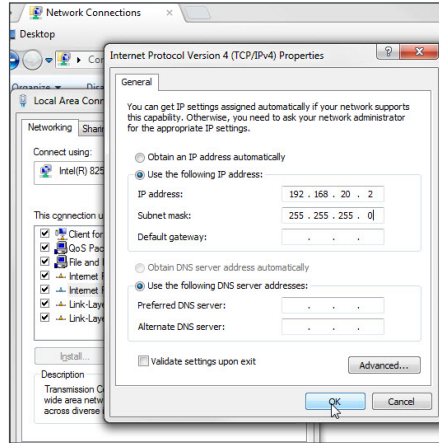
7. In the General tab, left-click **Use the following IP address:** and enter the IP address and subnet mask.

- IP Address: **192.168.20.2**
- Subnet Mask: **255.255.255.0**

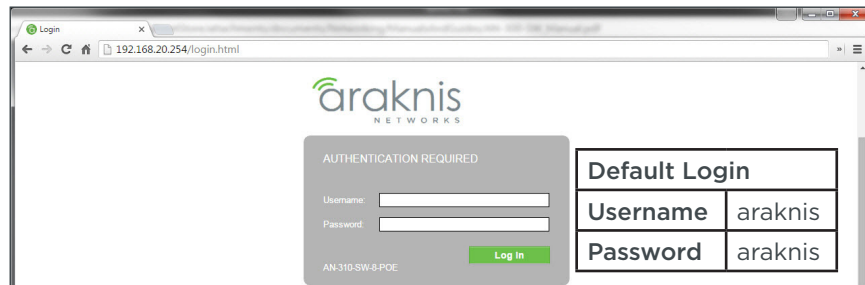




- Left-click **OK** to close **Internet Protocol Version 4 (TCP/IPv4) Properties**, then left-click **OK** to close **Network Connection Properties**.



- 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**.



- 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.

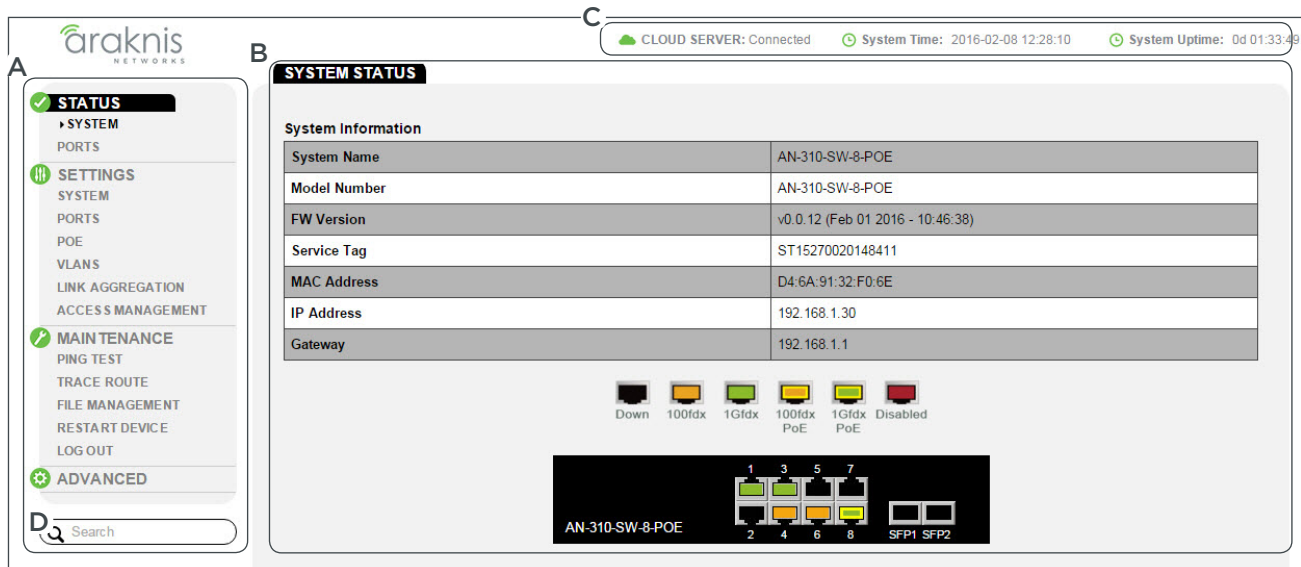


8 - Interface Overview

Page Layout

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

Figure 7. Interface Layout

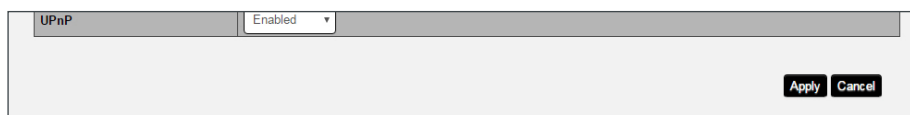


- **A - Main Navigation Menu**
Use the submenus under the Status, Settings, Maintenance, and Advanced headings to configure and maintain the switch.
- **B - Main Window**
The main window displays the currently selected submenu.
- **C - Top Bar**
The top bar displays the current connection status to the 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





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 STATUS

System Information

System Name	AN-310-SW-8-POE
Model Number	AN-310-SW-8-POE
FW Version	v0.0.12 (Feb 01 2016 - 10:46:38)
Service Tag	ST15270020148411
MAC Address	D4:6A:91:32:F0:6E
IP Address	192.168.1.30
Gateway	192.168.1.1

Port Status

Port	Name	Link Speed	Duplex
1	Port 1	1Gbps	Full
2	Port 2	Not Connected	Not Connected

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.



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

Time	Category	Severity	Message
Feb 08 2016 10:53:59	System	warning	System reboot
Feb 08 2016 10:15:48	System	warning	System reboot
Feb 05 2016 13:27:26	System	warning	System reboot

10 1 to 3 of 3 EVENT(s) Previous Next

Export Clear

- **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.

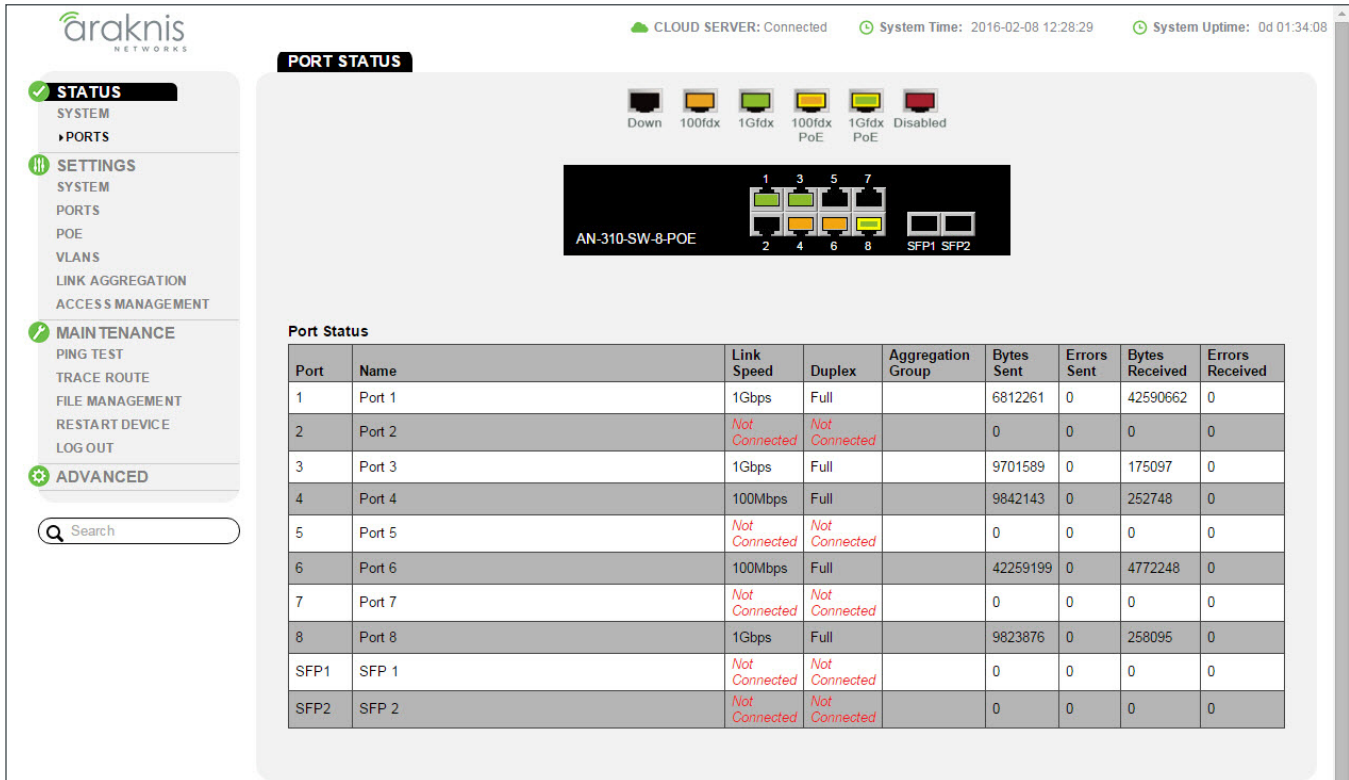


Port Status Page

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

Path – Status, Ports

Figure 11. Port Status



- **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.



10 - System Settings

Configure system level settings.

System Information

Path – Settings, System, System

Figure 12. System Information Settings

System	
System Name	AN-310-SW-8-POE (char : 1 ~ 255)
System Location	Home Rack (char : 0 ~ 255)
Admin Username	admin (char : 1 ~ 18)
Current Admin Password	(char : 4 ~ 32)
New Admin Password	(char : 4 ~ 32)
Confirm New Admin Password	(char : 4 ~ 32)
Management VLAN ID	1
LED	<input checked="" type="radio"/> 1Gbps <input type="radio"/> PoE <input type="radio"/> Disabled

- **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.



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

IP Address Settings		IPv4	
IPv4		IPv6	
Auto Configuration	<input type="radio"/> Static <input checked="" type="radio"/> DHCP	IPv6 State	Auto Configuration
IPv4 Address	192.168.1.30	IPv6 Address	fe80::d66a:91ff:fe32:f06e / 64 (1-127)
Subnet Mask	255.255.255.0	Default Gateway	::
Default Gateway	192.168.1.1	Link Local Address	fe80::d66a:91ff:fe32:f06e
DNS Server 1	192.168.1.1		
DNS Server 2			

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).



Figure 14. Date and Time Settings, UPnP

Date and Time Settings

Manually Set Date and Time

Date: 2016 / 2 / 08

Time: 12 : 28 (24-Hour)

Synchronize with PC

Automatically Get Date and Time

NTP Server: time.nist.gov

Time Zone: (GMT-05:00) Eastern Time (US and Canada)

Enable Daylight Saving

Start: March 2nd Sun 02 : 00

End: November 1st Sun 02 : 00

UPnP Configuration

UPnP: Enabled

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 Connect or OvrC web monitoring. Contact technical support if you need to disable OvrC functionality.



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

Default Setting	
Username	araknis
Password	araknis

The screenshot shows the 'System' configuration page. The 'System' section includes fields for System Name, System Location, Admin Username, Current Admin Password, New Admin Password, Confirm New Admin Password, and Management VLAN ID. The 'IP Address Settings' section has tabs for IPv4 and IPv6. The IPv4 section includes options for Auto Configuration (Static/DHCP), IP Address, Subnet Mask, Default Gateway, DNS Server 1, and DNS Server 2. The IPv6 section includes options for IPv6 State, IPv6 Address, Default Gateway, and Link Local Address. The 'Date and Time Settings' section includes options for Manually Set Date and Time, Synchronize with PC, Automatically Get Date and Time, NTP Server, Time Zone, and Enable Daylight Saving. The 'UPnP Configuration' section includes an option for UPnP.

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.



12 - Port Configuration Settings

Customize individual port settings and jumbo frame size.

Path - Settings, Ports

Figure 16. Jumbo Frame and Basic Port Settings

The screenshot shows a web interface for configuring network settings. On the left is a navigation menu with categories: SYSTEM, PORTS, SETTINGS (highlighted), MAINTENANCE, and ADVANCED. A search bar is located below the menu. The main content area is divided into two sections:

- Jumbo Frame:** A single row with a 'Size' field containing '9216' and a label 'Bytes (1522-9216)'.
- Basic Port Settings:** A table with columns 'Port', 'Name', 'Speed', and 'Duplex'. It lists settings for ports 1 through 8, SFP1 through SFP2, and LAG1 through LAG8.

Port	Name	Speed	Duplex
1	Port 1	Auto	Auto
2	Port 2	Auto	Auto
3	Port 3	Auto	Auto
4	Port 4	Auto	Auto
5	Port 5	Auto	Auto
6	Port 6	Auto	Auto
7	Port 7	Auto	Auto
8	Port 8	Auto	Auto
SFP1	SFP 1	Auto	Full
SFP2	SFP 2	Auto	Full
LAG1	LAG 1	Auto	Auto
LAG2	LAG 2	Auto	Auto
LAG3	LAG 3	Auto	Auto
LAG4	LAG 4	Auto	Auto
LAG5	LAG 5	Auto	Auto
LAG6	LAG 6	Auto	Auto
LAG7	LAG 7	Auto	Auto
LAG8	LAG 8	Auto	Auto

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



Advanced Port Settings

Path - Settings, Ports, Advanced Port Settings

Figure 17. Advanced Port Settings

Advanced Port Settings			
Port	Link Status	Flow Control	EEE Status
1	Link Up	Disabled	Disabled
2	Link Down	Disabled	Disabled
3	Link Up	Disabled	Disabled
4	Link Up	Disabled	Disabled
5	Link Down	Disabled	Disabled
6	Link Up	Disabled	Disabled
7	Link Down	Disabled	Disabled
8	Link Up	Disabled	Disabled
SFP1	Link Down	Disabled	
SFP2	Link Down	Disabled	
LAG1	Link Down	Disabled	
LAG2	Link Down	Disabled	
LAG3	Link Down	Disabled	
LAG4	Link Down	Disabled	
LAG5	Link Down	Disabled	
LAG6	Link Down	Disabled	
LAG7	Link Down	Disabled	
LAG8	Link Down	Disabled	

Apply **Cancel**

- **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.



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	Port	Power Limit Type	Priority	Status	Class	Output Voltage (V)	Output Current (mA)	Output Power (W)	Power Cycle
<input checked="" type="checkbox"/>	1	Auto	Low	Delivering	4	54.7	72	3.9	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Auto	Low	Detecting.....					<input type="checkbox"/>
<input checked="" type="checkbox"/>	3	Auto	Low	Detecting.....					<input type="checkbox"/>
<input checked="" type="checkbox"/>	4	Auto	Low	Detecting.....					<input type="checkbox"/>
<input checked="" type="checkbox"/>	5	Auto	Low	Detecting.....					<input type="checkbox"/>
<input checked="" type="checkbox"/>	6	Auto	Low	Detecting.....					<input type="checkbox"/>
<input checked="" type="checkbox"/>	7	Auto	Low	Detecting.....					<input type="checkbox"/>
<input checked="" type="checkbox"/>	8	Auto	Low	Detecting.....					<input type="checkbox"/>

- **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.



PoE Setup and Troubleshooting

Figure 19. PoE Settings Menu

Enable	Port	Power Limit Type	Priority	Status	Class	Output Voltage (V)	Output Current (mA)	Output Power (W)	Power Cycle
<input checked="" type="checkbox"/>	1	Auto	Low	Delivering	4	54.7	72	3.9	<input type="checkbox"/>
<input checked="" type="checkbox"/>	2	Auto	Low	Detecting.....					<input type="checkbox"/>

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

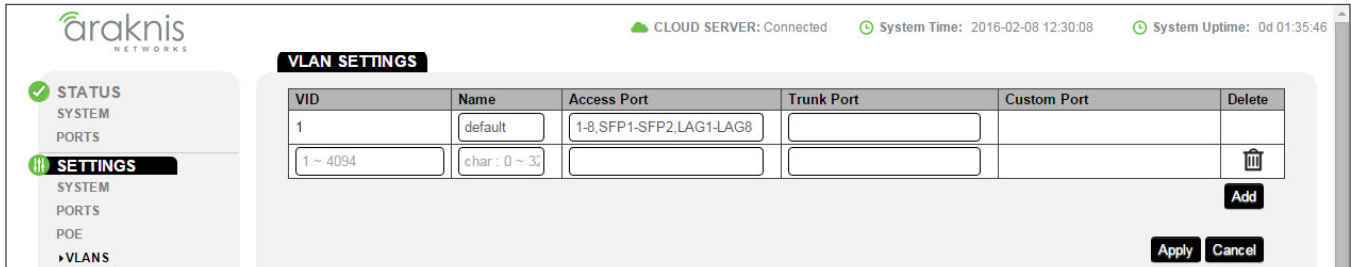
- **Power Cycle** – Check the box and click **Apply** to power cycle PoE on one or more ports.
- **Overcurrent Condition** – With default PoE settings, if the current drawn from PoE devices exceeds the total budget for the switch, PoE will be disabled on ports beginning with the highest numbered port.



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.

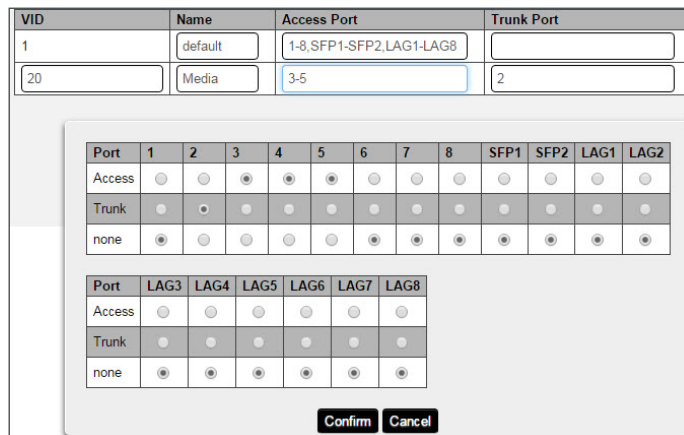
Figure 20. VLAN Settings



- **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.



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

VID	Name	Access Port	Trunk Port
1	default	1-8,SFP1-SFP2,LAG1-LAG8	
20	Media	3-5	2

Port	1	2	3	4	5	6	7	8	SFP1	SFP2	LAG1	LAG2
Access	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
none	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Port	LAG3	LAG4	LAG5	LAG6	LAG7	LAG8
Access	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trunk	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
none	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>

Confirm **Cancel**

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.

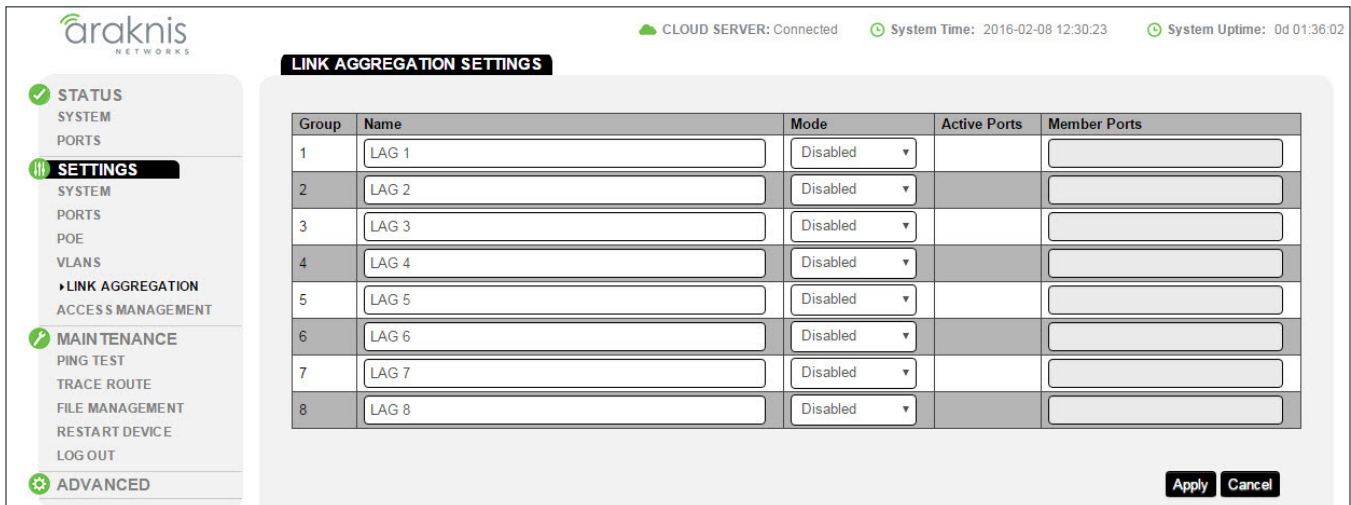


15 - Link Aggregation Settings

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.



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.

Group	Name	Mode	Active Ports	Member Ports
1	LAG 1	LACP		SFP1-SFP2
2	LAG 2	Disabled		
3	LAG 3	Disabled		
4	LAG 4	Disabled		
5	LAG 5	Disabled		
6	LAG 6	Disabled		
7	LAG			
8	LAG			

Port	1	2	3	4	5	6	7	8	SFP1	SFP2
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Confirm Cancel

Apply Cancel

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



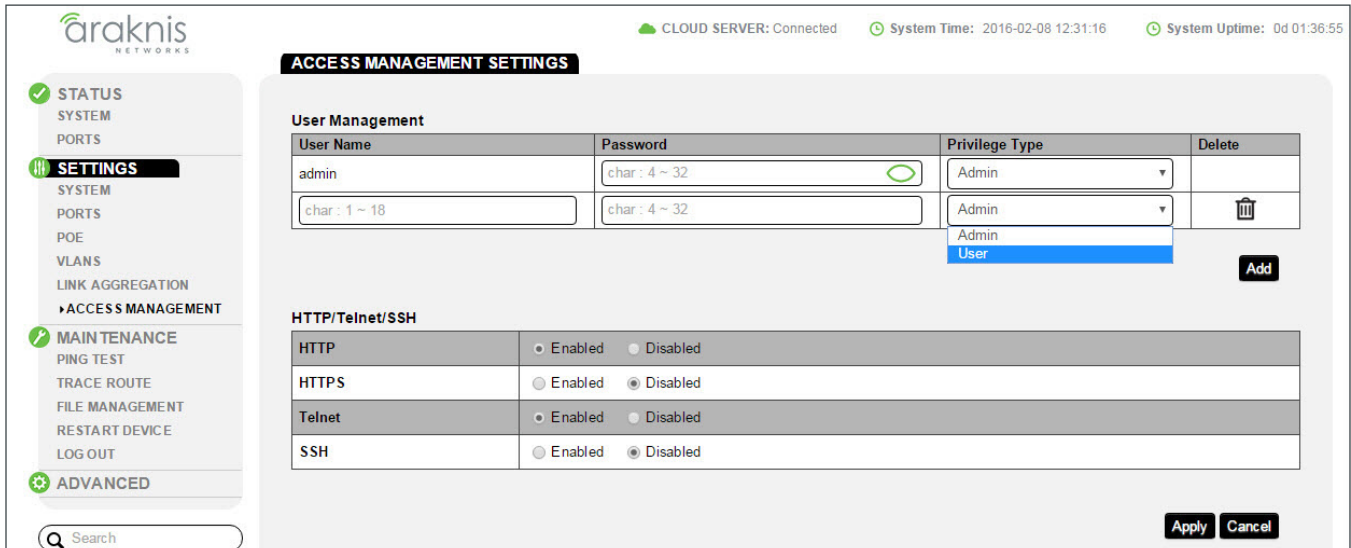
Note - LACP must be configured in equipment on both sides of the link to operate correctly.



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



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

The screenshot displays the Araknis Networks web interface for the Ping Test function. The sidebar on the left contains navigation options: STATUS (SYSTEM, PORTS), SETTINGS (SYSTEM, PORTS, POE, VLANS, LINK AGGREGATION, ACCESS MANAGEMENT), MAINTENANCE (PING TEST, TRACE ROUTE, FILE MANAGEMENT, RESTART DEVICE, LOG OUT), and ADVANCED. The main content area is titled "PING TEST" and features a form with the following fields: IP Address (192.168.1.100), Count (4), Interval (in sec) (1), and Size (in bytes) (56). A "Result:" label is followed by a large empty text area. A "Test" button is located at the bottom right of the form. The top of the page shows system status: CLOUD SERVER: Connected, System Time: 2016-02-08 12:31:35, and System Uptime: 0d 01:37:14.

- **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.



Understanding Ping Test Results

Figure 26. Successful Ping Test Result

The screenshot shows a web form for a ping test. The IP address field is set to 192.168.1.80. The count is 4, interval is 1 second, and size is 56 bytes. The result box shows four successful ping responses, each with 64 bytes and 0.0 ms round-trip time. The statistics show 4 packets transmitted, 4 received, 0% loss, and 0.0/0.0/0.0 ms round-trip times.

```
IP Address: 192.168.1.80 (x.x.x.x or hostname)
Count: 4 ( 1 - 5 | Default : 4 )
Interval (in sec): 1 ( 1 - 5 | Default : 1 )
Size (in bytes): 56 ( 8 - 5120 | Default : 56 )

Result:
PING 192.168.1.80 (192.168.1.80): 56 data bytes
64 bytes from 192.168.1.80: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.1.80: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.1.80: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.1.80: icmp_seq=3 ttl=64 time=0.0 ms

--- 192.168.1.80 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Figure 27. Failed Ping Test Result

The screenshot shows a web form for a ping test. The IP address field is set to 192.168.1.100. The count is 4, interval is 1 second, and size is 56 bytes. The result box shows a failed ping test with 0 packets received and 100% packet loss.

```
IP Address: 192.168.1.100 (x.x.x.x or hostname)
Count: 4 ( 1 - 5 | Default : 4 )
Interval (in sec): 1 ( 1 - 5 | Default : 1 )
Size (in bytes): 56 ( 8 - 5120 | Default : 56 )

Result:
PING 192.168.1.100 (192.168.1.100): 56 data bytes

--- 192.168.1.100 ping statistics ---
4 packets transmitted, 0 packets received, 100% packet loss
```

- 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

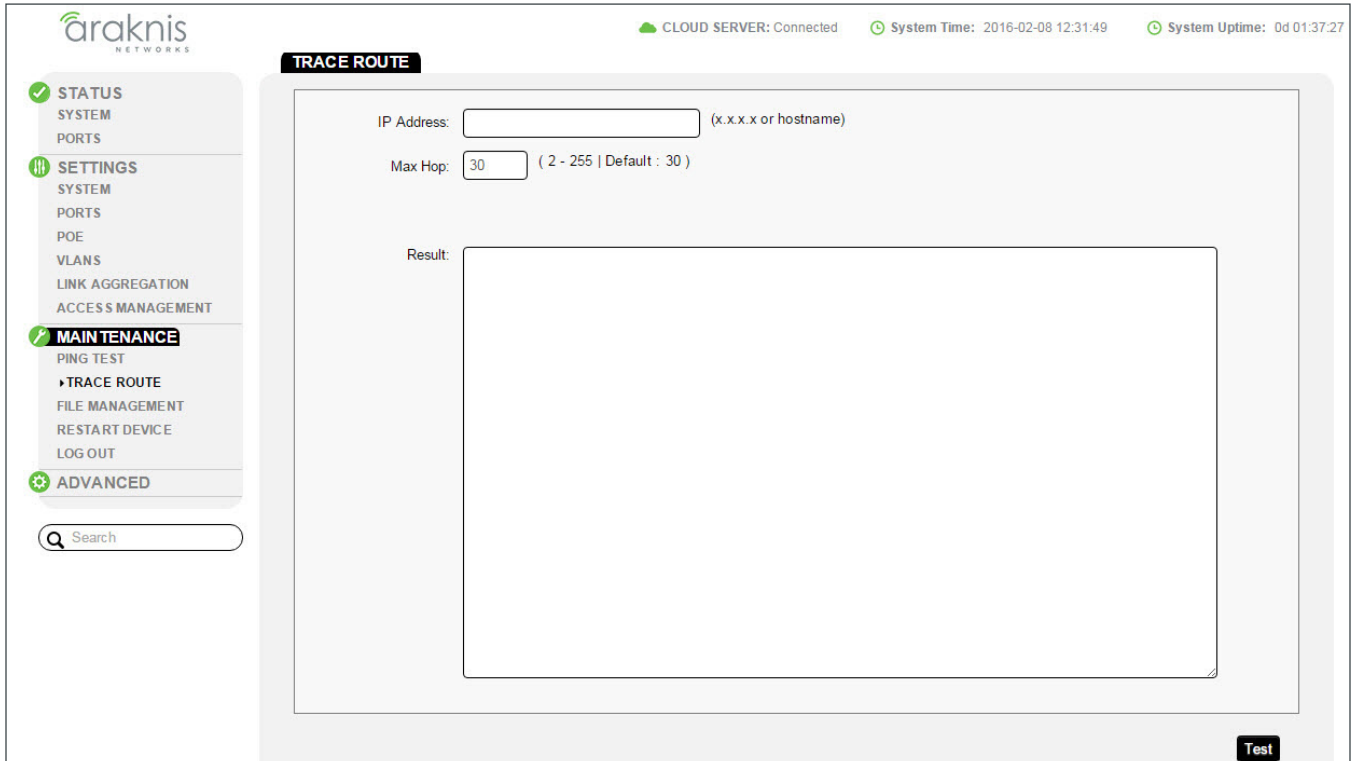
- If no packets are received, check the connections between the switch and the target device first. The target device may not be connected. If the connection is good, reset or power cycle the target device. It may have become unresponsive.
- If packets are still not received, check for a bad cable, port, 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.



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.



Understanding Trace Route Test Results

Figure 29. Trace Route Result

TRACE ROUTE

IP Address: (x.x.x.x or hostname)

Max Hop: (2 - 255 | Default : 30)

Result: `tracert to 8.8.8.8 (8.8.8.8), 30 hops max, 40 byte packets`

```
1 192.168.1.1 (192.168.1.1) 48 bytes to 192.168.1.30 0 ms 0 ms 0 ms
2 10.21.128.1 (10.21.128.1) 36 bytes to 192.168.1.30 10 ms
36 bytes from 92.168.1.30 to 192.168.1.30: icmp type 3 (Dest Unreachable) code 1
20 ms
36 bytes from 92.168.1.30 to 192.168.1.30: icmp type 3 (Dest Unreachable) code 1
10 ms
3
36 bytes from 92.168.1.30 to 192.168.1.30: icmp type 3 (Dest Unreachable) code 1
208.104.0.117 (208.104.0.117) 36 bytes to 192.168.1.30 10 ms 10 ms 10 ms
4 208.104.1.45 (208.104.1.45) 36 bytes to 192.168.1.30 10 ms 10 ms 10 ms
5 208.104.1.101 (208.104.1.101) 36 bytes to 192.168.1.30 20 ms 20 ms 20 ms
6 208.104.0.9 (208.104.0.9) 36 bytes to 192.168.1.30 20 ms 20 ms 10 ms
7 165.166.78.61 (165.166.78.61) 48 bytes to 192.168.1.30 30 ms 20 ms 10 ms
8 72.14.215.218 (72.14.215.218) 36 bytes to 192.168.1.30 20 ms 20 ms 10 ms
9 209.85.243.51 (209.85.243.51) 36 bytes to 192.168.1.30 20 ms 10 ms 20 ms
10 216.239.51.245 (216.239.51.245) 148 bytes to 192.168.1.30 30 ms 209.85.142.140 (209.85.142.140) 148 bytes to
192.168.1.30 10 ms 216.239.51.243 (216.239.51.243) 148 bytes to 192.168.1.30 20 ms
11 209.85.143.197 (209.85.143.197) 36 bytes to 192.168.1.30 20 ms 209.85.243.254 (209.85.243.254) 36 bytes to
192.168.1.30 10 ms 209.85.143.201 (209.85.143.201) 36 bytes to 192.168.1.30 20 ms
12 ***
13 8.8.8.8 (8.8.8.8) 36 bytes to 192.168.1.30 10 ms 30 ms 20 ms
```

Test

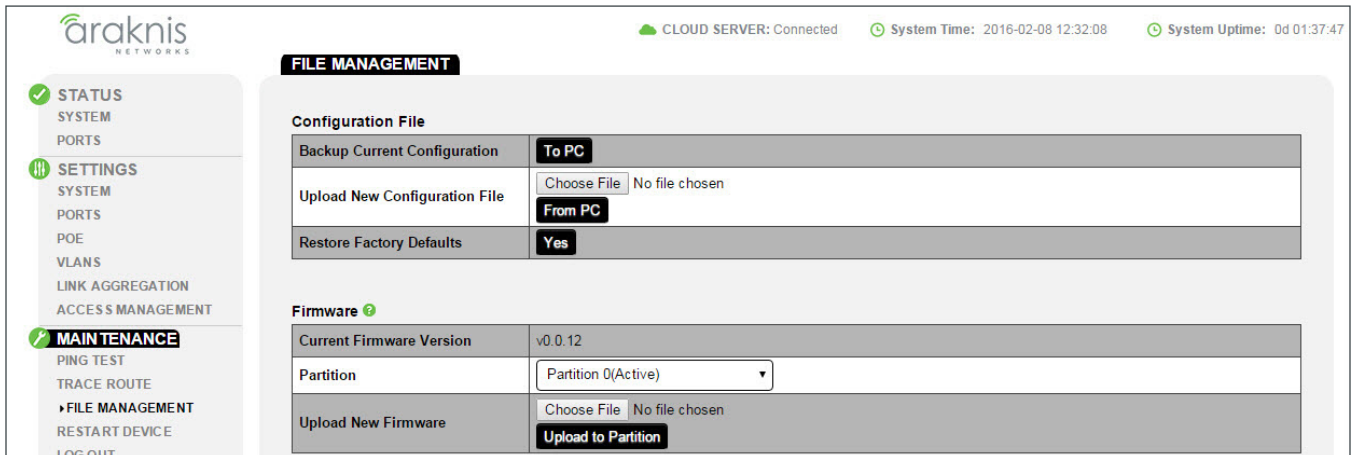
- The results window displays the parameters for the test, followed by information about each hop or hop attempt.
- Each line starting with a number indicates a hop in the path to the target IP address. Only hops between routers are shown, not between switches.
- Each hop is tested three times. In each 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.



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

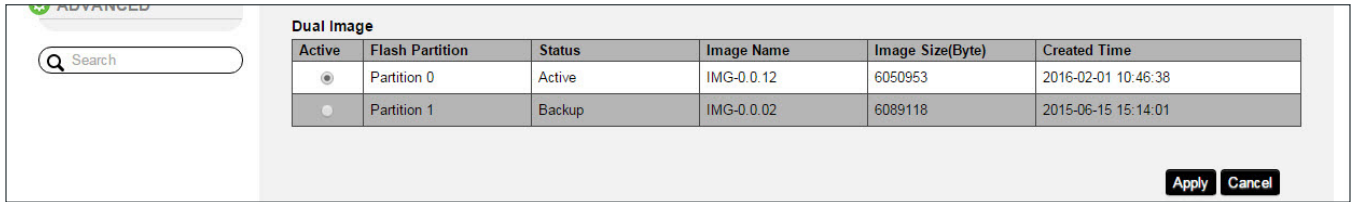
- **Current Firmware Version** – Indicates the current firmware version on the selected partition.
- **Partition** – Select the partition to change firmware for:
 - **Partition 0** – Default partition.
 - **Partition 1** – Backup partition. (In the event of one partition failing, the switch will reboot 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.



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.

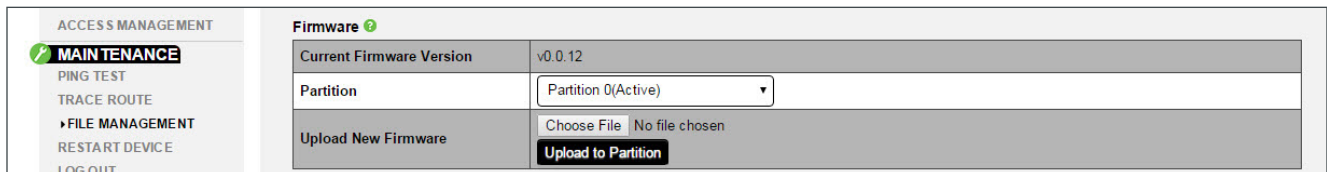
Figure 31. Dual Image Menu



- **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 known location on your computer.
2. Navigate to the Maintenance > File Management > Firmware menu.

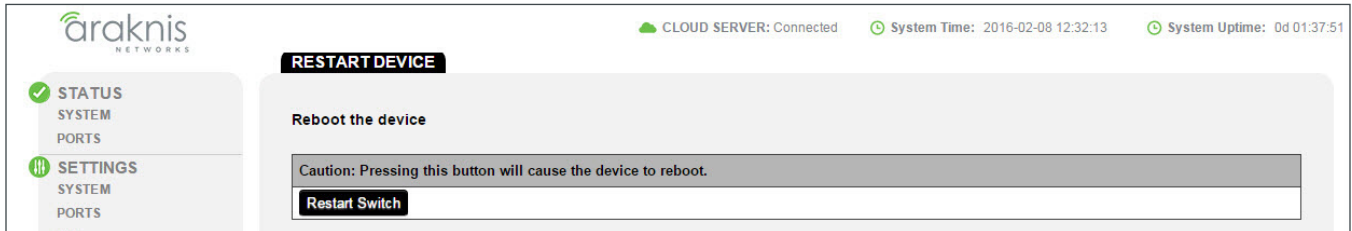


3. Click the **Choose File** button for Upload New Firmware, then find and select the new firmware and click **Open**.
4. Click Upload to Partition then follow the prompts to complete the update for the first partition.
5. After the first partition is updated, repeat the process, but before clicking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



Restart

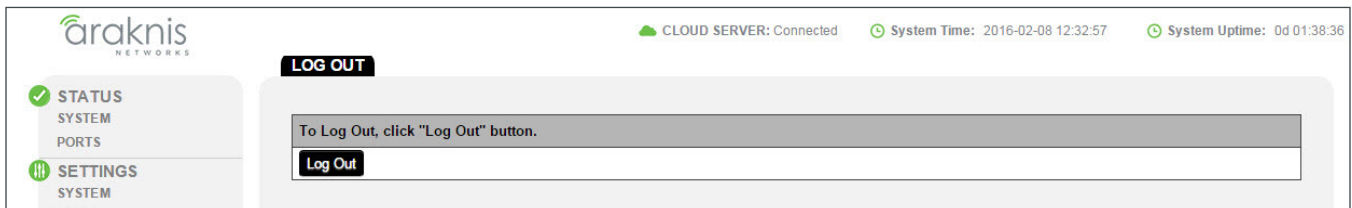
Figure 32. Restart Page



- **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.



18 - Advanced Menus

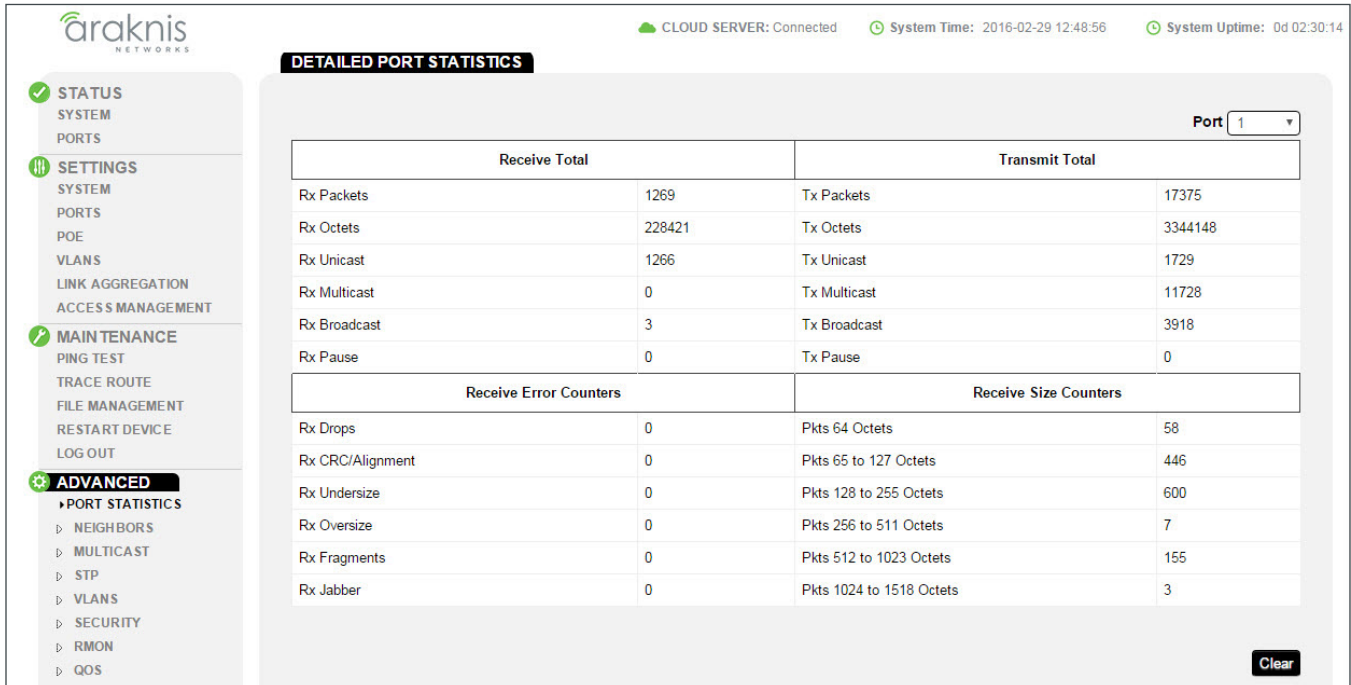
The remaining menus are meant only for advanced users. Proper setup and use of these features requires advanced networking knowledge.



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



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.



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

MAC ADDRESS TABLE

Static MAC Address

Index	Port	VID	MAC Address	Delete
1	1	1	XX:XX:XX:XX:XX:XX	

Add

Dynamic MAC Address

Index	Port	VID	MAC Address
1	4	1	00:03:EA:0A:A4:10
2	7	1	34:02:86:BB:32:FD
3	7	1	34:E6:D7:76:6A:62
4	7	1	6C:40:08:58:D8:EA
5	7	1	74:D0:2B:5D:C6:C0
6	7	1	80:D2:1D:13:12:B6
7	7	1	B0:83:FE:7F:3C:82
8	7	1	B0:E8:92:0D:41:6F
9	6	1	B8:27:EB:FA:7E:97
10	3	1	D4:6A:91:12:1E:6A
11	7	1	D4:6A:91:31:10:95
12	7	1	D4:6A:91:31:10:96
13	1	1	D4:6A:91:32:3B:56
14	7	1	D4:6A:91:32:EC:6A

Apply Cancel

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.



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

Information	
Chassis ID Subtype	MAC Address
Chassis ID	D4:6A:91:32:F0:6E
System Name	AN-310-SW-8-POE
System Description	Araknis 310 8 Port PoE
Capabilities Supported	Bridge
Capabilities Enabled	Bridge
Port ID Subtype	Local

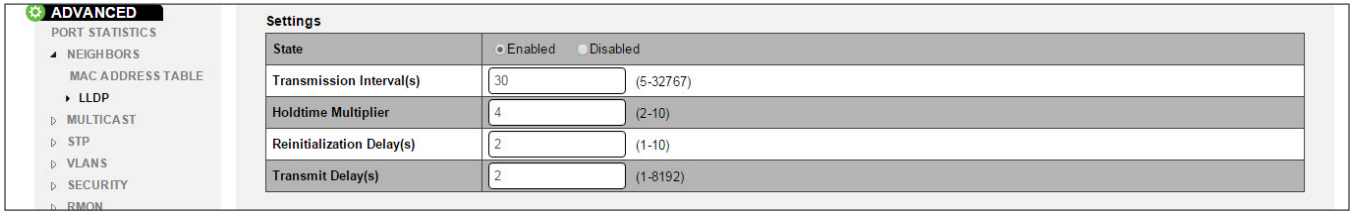
- **Chassis ID Subtype** - Method used for device identification.
- **Chassis ID** - MAC Address of the switch.
- **System Name** - System name of the switch (configured in the System Settings menu).
- **System Description** - System make and model.
- **Capabilities Supported** - Displays the capabilities 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**.



Settings

Customize settings for LLDP transmission.

Figure 37. LLDP Settings

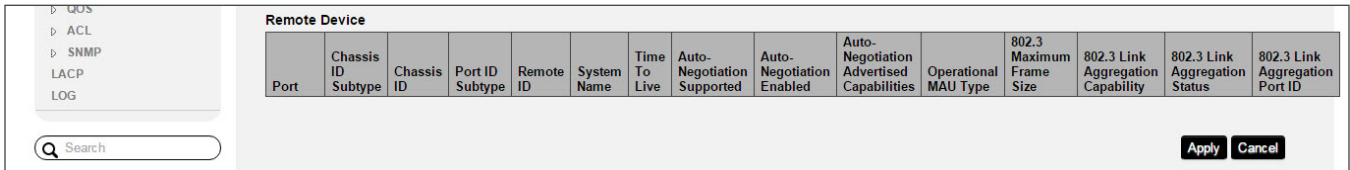


- **State**- Select whether LLDP is enabled or disabled.
- **Transmission Interval(s)** - How often LLDP information is transmitted. Range: 5-32767 seconds.
Default: 30 seconds
- **Holdtime Multiplier** - Multiplied by the transmission interval value to generate the TTL time transmitted to neighbors. 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.



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

Settings	
Status	<input type="radio"/> Enabled <input type="radio"/> Disabled
Version	<input checked="" type="radio"/> V2 <input type="radio"/> V3
Report Suppression	<input type="radio"/> Enabled <input type="radio"/> Disabled

- **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 Settings		
VLAN ID	IGMP Snooping Status	Fast Leave
1	Disabled	Disabled

- **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.



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	Querier State	Querier Version	Querier Status	Querier IP	Robustness	Interval	Oper Interval	Max Response Interval	Oper Max Response Interval	Last Member Query Counter	Oper Last Member Query Counter	Last Member Query Interval	Oper Last Member Query Interval
1	Disal ▾	v2 ▾	Non-Querier	---	2	125	125	10	10	2	2	1	1

- **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.



Group List

See current group subscriptions by VLAN.

Figure 42. IGMP Snooping Group List Settings

MLD SNOOPING	Group List		
▶ STP	VLAN ID	Group IP Address	Member Ports
GLOBAL 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

MST SETTINGS	Router Settings			
▶ VLANS	VLAN ID	Router Ports Auto-Learned	Dynamic Port List	Static Port List
▶ SECURITY	1	Enabled ▼		
▶ RMON				Forbidden Port List

- **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

▶ ACL	URC Settings		
▶ SNMP	URC State	Member Ports	VLAN
LACP	Disabled ▼	1	1 ▼
LOG			

- **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.



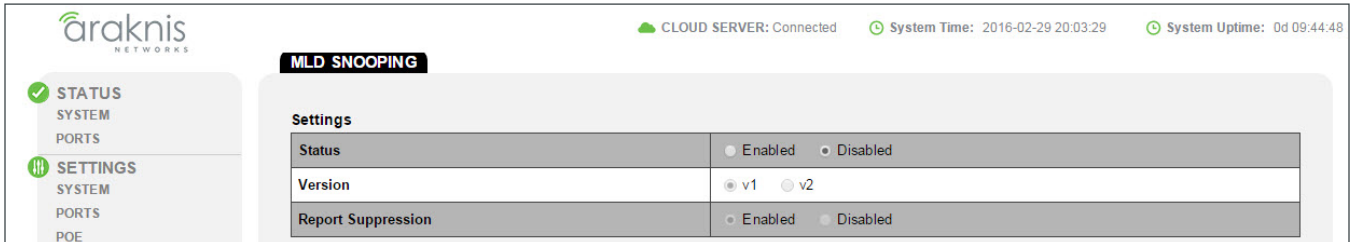
23 - Multicast - MLD Snooping

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

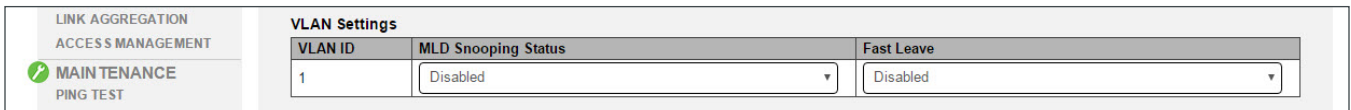


- **Status** – Enable or disable IGMP Snooping. When enabled, the switch monitors network traffic passing through it to determine which connected clients want to receive multicast traffic.
Default: Disabled
- **Version** – Select MLDv1 or v2.
- **Report Repression** – Enable to prevent the router from 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.



Router Settings

Configure MLD router ports on the switch.

Figure 48. MLD Snooping Router Settings

Router Settings				
VLAN ID	Router Ports Auto-Learned	Dynamic Port List	Static Port List	Forbidden Port List
1	Enabled			

- **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.



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	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Force Version	MSTP
Configuration Name	D4:6A:91:32:F0:6E (char : 0 - 32)
Configuration Revision	0 (0-65535)

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.



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

VLANS LINK AGGREGATION ACCESS MANAGEMENT MAINTENANCE PING TEST TRACE ROUTE FILE MANAGEMENT RESTART DEVICE LOG OUT ADVANCED PORT STATISTICS	Root Bridge Information	
	Root Address	74:D0:2B:5D:C6:C0
	Priority	32768
	Cost	20000
	Port	7
	Forward Delay	0 (sec)
	Maximum Age	20 (sec)
	Hello Time	2 (sec)

- **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.



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

▷ MULTICAST	Basic Setting
▲ STP	Bridge Address D4:6A:91:32:F0:6E
▷ GLOBAL SETTINGS	Priority 32768 (4096*N)
CIST SETTINGS	Maximum Hop 20 (1-40)
MST SETTINGS	Forward Delay 15 (4-30)
▷ VLANS	Maximum Age 20 (6-40)
▷ SECURITY	TX Hold Count 6 (1-10)
▷ RMON	Hello Time 2 (1-10)
▷ QOS	
▷ ACL	
▷ SNMP	

- **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



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	Priority	Path Cost Conf / Oper	Designated Root Bridge	External Root Cost	Regional Root Bridge	Internal Root Cost	Designated Bridge	Edge Port Conf / Oper	P2P MAC Conf / Oper	Port Role	Port State	Migration Start
1	128	0 / 20000	32768 / 0 / 74.D0.2B.5D.C6.C0	20000	32768 / 0 / D4.6A.91.32.F0.6E	0	32768 / 0 / D4.6A.91.32.F0.6E	Yes / Yes	Auto / Yes	Designated	Forwarding	<input type="checkbox"/>
2	128	0	0 / 0 /	0	0 / 0 /	0	0 / 0 /	Yes	Auto	Disabled	Disabled	<input type="checkbox"/>

- **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



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.



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	VLAN List	Priority	Regional Root Bridge	Internal Root Cost	Designated Bridge	Root Port
1	1-4094	32768	--	0	--	--
2	1-4094	32768	--	0	--	--
3	1-4094	32768	--	0	--	--
4	1-4094	32768	--	0	--	--

- **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.



Port Settings

Configure MSTP settings for each port.

Figure 54. STP MST Port Settings Menu

MST ID	Port	Priority	Internal Path Cost Conf / Oper	Regional Root Bridge	Internal Root Cost	Designated Bridge	Port Role	Port State
1	1	128	0 /20000	--	--	--	--	--
1	2	128	0 /20000	--	--	--	--	--
1	3	128	0 /20000	--	--	--	--	--
1	4	128	0 /200000	--	--	--	--	--
1	5	128	0 /200000	--	--	--	--	--

- **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.



26 - Advanced VLANs - Overview

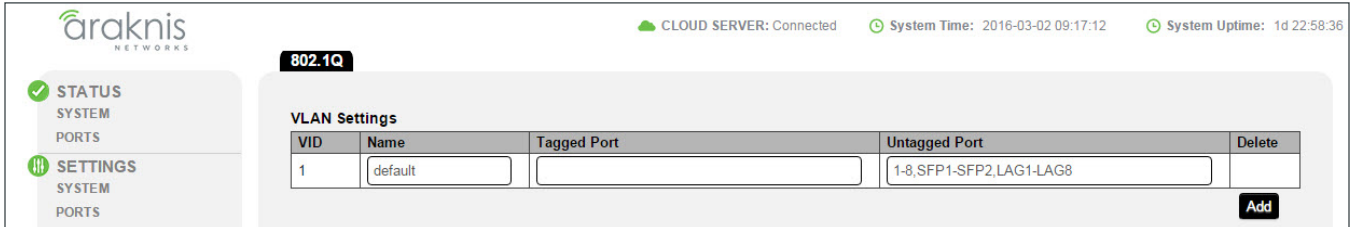
The advanced VLAN pages contain settings for customizing VLANs beyond basic port-based settings.

Advanced VLANs - 802.1Q VLANs

VLAN Settings

Manually configure VLAN tagging for each port.

Figure 55. 802.1Q VLAN Settings Menu

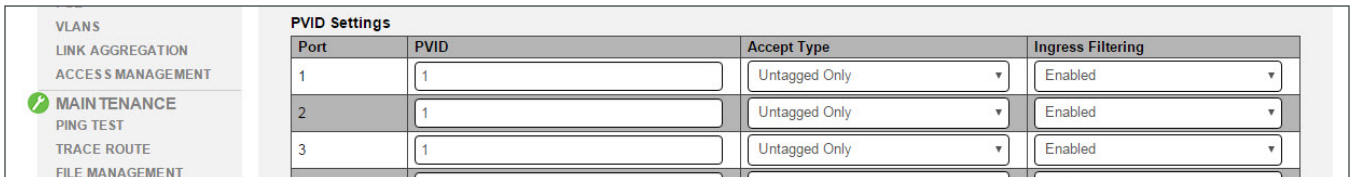


- **VID** - VLAN ID.
- **Name** - Use this field to enter a custom VLAN name for easy identification.
- **Tagged Port** - Tagged ports and LAGs for the VLAN. Click the field to configure.
- **Untagged Port** - Untagged ports and LAGs for the VLAN. Click the field to configure.
Default: All ports untagged
- **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.

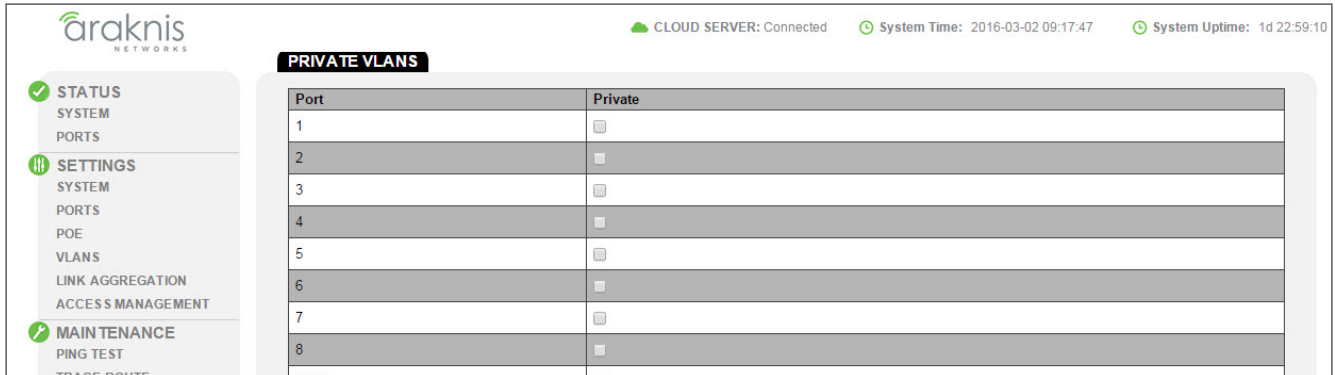


Advanced VLANs – Private VLANs

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



Advanced VLANs – Voice VLANs

Configure 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 VLANS	
Settings	
Voice VLAN State	<input type="radio"/> Enabled <input checked="" type="radio"/> Disabled
Voice VLAN ID	None
802.1p Remark	Disabled
Remark CoS/802.1p	6
Aging Time	1440 (30-65535)min

- **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



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	OUI Address	Description	Delete
1	00:E0:BB	3COM	
2	00:03:6B	Cisco	
3	00:E0:75	Veritel	
4	00:D0:1E	Pingtel	
5	00:01:E3	Siemens	
6	00:60:B9	NEC/Philips	
7	00:0F:E2	H3C	
8	00:09:6E	Avaya	

- **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	State	CoS Mode	Operate Status
1	Disabled	Src	--
2	Disabled	Src	--
3	Disabled	Src	--

- **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.



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	Enable	Destination Port	Source TX Port	Source RX Port	Ingress State
1	<input type="checkbox"/>	1			Disabled
2	<input type="checkbox"/>	1			Disabled
3	<input type="checkbox"/>	1			Disabled
4	<input type="checkbox"/>	1			Disabled

- **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

802.1x Global Setting	
State	<input type="radio"/> Enabled <input type="radio"/> Disabled
Guest VLAN	Disabled
Guest VLAN ID	None

- **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.



Port Settings

Configure 802.1x settings for each switch port.

Figure 63. 802.1x Port Settings Menu

ACCESS MANAGEMENT		Port Settings								
MAINTENANCE		Port	Mode	Reauthentication	Reauthentication period	Quiet Period	Supplicant Period	Max Retry	Authorized Status	Guest VLAN
PING TEST		1	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled
TRACE ROUTE		2	Disabled	Enabled	3600	60	30	2	AUTH_INITIALIZE	Enabled
FILE MANAGEMENT										

- **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:



Authenticated Host

See currently connected authenticated hosts connected using 802.1x.

Figure 64. 802.1x Authenticated Host Table

MAC ADDRESS FILTER		Authenticated Host				
		User Name	Port	Session Time	Authenticate Method	MAC Address

- **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.



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	Server IP	Authorized Port	Key String	Timeout Reply	Retry	Server Priority	Dead Timeout	Delete
	x.x.x.x	1812	char: 0-6	3	3	1	0	

Buttons: Add, Apply, Cancel

- **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.



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

Global Settings	
DMAC = SMAC	Enabled
Land	Enabled
UDP Blat	Enabled
TCP Blat	Enabled
POD	Enabled
IPv6 Min Fragment	Enabled
Bytes	1240 (0-65535)
ICMP Fragments	Enabled
IPv4 Ping Max Size	Enabled
IPv6 Ping Max Size	Enabled
Ping Max Size Setting	512 Bytes (0-65535)
Smurf Attack	Enabled
Netmask Length	0 (0-32)
TCP Min Hdr Size	Enabled
TCP Min Hdr Bytes	20 (0-31)
TCP-SYN(SPORT<1024)	Enabled
Null Scan Attack	Enabled
X-Mas Scan Attack	Enabled
TCP SYN-FIN Attack	Enabled
TCP SYN-RST Attack	Enabled
TCP Fragment (Offset = 1)	Enabled

- **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



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 Settings	
Port	DoS Protection
1	No

- **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.



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

The screenshot shows the Araknis Networks web interface. At the top, it displays 'arakanis NETWORKS' and system status: 'CLOUD SERVER: Connected', 'System Time: 2016-03-02 09:21:26', and 'System Uptime: 1d 23:02:50'. On the left, a navigation menu includes 'STATUS SYSTEM PORTS' and 'SETTINGS SYSTEM PORTS POE VLANS LINK AGGREGATION'. The main content area is titled 'PORT SECURITY' and contains a table with the following data:

Port	State	Max MAC Address
1	Disabled	256
2	Disabled	256
3	Disabled	256
4	Disabled	256
5	Disabled	256

- **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

The screenshot shows the Araknis Networks web interface. At the top, it displays 'arakanis NETWORKS' and system status: 'CLOUD SERVER: Connected', 'System Time: 2016-03-02 09:21:59', and 'System Uptime: 1d 23:03:22'. On the left, a navigation menu includes 'STATUS SYSTEM PORTS' and 'SETTINGS SYSTEM PORTS POE VLANS LINK AGGREGATION'. The main content area is titled 'MAC ADDRESS FILTER' and contains a table with the following data:

Index	VID	MAC Address	Delete
	1	XXXXXXXXXXXX	

Below the table, there is an 'Add' button and 'Apply' and 'Cancel' buttons.

- **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.



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	Event Type	Community	Description	Last Time Sent	Owner	Delete
1 ~ 65535	Log	private	char : 0 ~ 127		char : 0 ~ 32	

Add

- **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: none **Refresh**

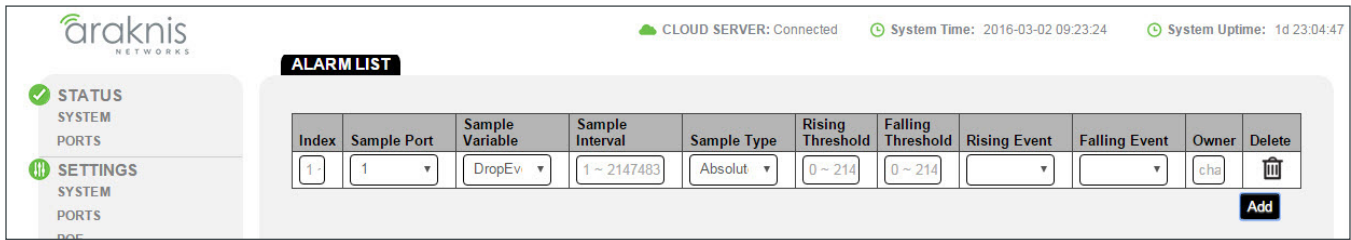
- **Select Event Index** - Select an Event identifier from the drop down. There must be configured entries in the RMON Event List to use the drop down.
- **Refresh** - Click to refresh the list and see the newest events.



RMON - Alarm List

Configure alarms for RMON events.

Figure 72. Alarm List



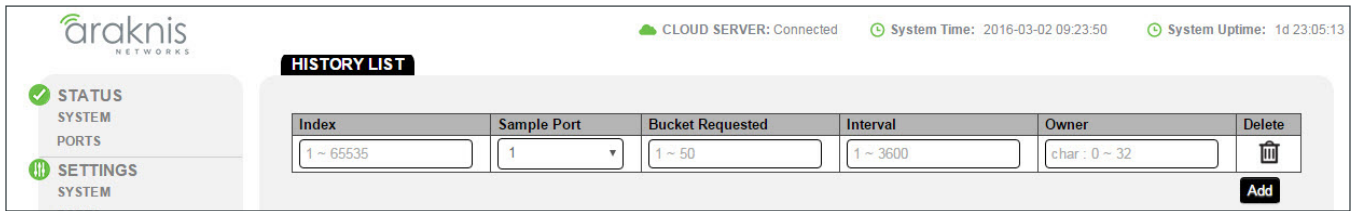
- **Index** - Enter an identifier for the Alarm List entry.
- **Sample Port** - Select the port to monitor from the drop down.
- **Sample Variable** - Select the event type to monitor for. Options: DropEvents, Octets, Pkts, BroadcastPkts, MulticastPkts, CRCAAlignErrors, UnderSizePkts, OverSizePkts, Fragments, 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.



RMON - History List

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

Figure 73. History List

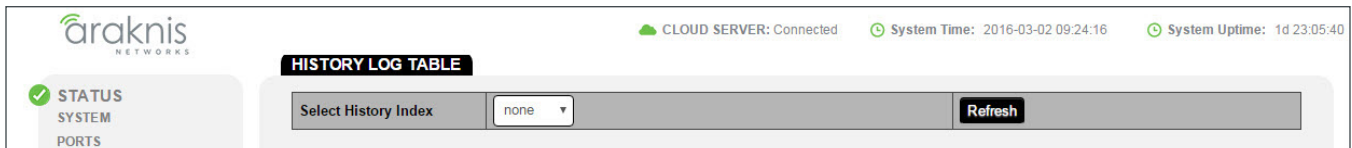


- **Index** - History Log identifier
- **Sample Port** - Select the port to monitor.
- **Bucket Requested** - Enter the number of samples to save in each entry.
- **Interval** - Enter the interval for recording samples on the port.
- **Owner** - Enter the name of the requester.
- **Delete** - Click the 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.

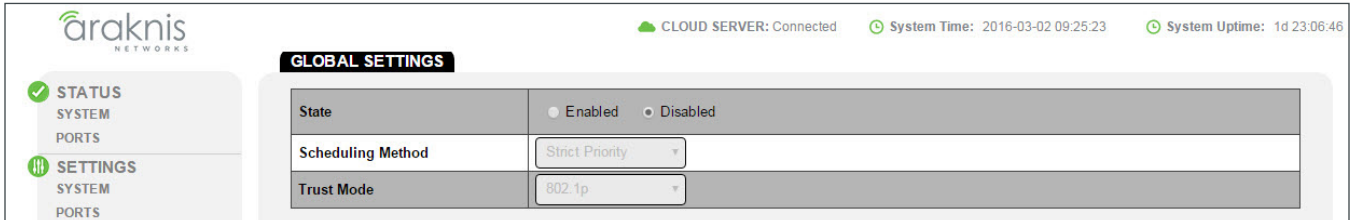


34 - QoS - Overview

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

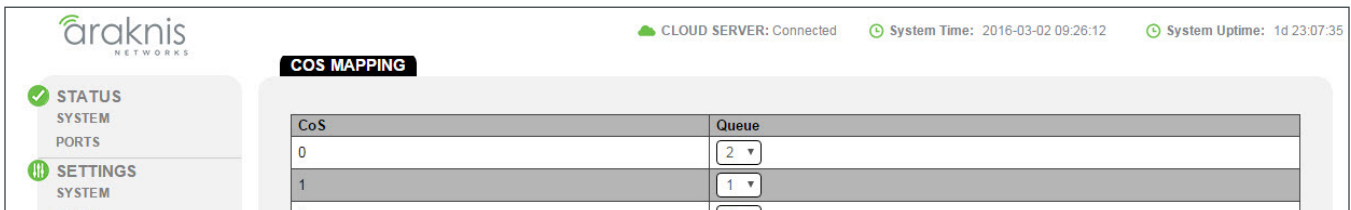


- **State** - Enabled or Disabled.
- **Scheduling Method** - Select the desired mode for scheduling traffic from the drop down:
 - **Strict Priority** - Traffic is scheduled specifically based on queue priority.
 - **WRR** - Use the Weighted Round Robin algorithm to prioritize traffic queues.
- **Trust 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.



QoS - DSCP Mapping

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

Figure 77. DSCP Mapping Table

DSCP	Queue
0	1
1	1

- **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	CoS Value	Trust
1	0	Enabled
2	0	Enabled

- **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	Ingress	Ingress Rate (kbps)	Egress	Egress Rate (kbps)
1	Disabled	Off	Disabled	Off
2	Disabled	Off	Disabled	Off

- **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.



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	Status	Broadcast (kbps)	Unknown Multicast (kbps)	Unknown Unicast (kbps)
1	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
2	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
3	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
4	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
5	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
6	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
7	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
8	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
SFP1	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)
SFP2	Disabled	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)	<input type="checkbox"/> Off (10000)

- **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.



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

MAC ACL List

Index	Name	Delete
1	ACL1	
	<input type="text" value="char: 1 ~ 32"/>	

MAC ACE List

ACL Name	Sequence	Action	Destination MAC Value	Destination MAC Mask	Source MAC Value	Source MAC Mask	VLAN ID	802.1p Value	Ethertype	Delete
ACL1	<input type="text"/>	Permit	Any	Any	Any	Any	Any	Any	Any	

Apply **Cancel**

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.



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.

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

The screenshot shows the IPv4 ACL configuration page. At the top, there's a status bar with 'CLOUD SERVER: Connected', 'System Time: 2016-03-16 10:55:16', and 'System Uptime: 15d 23:37:15'. The sidebar on the left includes sections for STATUS, SETTINGS, MAINTENANCE, and ADVANCED. The main area is titled 'IPv4 ACL' and contains two tables. The first table, 'IPv4 ACL List', has columns for Index, Name, and Delete. The second table, 'IPv4 ACE List', has columns for ACL Name, Sequence, Action, Protocol, Source IP Address, Source IP Mask, Destination IP Address, Destination IP Mask, Source Port Range, Destination Port Range, Flag Set, DSCP, ICMP Code, and Delete. There are 'Add', 'Apply', and 'Cancel' buttons at the bottom of the ACE List table.

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.



IPv4 ACE List Editor

Figure 84. IPv4 ACL ACE Editor

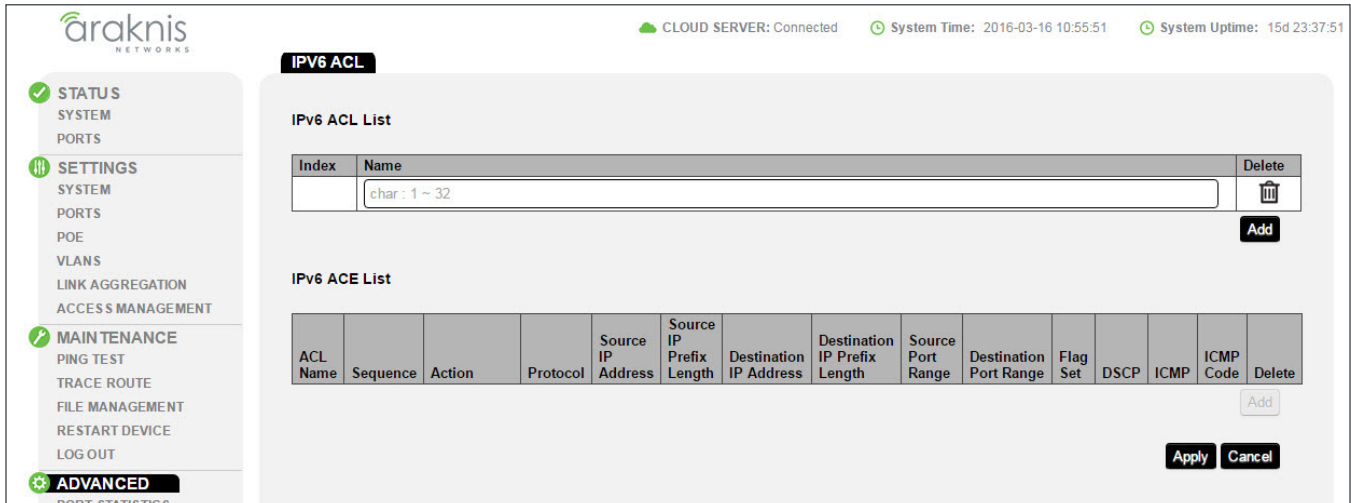
- **ACL Name** – Select the ACL to associate the ACE with.
- **Sequence** – Enter a value for the sequence in relation to other ACLs. The smallest value is processed first.
- **Action** – Select whether to Permit or Deny traffic that meets the set criteria.
- **Protocol** – Select whether traffic using 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 ICMP 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.



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.

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.



ACL - ACL Binding

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

Figure 87. ACL Binding Menu Page

Port	MAC ACL	IPv4 ACL	IPv6 ACL
1	(none)	(none)	(none)
2	(none)	(none)	(none)
3	(none)	(none)	(none)
4	(none)	(none)	(none)
5	(none)	(none)	(none)
6	(none)	(none)	(none)
7	(none)	(none)	(none)
8	(none)	(none)	(none)
SFP1	(none)	(none)	(none)

- **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.



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

Settings	
SNMP State	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Engine ID	<input type="text" value="8000B55303D46A9132F06E"/> <input type="checkbox"/> Default

(10-64 hex letters, the length of the Engine ID should be even.)

- **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.



Trap Settings

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

Figure 89. SNMP Trap Settings

Server IP/Hostname	SNMP Version	Notify Type	Community Name	User Name	UDP	Timeout	Retry	Delete
char: 1	v1	Traps	private		162	15	3	

Add

- **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	Remote Engine ID	Delete
x.x.x.x/xx:xx:xx:xx	10-64 hex	

Add

- **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.

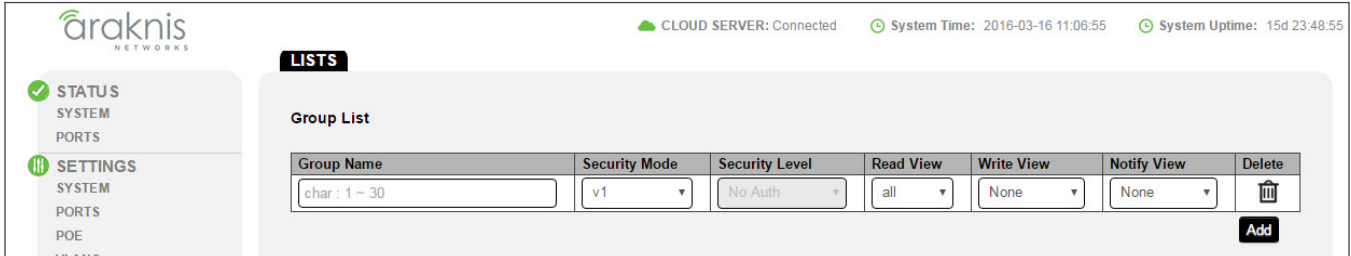


SNMP – Lists

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

Group Lists

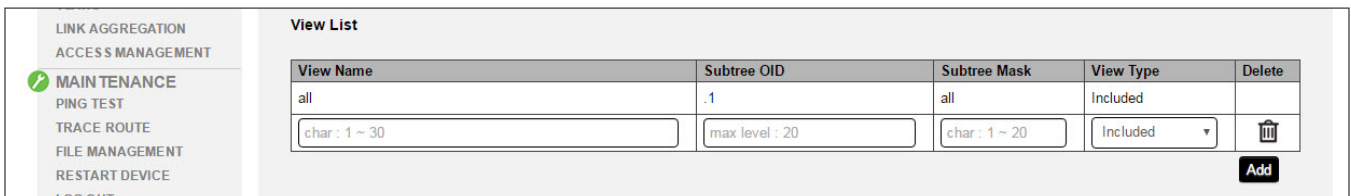
Figure 91. SNMP Group List



- **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.



SNMP Community List

Figure 93. SNMP Community List

Community Name	Community Mode	Group Name	View Name	Access Rights	Delete
private	Basic		all	Read Write	
public	Basic		all	Read Only	
char : 1 ~ 20	Basic		all	Read Only	

Add

- **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	Group Name	Privilege Mode	Authentication Protocol	Authentication Password	Encryption Protocol	Encryption Key	Delete
char : 4 ~ 30		No Auth	None	char : 8 ~ 32	None	char : 8 ~ 64	

Add

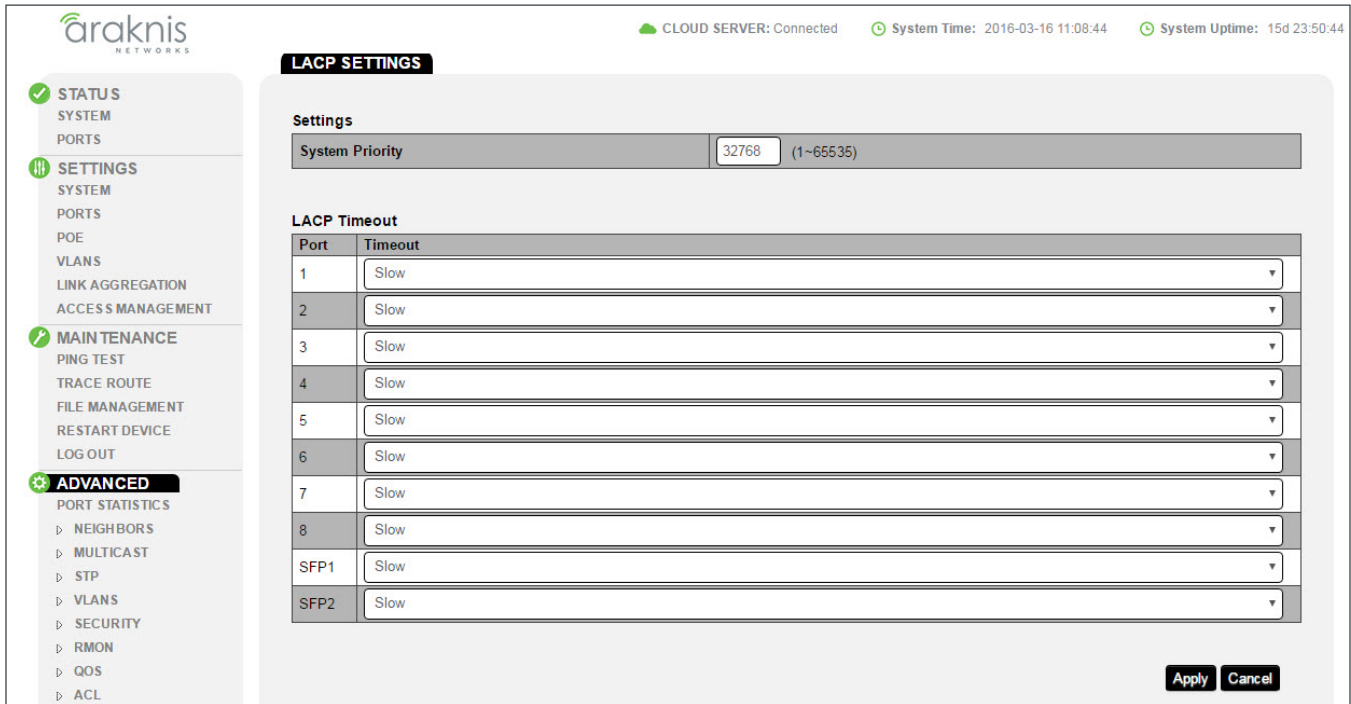
- **User Name** – Enter a name for the user.
- **Group Name** – Select which group the user is a part of. You must configure an SNMP group before configuring this setting.
- **Privilege Mode** –
 - **NoAuth** – No authentication or privacy for group members.
 - **Auth** – SNMP messages are authenticated.
 - **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.



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.



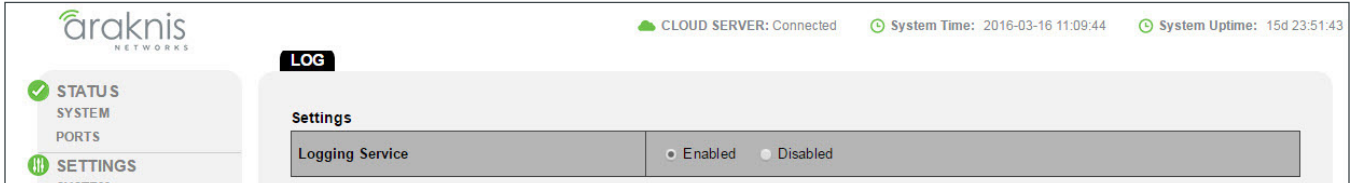
38 - Advanced Log

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

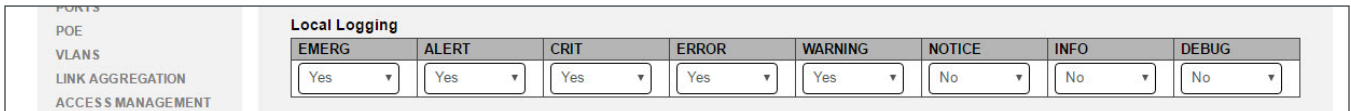


- **Logging Service** - Enabled or disable logging services.

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.

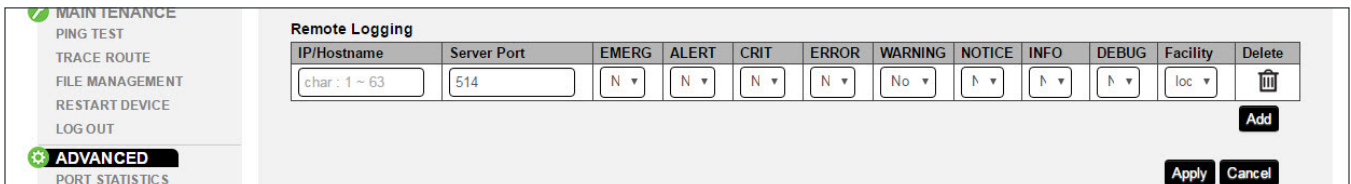
Figure 97. Local Logging



- **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.



Table of Figures

Figure 1.	Package Contents	8
Figure 2.	Mounting Methods	11
Figure 3.	Connection Diagram	13
Figure 4.	EIA/TIA 568B Termination Pattern	13
Figure 5.	PoE Calculation Example	14
Figure 6.	OvrC Operation Diagram	15
Figure 7.	Interface Layout	21
Figure 8.	Apply Button	21
Figure 9.	System Information and Port Status	22
Figure 10.	Events Log	23
Figure 11.	Port Status	24
Figure 12.	System Information Settings	25
Figure 13.	IP Address Settings Menu	26
Figure 14.	Date and Time Settings, UPnP	27
Figure 15.	Recommended System Settings	28
Figure 16.	Jumbo Frame and Basic Port Settings	29
Figure 17.	Advanced Port Settings	30
Figure 18.	PoE Settings Menu	31
Figure 19.	PoE Settings Menu	32
Figure 20.	VLAN Settings	33
Figure 21.	Access and Trunk Port Selection	33
Figure 22.	Configuring Ports in a VLAN	34
Figure 23.	Link Aggregation Settings Menu	35
Figure 24.	Access Management Menu Page	37
Figure 25.	Ping Test Page	38
Figure 26.	Successful Ping Test Result	39
Figure 27.	Failed Ping Test Result	39
Figure 28.	Trace Route Test Page	40
Figure 29.	Trace Route Result	41
Figure 30.	File Management Menu	42
Figure 31.	Dual Image Menu	43
Figure 32.	Restart Page	44
Figure 33.	Log Out Page	44
Figure 34.	Detailed Port Statistics	46
Figure 35.	Neighbors MAC Address Table	48
Figure 36.	LLDP Information	49
Figure 37.	LLDP Settings	50
Figure 38.	LLDP Remote Device Menu	50
Figure 39.	IGMP Snooping Settings	51
Figure 40.	IGMP Snooping VLAN Settings	51



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



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



39 - AN-210-SW Hardware Specifications

	AN-210-SW-8	AN-210-SW-16	AN-210-SW-24	AN-210-SW-48
Ethernet Ports				
10/100/1000BaseT RJ-45 PoE Ports	8	16	24	48
1000BaseT SFP Ports	2	2	2	4
Hardware Performance				
Flash Memory	16MB	16MB	16MB	32MB
SDRAM	128MB	128MB	128MB	256MB
Packet Buffer	524KB	524KB	524KB	1.5MB
MAC Address Table Size	8K	8K	8K	16K
Switching Capacity	20Gbps	36Gbps	52Gbps	104Gbps
Forwarding Rate	14.8Mpps	26.8Mpps	38.7Mpps	77.4Mpps
PoE Features (802.3af/at Compliant)				
Max Power Output per Port	30W	30W	30W	30W
Total PoE Power Budget	65W	130W	190W	375W
Enable/Disable per port	Yes			
Priority Setting per port	Yes			
Overloading Protection per port	Yes			
Power level setting per port	Yes			
Environmental				
Dimensions (W x H x D inches)	12.99x1.73x9.05	17.32x1.73x10.23	17.32x1.73x10.23	17.32x1.73x16.14
Power Supply	100-240V AC, 50/60 Hz			
Max Watts Power Consumption	87W	168W	312W	482W
Operating Temperature	0-50°C/32-122°F			
Humidity (non-condensing)	10 - 90%			



40 - AN-310-SW (Non-PoE) Hardware Specifications

	AN-310-SW-8	AN-310-SW-16	AN-310-SW-24	AN-310-SW-48
Ethernet Ports				
10/100/1000BaseT RJ-45 PoE Ports	8	16	24	48
1000BaseT SFP Ports	2	2	2	4
Hardware Performance				
Flash Memory	16MB	16MB	16MB	32MB
SDRAM	128MB	128MB	128MB	256MB
Packet Buffer	524KB	524KB	524KB	1.5MB
MAC Address Table Size	8K	8K	8K	16K
Switching Capacity	20Gbps	36Gbps	52Gbps	104Gbps
Forwarding Rate	14.8Mpps	26.8Mpps	38.7Mpps	77.4Mpps
Environmental				
Dimensions (W x H x D inches)	12.99x1.73x9.05	17.32x1.73x10.23	17.32x1.73x10.23	17.32x1.73x16.14
Power Supply	100-240V AC, 50/60 Hz			
Max Watts Power Consumption	87W	168W	312W	482W
Operating Temperature	0-50°C/32-122°F			
Humidity (non-condensing)	10 - 90%			



41 - AN-310-SW-POE Hardware Specifications

	AN-310-SW-8-POE	AN-310-SW-16-POE	AN-310-SW-24-POE
Ethernet Ports			
10/100/1000BaseT RJ-45 PoE Ports	8	16	24
1000BaseT SFP Ports	2	2	2
Hardware Performance			
Flash Memory	16MB	16MB	16MB
SDRAM	128MB	128MB	128MB
Packet Buffer	524KB	524KB	524KB
MAC Address Table Size	8K	8K	8K
Switching Capacity	20Gbps	36Gbps	52Gbps
Forwarding Rate	14.8Mpps	26.8Mpps	38.7Mpps
PoE Features (802.3af/at Compliant)			
Max Power Output per Port	30W	30W	30W
Total PoE Power Budget	130W	250W	375W
Enable/Disable per port	Yes		
Priority Setting per port	Yes		
Overloading Protection per port	Yes		
Power level setting per port	Yes		
Environmental			
Dimensions (W x H x D inches)	12.99x1.73x9.05	17.32x1.73x10.23	17.32x1.73x16.14
Power Supply	100-240V AC, 50/60 Hz		
Max Watts Power Consumption	167W	307W	456W
Operating Temperature	0-50°C/32-122°F		
Humidity (non-condensing)	10 - 90%		



42 - General Specifications (All 210/310 Models)

Feature		Supported?	
		AN-210-SW	AN-310-SW
Layer 2 Features			
HOL Blocking	Head-of-line blocking	Yes	Yes
Flow Control	802.3x, Back Pressure	Yes	Yes
Forwarding Mode	Store-and-forward	Yes	Yes
Energy Efficient Ethernet	IEEE 802.3az	Yes	Yes
Spanning Tree	802.1D (STP)	Yes	Yes
	802.1w (RSTP)	Yes	Yes
	802.1s (MSTP)	Yes	Yes
VLAN	802.1Q	Yes	Yes
	Port-based VLANs (Max groups: 4094)	Yes	Yes
	Private VLANs	No	Yes
	QinQ	No	No
	Protocol-based VLAN	No	No
	Voice VLAN	Yes	Yes
Link Aggregation	Static, 802.3ad LACP	Yes	Yes
	Max ports per group	8	8
	Max Group	8	8
Multicast Snooping	IGMP Snooping v1/v2/v3; MLD Snooping v1/v2	Yes	Yes
	IGMP Querier	Yes	Yes
	IGMP Immediate Leave	Yes	Yes
Storm Control	Broadcast/Unknown Multicast/Unknown Unicast	Yes	Yes
Jumbo Frame Support		9k	9k
QoS Features			
Priority queues per port		8	8
Rate Limiting	Ingress	1Kbps/1pps	1Kbps/1pps
	Egress	1Kbps/1pps	1Kbps/1pps
DiffServ (RFC2474)		Yes	Yes
Scheduling	WRR	Yes	Yes
	Strict	Yes	Yes
	Hybrid	No	No
CoS	802.1p	Yes	Yes
	IP ToS Precedence	Yes	Yes
	IP DSCP	Yes	Yes



General Specifications, Continued

Feature	Supported?		
	AN-210-SW	AN-310-SW	
Security			
MAC-based Port Security	Yes	Yes	
802.1x	Yes	Yes	
ACL	L2	No	Yes
	L3	No	Yes
	L4	No	Yes
IP Source Guard	No	No	
RADIUS	Yes	Yes	
TACACS+	No	No	
HTTPS and SSL	Yes	Yes	
SSH v2.0	Yes	Yes	
MAC Filter	Yes	Yes	
IP Filter	No	No	
Management			
Management	CLI, Web, Telnet	Yes	Yes
Dual FW Images		Yes	Yes
FW Upgrade	TFTP upgrade	Yes	Yes
	HTTP upgrade	Yes	Yes
Management Access Filtering	SNMP/Web/Telnet	Yes	Yes
SNMP	v1, v2c, v3	Yes	Yes
SNTP		Yes	Yes
RMON (1,2,3 and 9 groups)		Yes	Yes
DHCP	Server	No	No
	Client	Yes	Yes
	Relay	No	No
	Option82	No	No
	Snooping	No	No
Event log	Local flash, remote server	Yes	Yes
sFlow		No	No
Port Mirroring	One to One, Many to One	Yes	Yes
Remote Ping		Yes	Yes
LLDP (IEEE802.1ab)		Yes	Yes
UPnP		Yes	Yes



43 - 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.



44 - 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



160824-1500