

210/310 SERIES MANAGED NETWORK SWITCH PRODUCT MANUAL

Models:

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





About this Manual

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

| i | 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. |

| \equiv | 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

ପି

| 1 - Welcome to Araknis Networks™ | |
|---|----|
| 2 - Package Contents | |
| 3 - Series Overview | |
| 4 - Device Layout | |
| Rear Facing Models | |
| Front Facing Models | |
| 5 - Hardware Installation | |
| Mounting | 10 |
| Rack Mounting Guidelines | |
| Rack Mount | |
| Wall Mount | 10 |
| Shelf Mount | |
| Connections | 11 |
| Input Power Requirements | |
| Network Cable Requirements | |
| SFP Ports | |
| Switch | |
| PoE Budget Calculation Example | |
| 6 - OvrC Setup | |
| 7 - Interface Access | 14 |
| OvrC Web Connect Access | |
| Direct Access Using LAN IP Address (DHCP) | |
| Default IP Address Access | 16 |
| 8 - Interface Overview | |
| Page Layout | |
| Applying or Canceling Changes | 19 |
| 9 - Switch Status Pages | 20 |
| System Status Page | 20 |
| System Information | 20 |
| Port Status | 20 |
| Events Log | 21 |
| Port Status Page | 22 |
| 10 - System Settings | |
| System Information | 23 |
| IP Address Settings | 24 |
| IPv4 IP Settings | |
| IPv6 IP Settings | 24 |
| Date and Time Settings | |
| UPnP Setting | |
| 11 - Recommended Setup – System Settings | |
| 12 - Port Configuration Settings | |
| Jumbo Frame Setting | |
| Basic Port Settings | 07 |
| Advanced Port Settings | |

ପି

| 13 - PoE Settings | 29 |
|---|-----|
| PoE Setup and Troubleshooting | 30 |
| Checking Status of PoE Devices | 30 |
| Configuring PoE Ports | 30 |
| Troubleshooting PoE Issues | |
| 14 - VLAN Settings (Basic Port-Based) | |
| Access and Trunk Port Selection | |
| Creating a New VLAN | |
| 15 - Link Aggregation Settings | 33 |
| Creating a New Link Aggregation Rule | 34 |
| 16 - Access Management Settings | 35 |
| User Management | 35 |
| HTTP/Telnet/SSH | |
| 17 - Maintenance Menus | 36 |
| Ping Test | |
| Running a Ping Test | |
| Understanding Ping Test Results | 37 |
| Troubleshooting Using Ping Test Results | |
| Trace Route Test | 38 |
| Running a Trace Route Test | |
| Understanding Trace Route Test Results | 39 |
| File Management Settings | 40 |
| Configuration File | |
| Firmware | |
| Dual Image | /1 |
| Firmware Update Instructions | |
| Restart | |
| Log Out | |
| 18 - Advanced Menus | 43 |
| 19 - Advanced Port Statistics | |
| 20 - Neighbors - MAC Address Table | 10 |
| Static and Dynamic MAC Address | 46 |
| 21 - Neighbors - LLDP | |
| Information Table | |
| Settings | 4.0 |
| Remote Device Table | 48 |
| 22 - Multicast - IGMP Snooping | 49 |
| Settings | 49 |
| VLAN Settings | |
| Querier Settings | |
| Group List | |
| Router Settings | |
| URC Settings | 51 |

| 23 - Multicast - MLD Snooping | |
|-------------------------------|----------|
| Settings | |
| | |
| | |
| Router Settings | 53 |
| 24 - STP - Overview | 54 |
| STP - Global Settings | |
| Settings | |
| Root Bridge Information | |
| Basic Setting | 56 |
| | rview57 |
| STP - CIST Settings | |
| | 57 |
| | |
| | |
| | |
| | 61 |
| Advanced VLANs - 802.1Q VLANs | 61 |
| | 61 |
| | |
| | |
| Advanced VLANs - Voice VLANs | 63 |
| | 63 |
| | 64 |
| | 64 |
| | |
| | |
| | |
| | |
| Authenticated Host | |
| 29 - Security - Radius Server | |
| | |
| | 69 |
| | tinued70 |
| | 70 |
| 31 - Security – Port Security | |
| | 71 |
| | |
| | |
| | |
| | |
| | 74 |
| | |
| 34 - QoS - Overview | 75 |
| | 75 |
| | |

ପି

| QoS - COS Mapping | |
|---|-----|
| QoS - DSCP Mapping | |
| QoS - Port Settings | |
| QoS – Bandwidth Control | |
| QoS – Storm Control | |
| 35 - ACL - Overview | 78 |
| ACL - MAC ACL | |
| MAC ACL List | |
| MAC ACE List | |
| MAC ACE List Editor | |
| ACL - IPV4 ACL | |
| IPv4 ACL List | |
| IPv4 ACE List | |
| IPv4 ACE List Editor | |
| ACL - IPV6 ACL | 82 |
| IPv6 ACL List | |
| IPv6 ACE List | |
| IPv6 ACE List Editor | |
| ACL - ACL Binding | |
| 36 - SNMP - Overview | |
| SNMP – Global Settings | 85 |
| Settings | |
| Trap Settings | |
| Remote Engine ID List | |
| SNMP - Lists | 87 |
| Group Lists | |
| View List | |
| SNMP Community List | |
| User List | 88 |
| 37 - Advanced LACP | 89 |
| Settings | |
| LACP Timeout | 89 |
| 38 - Advanced Log | 90 |
| Settings | |
| Local Logging | |
| Remote Logging | |
| 39 - AN-210-SW Specifications | 94 |
| 40 - AN-310-SW Specifications | |
| 41 - Appendix - Safety and Regulatory Information | |
| FCC Warning | |
| CE Warning | 98 |
| UL Statement | 98 |
| 42 - Warranty | 00 |
| 2 Year Limited Warranty | |
| Contact Information | 0.0 |
| | |



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)





Quick Start Guide



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

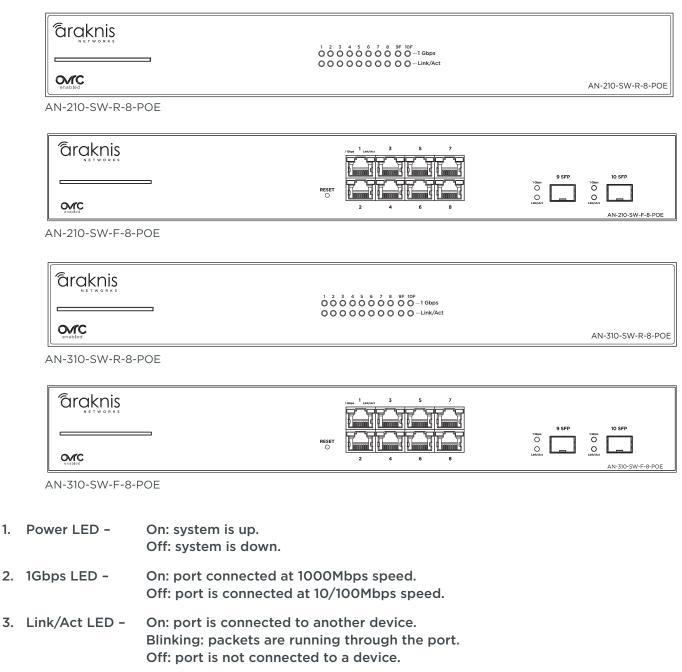


AC Power Cord

3 - Series Overview

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

4 - Device Layout



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

1.

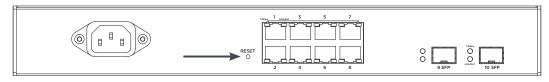
[≡]



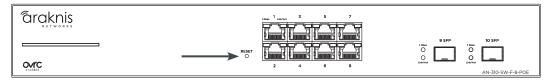
Factory Reset

Reboot or default the switch configuration settings.

Rear Facing Models



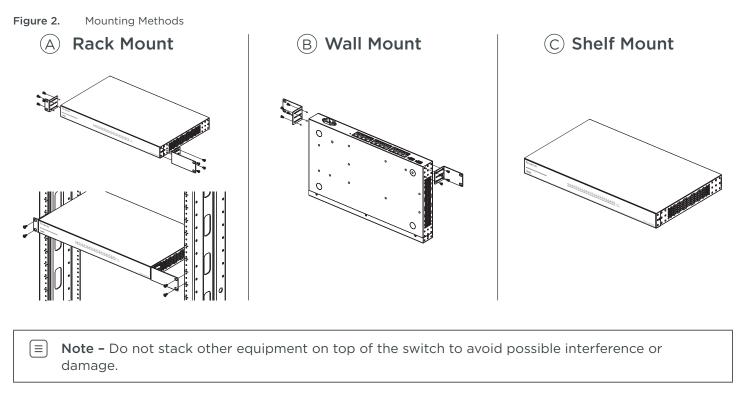
Front Facing Models



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

5 - Hardware Installation

Mounting



 \exists **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.

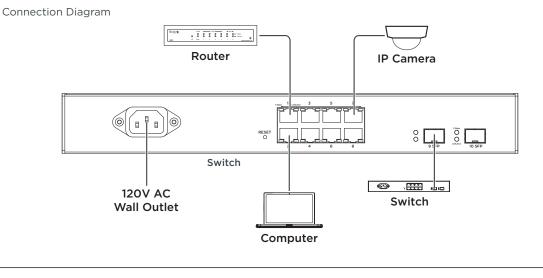
Reliable Earthing – Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (e.g. use of power strips).



Figure 3.

[≡]

Connections



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

| 1 2 3 4 5 6 7 8 | Pin 1 | White/Orange |
|-----------------|-------|--------------|
| | Pin 2 | Orange |
| TIA/EIA-568-B | Pin 3 | White/Green |
| | Pin 4 | Blue |

(Gold pins facing up)

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

Pin 5 Pin 6

Pin 7 Pin 8 White/Blue

White/Brown

Green

Brown

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.

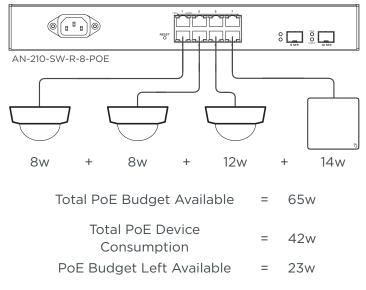
PoE Budgeting

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-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.

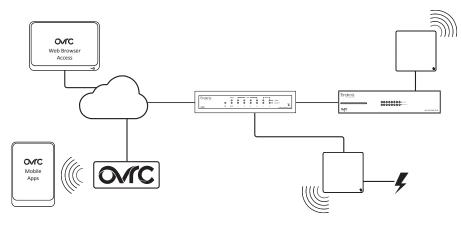
[≡]



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

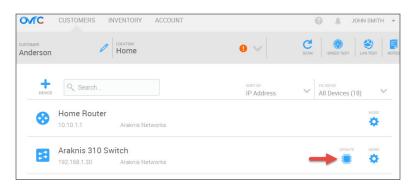


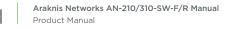
To add this device to your OvrC account:

- 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.

| OVIC CUSTOMERS INVE | NTORY ACCOUNT | 0 | A JOHN SMITH 🔻 | |
|---------------------|-------------------|------------------|----------------|------------------|
| Customers | | Search Customers | Add Customer | |
| A | CUSTOMERS INVENTO | RY ACCOUNT | 8 24 | 🕜 🙏 JOHN SMITH 🔻 |
| | nderson | | • ~ | NOT |
| | Device Search | | SORT BY | All Devices (1) |

- 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.

| | Araknis 310 Switch | | | | MORE | |
|------------|--------------------|------------------|---------------|------|----------|----------|
| | 192.168.1.30 | Araknis Networks | | | | <u> </u> |
| 5 <u>-</u> | | | WEB | INFO | TRANSFER | DELETE |
| Pog | Unspecified | | \rightarrow | 1 | | 2 |
| 0 | 192.168.1.31 | Snap AV | | | | |

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

| Web Connect | 3 |
|---|---|
| This feature is in Beta testing and may not work on all networks. | |
| This will launch the web user interface of the device in a new window. Pop up blockers must be disabled. | |
| Are you on the same local network as the device? | |
| If your computer is on the same LAN as the switch | |
| Cancel | |

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**.

| G Login × ← → C fi 192.168.20.254/login.html | own black of the state of the base | ut pill |) » | × |
|--|------------------------------------|-------------|---------|---|
| | | | | |
| | AUTHENTICATION REQUIRED | Default Log | jin | |
| | Usemame: Password: | Username | araknis | |
| | AN-310-SW-8-POE | Password | araknis | |

- 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**.



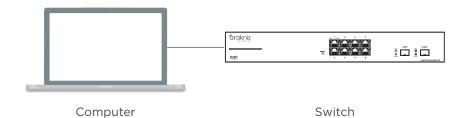
- If you were able to log in successfully, go to the System Settings menu to begin completing the recommended setup for all users. See section "11 - Recommended Setup – System Settings" on page 26.
- 4. If this access method does not work for your application, see the next section for instructions to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

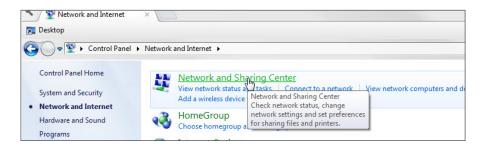
1. Connect your PC to the switch using a network patch cable.



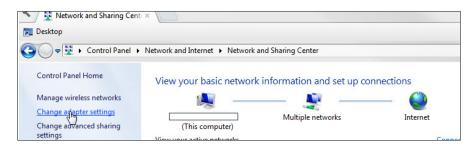
2. On your PC, open the Control Panel and left-click **Network and Internet**.

| Nontrol Panel X | | |
|-----------------|---|--|
| 🕞 Desktop | | |
| Soutrol Panel > | | |
| | Adjust your computer's settings | View by: Category |
| | System and Security Review your computer's status Back up your computer Find and fix problems Network and Internet View network statut Choose homegroup Hardware and View devices and pr Add a device Connect to a proje Adjust commonly used mobility settings | Clock, Language, and Region Change keyboards or other input methods |
| | Programs | A 2.2 |

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.

| Vetwork Connections × Vetwork Connections × Desktop Vetwork an | d Internet → Network Connecti | ons 🕨 | | | |
|---|---|------------------------|-------------|-------------------------|-----------------------------|
| Organize Disable this network device | Diagnose this connection | Rename this connection | Change sett | ings of this connection | |
| Bluetooth Network Connection 2 Not connected Bluetooth Device (Personal Area Wireless Network Connection 5 Not connected Microsoft Virtual WiFi Miniport A | fortissl Disconnected PPPoP WAN Adapter | X | 6 | | VPN Conne conne N Min |

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

| Connect using: | |
|----------------------------------|---|
| | |
| 1ntel(R) 82579 | LM Gigabit Network Connection |
| | Configure |
| This connection use | |
| 🗹 🍨 Client for M | icrosoft Networks |
| QoS Packe | |
| | nter Sharing for Microsoft Networks |
| | tocol Version 6 (TCP/IPv6) |
| | tocol Version 4 (TCP/IPv4) |
| | Topology Discovery Mapper I/O Driver Topology Discovery Responder |
| Contraction of the Carlot Carlot | ropology biscovery hesponder |
| | |
| Install | Uninstall Properties |
| Description | 45 |
| wide area network | trol Protocol/Internet Protocol. The default c protocol that provides communication erconnected networks. |
| | |

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





- 8. Left-click OK to close Internet Protocol Version 4 (TCP/IPv4) Properties, then left-click OK to close Network Connection Properties.
 - Network Connections Desktop nternet Protocol Version 4 (TCP/IPv4) Properties ? 🗙 🖉 🗢 😨 🕨 Cor eneral Local Area Cor You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings. Networking Sha Connect using: Obtain an IP address automatically Intel(R) 825 Use the following IP address: IP address: 192 . 168 . 20 . 2 Subnet mask: 255 . 255 . 255 . 0 Client fr Default gateway: Obtain DNS server address automatically O Use the following DNS server addresses: Preferred DNS server: - Link-Li Alternate DNS server: Instal Validate settings upon exit Advanced... cription Transmission wide area ne across diven Cancel
- 9. Open a web browser and navigate to *http://192.168.20.254/* to load the login screen. Enter your username and password, then click Log In.

| Co Login x | en, Shanking Merchandrates on 10 Strategy | 100 | | _ |
|-------------------------------------|---|-------------|---------|-----|
| ← → C 前 🗋 192.168.20.254/login.html | | | 1 | » = |
| | | | | |
| | AUTHENTICATION REQUIRED | Default Log | Jin | |
| | Usemame: Password: | Username | araknis | |
| | AN-310-SW-8-POE | Password | araknis | |

 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

| araknis | B CLOUD SERVER | Connected O System Time: 2016-02-08 12:28:10 O System Uptime: 0d 01:33 |
|---|--------------------|---|
| STATUS SYSTEM PORTS | System Information | |
| | System Name | AN-310-SW-8-POE |
| SYSTEM | Model Number | AN-310-SW-8-POE |
| PORTS | FW Version | v0.0.12 (Feb 01 2016 - 10:46:38) |
| POE | Service Tag | ST15270020148411 |
| VLANS LINK AGGREGATION | MAC Address | D4:6A:91:32:F0:6E |
| ACCESS MANAGEMENT | IP Address | 192.168.1.30 |
| MAIN TENANCE | Gateway | 192.168.1.1 |
| TRACE ROUTE FILE MANAGEMENT RESTART DEVICE LOG OUT | Down 100fdx 1G | PoE PoE |
| ADVANCED | AN-310-SW-&-POE | 1 3 5 7 3 7 3 7 3 7 3 7 3 7 3 7 3 7 3 |

• 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

| UPnP | Enabled | |
|-------|---------|--------------|
| - | | |
| | | Apply Cancel |

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

| araknis | SYSTEM STATUS | CLOUD SERVER: Connec | () System Time: 2016-02-08 12:28:10 | ⊙ System Uptime: Od 01:33:49 |
|---|--------------------|----------------------|-------------------------------------|------------------------------|
| STATUS SYSTEM | System Information | | | |
| PORTS | System Name | AI | N-310-SW-8-POE | |
| | Model Number | AI | N-310-SW-8-POE | |
| PORTS | FW Version | V | .0.12 (Feb 01 2016 - 10:46:38) | |
| POE | Service Tag | S | F15270020148411 | |
| LINK AGGREGATION | MAC Address | D4 | 4:6A:91:32:F0:6E | |
| ACCESS MANAGEMENT | IP Address | 15 | 02.168.1.30 | |
| MAIN TENANCE PING TEST | Gateway | 19 | 12.168.1.1 | |
| TRACE ROUTE FILE MANAGEMENT RESTART DEVICE LOG OUT | | | Ofdx 1Gfdx Disabled loE PoE | |
| ADVANCED | | AN-310-SW-8-POE | 5 7 6 8 SFP1 SFP2 | |
| | 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

| | | | Q |
|------------------------|----------|----------|---------------|
| 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) | 1 | Previous Nex |

- 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

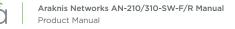
This page provides in-depth details about the status of each physical port.

Path - Status, Ports

Figure 11. Port Status

| STATUS SYSTEM PORTS | | | Down 100fdz | | 00fdx 1Gfd PoE PoE | x Disabled | | | | |
|--|-----------|--------|-----------------|------------------|-----------------------|-------------|----------|--------|----------|----------|
| BETTINGS SYSTEM PORTS POE VLANS LINK AGGREGATION ACCESS MANAGEMENT | | | AN-310-SW-8-POE | | | SFP1 SFP2 | | | | |
| MAIN TENANCE | Port Sta | itus | | Link | | Aggregation | Bytes | Errors | Bytes | Errors |
| TRACE ROUTE | Port | Name | | Speed | Duplex | Group | Sent | Sent | Received | Received |
| FILE MANAGEMENT | 1 | Port 1 | | 1Gbps | Full | | 6812261 | 0 | 42590662 | 0 |
| RESTART DEVICE | 2 | Port 2 | | Not Connected | Not Connected | | 0 | 0 | 0 | 0 |
| ADVANCED | 3 | Port 3 | | 1Gbps | Full | | 9701589 | 0 | 175097 | 0 |
| | 4 | Port 4 | | 100Mbps | Full | | 9842143 | 0 | 252748 | 0 |
| Q Search | 5 | Port 5 | | Not Connected | Not Connected | | 0 | 0 | 0 | 0 |
| | 6 | Port 6 | | 100Mbps | Full | | 42259199 | 0 | 4772248 | 0 |
| | 7 | Port 7 | | Not Connected | Not Connected | | 0 | 0 | 0 | 0 |
| | | Port 8 | | 1Gbps | Full | | 9823876 | 0 | 258095 | 0 |
| | 8 | | | Not | Not | | 0 | 0 | 0 | 0 |
| | 8 SFP1 | SFP 1 | | Connected | Connected | | | | | |

- **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

| araknis | SYSTEM SETTINGS | CLOUD SERVER: Connected | () System Time: 2016-02-08 12:28:48 | System Uptime: 0d 01:34: |
|--------------------------------|----------------------------|------------------------------|-------------------------------------|--------------------------|
| STATUS SYSTEM | System | | | |
| PORTS | System Name | AN-310-SW-8-POE | (char : 1 ~ 255) | |
| SETTINGS SYSTEM | System Location | Home Rack | (char : 0 ~ 255) | |
| PORTS | Admin Username | admin | (char : 1 ~ 18) | |
| POE | Current Admin Password | | (char : 4 ~ 32) | |
| VLANS LINK AGGREGATION | New Admin Password | | (char : 4 ~ 32) | |
| ACCESS MANAGEMENT | Confirm New Admin Password | | (char : 4 ~ 32) | |
| MAIN TENANCE PING TEST | Management VLAN ID | 1 • | | |
| TRACE ROUTE FILE MANAGEMENT | LED | ● 1Gbps ○ PoE ○ 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

| IPv4 | | IPv6 | | |
|--------------------|------------------|--------------------|--|--|
| Auto Configuration | Static OHCP | 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

| 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 T | ime (US and Canada) |
| 🕢 Enable Daylight Saving | |
| Start: March V 2nd V S | |
| End: November V 1st V S | un • 02 • : 00 • |
| | |
| JPnP 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 Conect or OvrC web monitoring. Contact technical support if you need to disable OvrC functionality.



Figure 15.

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

| SYSTEM | System | | | | |
|---------------------------|---|----------------------------|--------------------|---------------------------|-----------|
| PORTS | System Name | AN-310-SW-8-POE | (char : 1 ~ 255) | | |
| SETTINGS > SYSTEM | System Location | Home Rack | (char : 0 ~ 255) | | |
| PORTS | Admin Username | admin | (char : 1 ~ 18) | Default Set | ting |
| POE VLANS | Current Admin Password | | (char : 4 ~ 32) | | L |
| LINK AGGREGATION | New Admin Password | | (char : 4 ~ 32) | Username | araknis |
| ACCESS MANAGEMENT | Confirm New Admin Passwor | rd | (char : 4 ~ 32) | | <u> </u> |
| MAIN TENANCE PING TEST | Management VLAN ID | 1 1 | | Password | araknis |
| TRACE ROUTE | LED | ● 1Gbps PoE Dis | abled | | |
| FILE MANAGEMENT | | | | | |
| RESTART DEVICE LOG OUT | IP Address Settings | 14 | | | |
| ADVANCED | IPv4 | | IPv6 | | |
| | Auto Configuration | Static OHCP | IPv6 State | Auto Configuration | |
| Q Search | Auto configuration | State Offer | IF VO State | Auto Configuration | |
| | IPv4 Address | 192.168.1.30 | IPv6 Address | fe80::d66a:91ff:fe32:f06e | |
| | IF V4 Address | 132.100.1.30 | IF VO Address | 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 | | | | |
| | | | | | |
| | Date and Time Settings | | | | |
| | Manually Set Date and Tim | 10 | | | |
| | Date: 2016 / 2 / 08 | | | | |
| | Time: 12 : 28 (24-H | lour) | | | |
| | Synchronize with PC | | | | |
| | Automatically Get Date and | | | | |
| | NTP Server: time.nist.gov | T | | | |
| | Time Zone: (GMT-05:00) Eas | ntom Time (US and Canada) | | | |
| | Enable Daylight Saving | nom nime (US allu Gallaua) | | | |
| | | ▼ Sun ▼ 02 ▼ : 00 ▼ | | | |
| | End: November • 1st | | | | |
| | | | | | |
| | | | | | |
| | UPnP Configuration | [Factbook and] | | | |
| | UPnP | Enabled v | | | |
| | | | | | |
| | | | | App | ly Cancel |

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 |
|------------|-------------------------------------|
|------------|-------------------------------------|

| PORTS | Size | 9216 Bytes (1522-9216) | |
|-----------------------------------|---------|------------------------|---------------|
| SETTINGS | 5120 | 9216 Bytes (1522-9216) | |
| SYSTEM | | | |
| • PORTS | Basic F | t Settings | |
| POE VLANS | Port | Name | Speed Duplex |
| LINK AGGREGATION | 1 | Port 1 | Auto 🔻 Auto |
| ACCESS MANAGEMENT | 2 | Port 2 | Auto 🔻 Auto |
| MAIN TENANCE PING TEST | 3 | Port 3 | Auto V Auto |
| TRACE ROUTE | 4 | Port 4 | Auto • Auto • |
| FILE MANAGEMENT RESTART DEVICE | 5 | Port 5 | Auto • Auto • |
| LOG OUT | 6 | Port 6 | Auto |
| ADVANCED | 7 | Port 7 | Auto 🔻 Auto |
| C Search | 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 V 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

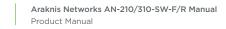
| Path - | Settings, | Ports, | Advanced | Port | Settings |
|--------|-----------|--------|----------|------|----------|
|--------|-----------|--------|----------|------|----------|

Figure 17. Advanced Port Settings

| 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 🔻 | |

- **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 |
|------------|-------------------|
|------------|-------------------|

| SYSTEM PORTS | Enable | Port | Power Lin Type | nit | Priority | | Status | Class | Output Voltage (V) | Output Current (mA) | Output Power (W) | Power Cycle |
|-----------------------------------|--------|------|-------------------|-----|----------|---|------------|-------|-----------------------|------------------------|---------------------|----------------|
| SETTINGS | | 1 | Auto | * | Low | * | Delivering | 4 | 54.7 | 72 | 3.9 | |
| SYSTEM PORTS | | 2 | Auto | • | Low | • | Detecting | | | | | |
| ▶ POE | | 3 | Auto | • | Low | * | Detecting | | | | | |
| VLANS LINK AGGREGATION | ~ | 4 | Auto | • | Low | • | Detecting | | | | | |
| ACCESS MANAGEMENT | | 5 | Auto | * | Low | * | Detecting | | | | | |
| MAIN TENANCE | ~ | 6 | Auto | • | Low | • | Detecting | | | | | |
| TRACE ROUTE | | 7 | Auto | • | Low | • | Detecting | | | | | |
| FILE MANAGEMENT RESTART DEVICE | ~ | 8 | Auto | • | Low | • | Detecting | | | | | |

- **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

| STATUS | | | | | | | | | | |
|--------------------|--------|------|---------------------|----------|------------|-------|-----------------------|------------------------|---------------------|----------------|
| SYSTEM PORTS | Enable | Port | Power Limit Type | Priority | Status | Class | Output Voltage (V) | Output Current (mA) | Output Power (W) | Power Cycle |
| SETTINGS SYSTEM | | 1 | Auto 🔹 | Low • | Delivering | 4 | 54.7 | 72 | 3.9 | |

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

| araknis | _ | | CLOUD SERVER | R: Connected O System 1 | ime: 2016-02-08 12:30:08 | System Uptime: Od 01:3 |
|-----------------|--------------|---------------|-------------------------|-------------------------|--------------------------|------------------------|
| STATUS | VLAN SETTING | S Name | Access Port | Trunk Port | Custom Port | Delete |
| SYSTEM PORTS | 1 | default | 1-8,SFP1-SFP2,LAG1-LAG8 | | | |
| SETTINGS | 1 ~ 4094 | char : 0 ~ 32 | | | | ⑪ |
| SYSTEM | | | | | | Add |
| PORTS | | | | | | Add |
| POE | | | | | | |
| ▶ VLANS | | | | | | Apply Cancel |

- 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

| VID | | N | ame | | Acces | ss Por | t | | | Trunk | Port | | |
|-----|--------|------|---------|-----|-------|--------|-----|---------|-----|-------|------|------|------|
| 1 | | | default | | 1-8,5 | SFP1-S | FP2 | LAG1-LA | AG8 | | | | |
| 20 | Media | | | 3-5 | | | | 2 | | | | | |
| | | | | | | | | | | | | | |
| | Port | 1 | 2 | 3 4 | 4 | 5 | 6 | 7 | 8 | SFP1 | SFP2 | LAG1 | LAG2 |
| | Access | 0 | 0 | ۲ | ۲ | ۲ | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| | Trunk | | • | • | • | • | • | | • | • | | • | |
| | none | ۲ | 0 | 0 | 0 | 0 | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ |
| | | | | | 1 | | | | | | | | |
| | Port | LAG3 | LAG4 | | | | | LAG8 | | | | | |
| | Access | | 0 | 0 | 0 | 0 | | 0 | | | | | |
| | Trunk | | • | • | • | |)/ | • | | | | | |
| | none | ۲ | ۲ | ۲ | ۲ | ۲ | | ۲ | | | | | |
| | | | | | | _ | | | | | | | |
| | | | | | | Conf | m | Cancel | | | | | |

- 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.

| /ID | | N | ame | | Acces | ss Po | rt | | | Trunk | Port | | |
|-----|--------|------|---------|-----|-------|-------|------|--------|-----|-------|------|------|-----|
| | | | default | | 1-8,5 | SFP1- | SFP2 | LAG1-L | AG8 | | | | |
| 0 | | | Media | | 3-5 | | | | | 2 | | | |
| Ĩ | | | | | | | | | | | | | |
| - 1 | Port | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | SFP1 | SFP2 | LAG1 | LAG |
| | Access | | \odot | ۲ | ۲ | ۲ | C | 0 | | 0 | 0 | 0 | 0 |
| | Trunk | • | • | | | | | | | • | • | | |
| | none | ۲ | 0 | 0 | 0 | 0 | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ | ۲ |
| | Port | LAG3 | LAG4 | LAG | 5 LAG | 6 L/ | AG7 | LAG8 | | | | | |
| | Access | 0 | 0 | 0 | 0 | | 0 | 0 | | | | | |
| | Trunk | • | • | • | • | | • | • | | | | | |
| | none | ۲ | ۲ | ۲ | ۲ | 2 | ۲ | ۲ | | | | | |
| | none | ۲ | ۲ | ۲ | ۲ | _ | | Oancel | | | | | |

Figure 22. Configuring Ports in a VLAN

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



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.

| STATUS SYSTEM | Group | Name | Mode | Active Ports | Member Ports |
|--|-------|-------|------------|--------------|--------------|
| PORTS | 1 | LAG 1 | Disabled • | | |
| SETTINGS SYSTEM | 2 | LAG 2 | Disabled v | | |
| PORTS POE | 3 | LAG 3 | Disabled • | | |
| VLANS | 4 | LAG 4 | Disabled • | | |
| ►LINK AGGREGATION ACCESS MANAGEMENT | 5 | LAG 5 | Disabled 🔹 | | |
| MAIN TENANCE | 6 | LAG 6 | Disabled • | | |
| PING TEST TRACE ROUTE | 7 | LAG 7 | Disabled • | | |
| FILE MANAGEMENT | 8 | LAG 8 | Disabled • | | |



- **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 | | |
| | Confirm Cancel | | | Apply Cancel |

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

 \blacksquare 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.



| User Management User Name | | Password | | Privilege Type | | Delete |
|------------------------------|---|--|---|---|--|---|
| admin | | char : 4 ~ 32 | 0 | Admin | | |
| char : 1 ~ 18 | | char : 4 ~ 32 | | Admin | • | 匬 |
| | | | | Admin | | |
| | | | | User | | Add |
| | | | | | | 100 |
| HTTP/Teinet/SSH | | | | | | |
| нттр | • Enabl | ed 🔿 Disabled | | | | |
| HTTPS | Enable | ed 💿 Disabled | | | | |
| Telnet Enabled Disabled | | | | | | |
| | | | | | | |
| | User Name admin char:1~18 HTTP/Telnet/SSH HTTP HTTPS | User Name admin (char : 1 ~ 18 HTTP/Telnet/SSH HTTP • Enable HTTPS • Enable | User Name Password admin char : 4 ~ 32 char : 1 ~ 18 char : 4 ~ 32 HTTP/Telnet/SSH HTTP • Enabled HTTPS © Enabled | User Name Password admin char : 4 ~ 32 (char : 1 ~ 18 char : 4 ~ 32 | User Name Password Privilege Type admin char: 4 ~ 32 Admin (char: 1 ~ 18 char: 4 ~ 32 Admin HTTP/Telnet/SSH HTTP • Enabled Disabled HTTPS © Enabled @ Disabled | User Name Password Privilege Type admin Char : 4 ~ 32 Admin Char : 1 ~ 18 Char : 4 ~ 32 Admin |

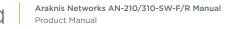
User Management

- 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 2 | 5. Ping | Test Page | |
|----------|---------|-----------|--|
|----------|---------|-----------|--|

| araknis | PING TEST | CLOUD SERVER: Connected | • System Time: 2016-02-08 12:31:35 | ⊙ System Uptime: 0d 0 |
|--------------------------------|---------------------------|--------------------------|------------------------------------|-----------------------|
| STATUS SYSTEM PORTS | | | | |
| | IP Address: 192.168.1.100 | (x.x.x.x or hostname) | | |
| PORTS POE | Count: 4 (1 | - 5 Default:4) | | |
| VLANS LINK AGGREGATION | | - 5 Default : 1) | | |
| ACCESS MANAGEMENT | Size (in bytes): 56 (8 | 3 - 5120 Default : 56) | | |
| PING TEST | | | | |
| TRACE ROUTE FILE MANAGEMENT | Result: | | | |
| RESTART DEVICE LOG OUT | | | | |
| O ADVANCED | | | | |
| Q Search | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | Test |

- 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

| 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 |
| Result. | I 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=0 ttl=64 time=0.0 ms |
| | 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 |

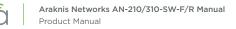
Figure 27. Failed Ping Test Result

| 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.



| araknis. | ACE ROUTE | CLOUD SERVER: Connected | • System Time: 2016-02-08 12:31:49 | System Uptime: 0d 01:3 |
|--|-------------|--------------------------|------------------------------------|------------------------|
| STATUS SYSTEM PORTS | IP Address: | (x.x.x.x or hostname) | | |
| SETTINGS SYSTEM PORTS POE | Max Hop: 30 | 2 - 255 Default : 30) | | |
| VLANS LINK AGGREGATION ACCESS MANAGEMENT | Result: | | | |
| MAINTENANCE PING TEST →TRACE ROUTE | | | | |
| FILE MANAGEMENT RESTART DEVICE LOG OUT | | | | |
| ADVANCED | | | | |
| (Q Search) | | | | |
| | | | | |
| | | | | Test |

- 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 clickdrag.
- 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

| IP Address: | 8.8.8.8 (x.x.x.x or hostname) |
|-------------|---|
| Max Hop: | 30 (2 - 255 Default : 30) |
| Result: | traceroute 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 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 20 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 20 ms 20 ms 11 209.85.143.197 (209.85.143.197) 36 bytes to 192.168.1.30 20 ms 20.985.243.254 (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 21 2.168.1.30 10 ms 209.85.143.201 (209.85.143.201) 36 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 209.85.143.197 (209.85.143.201) (209.85.143.201) 36 bytes to 192.168.1.30 20 ms 11 209.85.143.197 (209.85.143.107) 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 11 38.8.8.8 (8.8.8.8) 36 bytes to 192.168.1.30 10 ms 30 ms 20 ms |
| | |

- 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.



| araknis | FILE MANAGEMENT | CLOUD SERVER: Connected | System Time: 2016-02-08 12:32:08 | System Uptime: 0d 01:37:47 |
|---------------------------|-------------------------------|----------------------------|----------------------------------|----------------------------|
| STATUS SYSTEM PORTS | Configuration File | | | |
| | Backup Current Configuration | To PC | | |
| SYSTEM | Upload New Configuration File | Choose File No file chosen | | |
| PORTS | | From PC | | |
| POE | Restore Factory Defaults | Yes | | |
| VLANS | | | | |
| LINK AGGREGATION | | | | |
| ACCESS MANAGEMENT | Firmware 🚱 | | | |
| MAINTENANCE | Current Firmware Version | v0.0.12 | | |
| PING TEST | Partition | Partition 0(Active) | | |
| TRACE ROUTE | T di di di di | | | |
| FILE MANAGEMENT | Upload New Firmware | Choose File No file chosen | | |
| RESTART DEVICE | opioad New Pittiwale | Upload to Partition | | |
| LOGOUT | | | | |

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

| | Flash Partition | Status | Image Name | Image Size(Byte) | Created Time |
|-------|-----------------|--------|------------|------------------|---------------------|
| ۲ | Partition 0 | Active | IMG-0.0.12 | 6050953 | 2016-02-01 10:46:38 |
| | Partition 1 | Backup | IMG-0.0.02 | 6089118 | 2015-06-15 15:14:01 |

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

Firmware Update Instructions

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

| ACCESS MANAGEMENT | Firmware 😧 | |
|--------------------------|--------------------------|----------------------------|
| MAIN TENANCE | Current Firmware Version | v0.0.12 |
| PING TEST TRACE ROUTE | Partition | Partition 0(Active) |
| FILE MANAGEMENT | | Choose File No file chosen |
| RESTART DEVICE | Upload New Firmware | Upload to Partition |

- 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

| araknis, | | CLOUD SERVER: Connected | • System Time: 2016-02-08 12:32:13 | • System Uptime: | 0d 01:37:51 |
|-------------------------------|---|-------------------------------|------------------------------------|------------------|-------------|
| STATUS SYSTEM PORTS | RESTART DEVICE | | | | |
| SETTINGS SYSTEM PORTS | Caution: Pressing this button wil Restart Switch | I cause the device to reboot. | | | |

• 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

| araknis | LOG OUT | CLOUD SERVER: Connected | • System Time: 2016-02-08 12:32:57 | System Uptime: 0d 01:38:36 |
|---------------------------|-------------------------------------|-------------------------|------------------------------------|----------------------------|
| STATUS SYSTEM PORTS | To Log Out, click "Log Out" button. | | | |
| (I) SETTINGS SYSTEM | Log Out | | | |

• 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.



| STATUS SYSTEM PORTS | | | | Port 1 | |
|-----------------------------------|------------------|---------------|--------------------------|---------|--|
| | Rece | eive Total | Transmit | Total | |
| SYSTEM | Rx Packets | 1269 | Tx Packets | 17375 | |
| PORTS | Rx Octets | 228421 | Tx Octets | 3344148 | |
| VLANS | Rx Unicast | 1266 | Tx Unicast | 1729 | |
| LINK AGGREGATION | Rx Multicast | 0 | Tx Multicast | 11728 | |
| ACCESSMANAGEMENT | Rx Broadcast | 3 | Tx Broadcast | 3918 | |
| MAIN TENANCE PING TEST | Rx Pause | 0 | Tx Pause | 0 | |
| | Receive E | Fror Counters | Receive Size Counters | | |
| FILE MANAGEMENT RESTART DEVICE | Rx Drops | 0 | Pkts 64 Octets | 58 | |
| LOG OUT | Rx CRC/Alignment | 0 | Pkts 65 to 127 Octets | 446 | |
| ADVANCED PORT STATISTICS | Rx Undersize | 0 | Pkts 128 to 255 Octets | 600 | |
| NEIGHBORS | Rx Oversize | 0 | Pkts 256 to 511 Octets | 7 | |
| ▶ MULTICAST | Rx Fragments | 0 | Pkts 512 to 1023 Octets | 155 | |
| D STP D VLANS | Rx Jabber | 0 | Pkts 1024 to 1518 Octets | 3 | |

• 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

| | Static N | AC Address | | | |
|----------------------------|----------|---------------|----------|-------------------|---------|
| PORTS | Index | Port | VID | MAC Address | Delete |
| | | 1 | r] [1 v] | XXXXXXXXXXXXXX | <u></u> |
| SYSTEM PORTS | L | | | | Add |
| POE | | | | | |
| VLANS | Dynami | c MAC Address | | | |
| LINK AGGREGATION | Index | Port | VID | MAC Address | |
| ACCESS MANAGEMENT | 1 | 4 | 1 | 00:03:EA:0A:A4:10 | |
| | 2 | 7 | 1 | 34:02:86:BB:32:FD | |
| PING TEST TRACE ROUTE | 3 | 7 | 1 | 34:E6:D7:76:6A:62 | |
| FILE MANAGEMENT | 4 | 7 | 1 | 6C:40:08:58:D8:EA | |
| RESTART DEVICE | 5 | 7 | 1 | 74:D0:2B:5D:C6:C0 | |
| LOG OUT | 6 | 7 | 1 | 80:D2:1D:13:12:B6 | |
| | | | | | |
| PORT STATISTICS NEIGHBORS | 7 | 7 | 1 | B0:83:FE:7F:3C:82 | |
| MAC ADDRESS TABLE | 8 | 7 | 1 | B0:E8:92:0D:41:6F | |
| LLDP | 9 | 6 | 1 | B8:27:EB:FA:7E:97 | |
| D MULTICAST | 10 | 3 | 1 | D4:6A:91:12:1E:6A | |
| ⊳ STP | 11 | 7 | 1 | D4:6A:91:31:10:95 | |
| VLANS SECURITY | 12 | 7 | 1 | D4:6A:91:31:10:96 | |
| | 13 | 1 | 1 | D4:6A:91:32:3B:56 | |
| RMON | 15 | 7 | 1 | D4:6A:91:32:EC:6A | |
| D RMON D QOS | 14 | | | | |

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 | |
|------------|------------------|--|
|------------|------------------|--|

| araknis | LLDP | | CLOUD SERVER: Connected | • System Time: 2016-02-29 19:57:22 | System Uptime: 0d 09:38: |
|---------------------------|------------------------|------------------------|-------------------------|------------------------------------|--------------------------|
| STATUS SYSTEM | Information | | | | |
| PORTS | Chassis ID Subtype | MAC Address | | | |
| BETTINGS SYSTEM | Chassis ID | D4:6A:91:32:F0:6E | | | |
| PORTS | System Name | AN-310-SW-8-POE | | | |
| POE VLANS | System Description | Araknis 310 8 Port PoE | | | |
| LINK AGGREGATION | Capabilities Supported | Bridge | | | |
| ACCESSMANAGEMENT | Capabilities Enabled | Bridge | | | |
| MAIN TENANCE PING TEST | 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 | LLDP Settings |
|--------------------------|---------------|
|--------------------------|---------------|

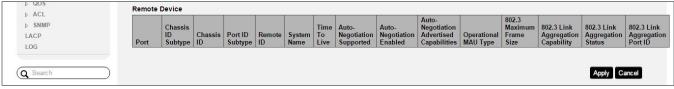
| PORT STATISTICS | Settings | Settings | | | | | | | |
|-----------------------|---------------------------|--------------|-----------|--|--|--|--|--|--|
| ▲ NEIGHBORS | State | Enabled Disa | abled | | | | | | |
| MAC ADDRESS TABLE | Transmission Interval(s) | 30 | (5-32767) | | | | | | |
| LLDP MULTICAST | Holdtime Multiplier | 4 | (2-10) | | | | | | |
| ⊳ STP | Reinitialization Delay(s) | 2 | (1-10) | | | | | | |
| D VLANS D SECURITY | Transmit Delay(s) | 2 | (1-8192) | | | | | | |
| N RMON | 3 | | | | | | | | |

- 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.





- **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 IDSystem 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.



| SYSTEM | Settings | |
|----------------------|--------------------|---------------------------------------|
| PORTS | Status | Enabled • Disabled |
| B SETTINGS SYSTEM | Version | ●V2 |
| PORTS | Report Suppression | Enabled Disabled |
| PUE | | · · · · · · · · · · · · · · · · · · · |

- **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 |
|------------|------|----------|------|----------|
|------------|------|----------|------|----------|

| LINK AGGREGATION | VLAN Settings | | | | |
|---------------------------|---------------|----------------------|---|------------|---|
| ACCESS MANAGEMENT | VLAN ID | IGMP Snooping Status | | Fast Leave | |
| MAIN TENANCE PING TEST | 1 | Disabled | ٣ | 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

| FILE MANAGEMENT | Querier | Settings | | | | | | | | 2 | | | | |
|--|------------|------------------|--------------------|-----------------|---------------|------------|----------|------------------|----|----------------------------------|---|--|-------|---|
| RESTART DEVICE LOG OUT ADVANCED PORT STATISTICS | VLAN ID | Querier State | Querier Version | | Querier IP | Robustness | Interval | Oper Interval | | Oper Max Response Interval | | Oper Last Member Query Counter | Query | Oper Last Member Query Interval |
| ▶ NEIGHBORS▲ MULTICAST | 1 | Disal 🔻 | v2 v | 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 | l ist | Settinas |
|------------|-------|----------|-------|-------|----------|
| Figure 42. | IGHIP | Shooping | Group | LISU | Settings |

| MLD SNOOPING | Group List | | |
|-----------------|------------|------------------|--------------|
| ▷ STP | VLAN ID | Group IP Address | Member Ports |
| GLOBAL SETTINGS | 70 | | |

- 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 S | Settings | | | |
|---------------|------------|-------------------------------|-------------------|------------------|---------------------|
| D VLANS | VLAN ID | Router Ports Auto- Learned | Dynamic Port List | Static Port List | Forbidden Port List |
| SECURITY RMON | 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.

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

| SNMP | URC Settings | | |
|------|--------------|--------------|------|
| ACP | URC State | Member Ports | VLAN |
| LOG | Disabled | v [1 | 1 • |

- 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

| araknis | MLD SNOOPING | CLOUD SERVER: Connected | • System Time: 2016-02-29 20:03:29 | • System Uptime: Od 09:44:44 |
|--------------------|--------------------|-------------------------|------------------------------------|------------------------------|
| STATUS SYSTEM | Settings | | | |
| PORTS | Status | Enabled • Di | sabled | |
| BETTINGS SYSTEM | Version | ⊛ v1 | | |
| PORTS POE | Report Suppression | Enabled Di | sabled | |

- **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

| LINK AGGREGATION | VLAN Setting | s | | | |
|---------------------------|--------------|---------------------|---|------------|---|
| ACCESS MANAGEMENT | VLAN ID | MLD Snooping Status | | Fast Leave | |
| MAIN TENANCE PING TEST | 1 | Disabled | * | Disabled | • |

- 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.

| FILE MANAGEMENT | Group List | | |
|-----------------|------------|--------------|--------------|
| RESTART DEVICE | VLAN ID | IPv6 Address | Member Ports |
| LOG OUT | | | |

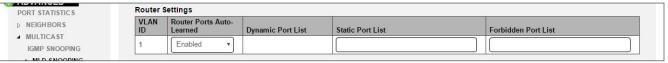
- VLAN ID VLAN identifier.
- IPv6 Address IP address for the multicast.
- Member Ports Switch ports that are part of the group.



Router Settings

Configure MLD router ports on the switch.





- 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.



| araknis | | CLOUD SERVER: Connected | System Time: 2016-04-28 11:26:28 | System Uptime: 9d 11:25:44 |
|------------------|------------------------|-------------------------|---|----------------------------|
| STATU S | GLOBAL SETTINGS | | | |
| PORTS | Settings | | | |
| | STP State | Enabled Disabled | | |
| SYSTEM | Force Version | MSTP T | | |
| PORTS | Configuration Name | D4:6A:91:32:F0:6E | (char : 0 ~ 32) | |
| POE VLANS | Configuration Revision | | (0-65535) | |
| LINK AGGREGATION | L | | | |

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

| 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 Priority Cost Port Forward Delay Maximum Age |

- 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 CIST SETTINGS | Priority | 32768 v (4096*N) | | | | | | |
| MST SETTINGS | Maximum Hop | 20 (1-40) | | | | | | |
| VLANS SECURITY | Forward Delay | 15 (4-30) | | | | | | |
| D RMON | Maximum Age | 20 (6-40) | | | | | | |
| D QOS D ACL | TX Hold Count | 6 (1-10) | | | | | | |
| D SNMP | Hello Time | 2 (1-10) | | | | | | |

- 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



CTD CICT Davit Catting and Manage

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

| NETWORKS | CIST SE | TTINGS | | | | | | | | | | | |
|-----------------------------|----------|----------|--------------------------------|----------------------------------|--------------------------|----------------------------------|--------------------------|----------------------------------|--------------------------|------------------------|------------|------------|-------------|
| STATUS SYSTEM | Port Set | tings | | | | | | | | | | | |
| PORTS BETTINGS SYSTEM | Port | Priority | Path Cost Conf / Oper | Designated Root Bridge | External Root Cost | Regional Root Bridge | Internal Root Cost | | Edge Port Conf / Oper | P2P MAC Conf / Oper | Port Role | Port State | Mig Star |
| PORTS POE | 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 Ves | Auto v /Yes | Designated | Forwarding | (|
| VLANS | 2 | [120 - | | 0/0/ | | 0/0/ | | 0/0/ | Yes v | Auto v | Disabled | Disabled | |

- 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.

| Linuxa EZ | CTD MCT Instance Cattings Manu | |
|------------|--------------------------------|--|
| Figure 53. | STP MST Instance Settings Menu | |

| araknis, | MST SET | TINGS | | | CLOUD SERVER: Connected | System Time: 2016 | -03-02 09:08:06 | System Uptime: | 1d 22:49:2 |
|---------------------------|----------|-----------|----------|---|-------------------------|--------------------|------------------|----------------|------------|
| STATUS SYSTEM PORTS | Instance | Settings | D.L. IV | _ | | | | | |
| 1.7360 | MSTID | VLAN List | Priority | | Regional Root Bridge | Internal Root Cost | Designated Bridg | je Root Port | |
| | 1 | 1-4094 | 32768 | • | -/ | 0 | / | - | |
| PORTS | 2 | 1-4094 | 32768 | • | -/ | 0 | / | | |
| POE VLANS | 3 | 1-4094 | 32768 | • | -/ | 0 | / | = | |
| LINK AGGREGATION | | 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.



| D QOS | Port Settings | | | | | | | | | | | | |
|-------------|---------------|------|----------|--------------------------------|-------------------------|-----------------------|----------------------|--------------|---------------|--|--|--|--|
| ⊳ SNMP | MST ID | Port | Priority | Internal Path Cost Conf / Oper | Regional Root Bridge | Internal Root Cost | Designated Bridge | Port Role | Port State | | | | |
| LACP LOG | 1 | 1 | 128 💌 | /20000 | -/ | - | _/ | - | - | | | | |
| Q Search | 1 • | 2 | 128 🔹 | 0 /20000 | / | - | / | | - | | | | |
| | 1 • | 3 | 128 🔹 | 0 /20000 | / | - | / | | - | | | | |
| | 1 • | 4 | 128 • | 0 /200000 | / | - | / | | | | | | |
| | 1 • | 5 | 128 🔻 | | / | - | / | | - | | | | |

- 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.

| araknis | 802.10 | | CLOUD SERVER: Conn | ected (System Time: 2016-03-02 09:17:12 | System Uptime: 1d 22:58:30 |
|---------------------------|--------|---------|--------------------|---|----------------------------|
| STATUS SYSTEM PORTS | VLAN S | ettings | | | |
| PORTS | VID | Name | Tagged Port | Untagged Port | Delete |
| BETTINGS SYSTEM | 1 | default | | 1-8,SFP1-SFP2,LAG1-LAG8 | |
| PORTS | | | | | Add |

- 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.



| VLANS | PVID Settin | gs | | | | |
|---------------------------|-------------|------|---------------|---|-------------------|---|
| LINK AGGREGATION | Port | PVID | Accept Type | | Ingress Filtering | |
| ACCESS MANAGEMENT | 1 | 1 | Untagged Only | • | Enabled | * |
| MAIN TENANCE PING TEST | 2 | 1 | Untagged Only | | Enabled | • |
| TRACE ROUTE | 3 | 1 | Untagged Only | * | Enabled | • |
| FILE MANAGEMENT | 12 | | | | C | |

- 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

| araknis | | CLOUD SERVER: Connected | System Time: 2016-03-02 09:17:47 | • System Uptime: 1d 22:59: |
|---------------------------|---------------|-------------------------|---|----------------------------|
| STATUS SYSTEM | PRIVATE VLANS | Private | | |
| PORTS | 1 | | | |
| | 2 | | | |
| SYSTEM | 3 | | | |
| PORTS | 4 | - | | |
| VLANS | 5 | | | |
| LINK AGGREGATION | 6 | | | |
| ACCESS MANAGEMENT | 7 | | | |
| MAIN TENANCE PING TEST | 8 | | | |
| TRACE BOUTE | | | | |

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



Advanced VLANs – Voice VLANs

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

General Settings

Note - In order to configure a new voice VLAN, you must first create a new VLAN. The default VLAN cannot be used. See:

- Section "14 VLAN Settings (Basic Port-Based)" on page 31, or
- Section "Advanced VLANs 802.1Q VLANs" on page 61

Figure 58. Voice VLANs Settings

| âraknis, | | CLOUD SERVER: Connected | () System Time: 2016-03-02 09:18:30 | System Uptime: 1d 22:59: |
|---------------------------|----------------------|-------------------------|-------------------------------------|--------------------------|
| STATUS SYSTEM PORTS | VOICE VLANS Settings | | | |
| | Voice VLAN State | Enabled Disable | ed | |
| SYSTEM | Voice VLAN ID | None * | | |
| PORTS | 802.1p Remark | Disabled | | |
| VLANS LINK AGGREGATION | Remark CoS/802.1p | 6 * | | |
| ACCESSMANAGEMENT | Aging Time | 1440 (30~65535)mi | n | |

- 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.

| PING TEST TRACE ROUTE | OUI Set | tings | | |
|--------------------------|---------|-------------|-------------|--|
| FILE MANAGEMENT | Index | OUI Address | Description | |
| RESTART DEVICE | 1 | 00:E0:BB | 3COM | |
| LOG OUT | 2 | 00:03:6B | Cisco | |
| ADVANCED | 3 | 00:E0:75 | Veritel | |
| PORT STATISTICS | 4 | 00:D0:1E | Pingtel | |
| MULTICAST | 5 | 00:01:E3 | Siemens | |
| STP VLANS | 6 | 00:60:B9 | NEC/Philips | |
| 802.1Q VLANS | 7 | 00:0F:E2 | H3C | |
| PRIVATE VLANS | 8 | 00:09:6E | Avaya | |
| VOICE VLANS SECURITY | | | | |

Figure 59. Voice VLANS OUI Settings

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

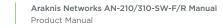
Port Settings

Configure port-based Voice VLAN settings.

Figure 60. Voice VLANS Port Settings

| | Port | State | | CoS Mode | | Operate Status |
|----|------|----------|---|----------|---|----------------|
| IP | 1 | Disabled | Ŧ | Src | Ŧ | - |
| | 2 | Disabled | ٣ | Src | v | - |

- 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

| araknis | PORT MIRROR | NG | | CLOUD SERVER: Connected | • System Time: 2016-03-02 09:18:57 | System Uptime: 1d 23 |
|--------------------|-------------|--------|------------------|-------------------------|------------------------------------|----------------------|
| STATUS SYSTEM | Session ID | Enable | Destination Port | Source TX Port | Source RX Port | Ingress State |
| PORTS | 1 | | 1 v | | | Disabled * |
| SETTINGS SYSTEM | 2 | | 1 v | | | Disabled • |
| PORTS POE | 3 | | 1 v | | | Disabled • |
| VLANS | 4 | | 1 v | | | Disabled T |

- 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.



| araknis | | CLOUD SERVER: Connected | • System Time: 2016-03-02 09:19:36 | System Uptime: 1d 23:00:5 |
|----------------------------------|---------------------------------|-------------------------|------------------------------------|---------------------------|
| STATUS SYSTEM | 802.1X 802.1x Global Setting | | | |
| | State | Enabled Disabled | | |
| SYSTEM PORTS | Guest VLAN | Disabled | | |
| POE VLANS LINK AGGREGATION | Guest VLAN ID | None v | | |

- 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.



| ACCESS MANAGEMENT | Port Set | ttings | | | | | | | |
|--------------------------|----------|------------|------------------|----------------------------|-----------------|----------------------|--------------|----------------------|------------|
| 🤗 MAIN TENANCE | Port | Mode | Reauthentication | Reauthentication period | Quiet Period | Supplicant Period | Max Retry | Authorized Status | Guest VLAN |
| PING TEST TRACE ROUTE | 1 | Disabled • | Enabled • | 3600 | 60 | 30 | 2 | AUTH_INITIALIZE | Enabled • |
| FILE MANAGEMENT | 2 | Disabled | Enabled | 3600 | 60 | 30 | | | Enabled |

- **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.





- 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.

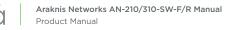
29 - Security - Radius Server

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 Se | rver Menu |
|------------|-----------|-----------|
|------------|-----------|-----------|

| araknis | RADIU | JS SERVER | | CLOUD SE | RVER: Connected | System Time: | 2016-03-02 09:20:07 | System U | ptime: 1d 23:01:3 |
|---------------------------------|-------|-----------|-----------------|----------------------------|-----------------|--------------|---------------------|--------------|-------------------|
| STATUS SYSTEM PORTS | | Server IP | Authorized Port | Key String char: 0 ~ 6. | Timeout Reply | Retry 3 | Server Priority | Dead Timeout | Delete |
| SYSTEM PORTS POE VLANS | | | | | | | | Apr | Add |

- 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

Figure 66. Global DOS Settings Menu

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

Global Settings

| SYSTEM PORTS | Global Settings | |
|---------------------------------------|---------------------------|---------------------|
| | DMAC = SMAC | Enabled 🔻 |
| SETTINGS SYSTEM | Land | Enabled * |
| PORTS | UDP Blat | Enabled |
| VLANS | TCP Blat | Enabled |
| LINK AGGREGATION ACCESS MANAGEMENT | POD | Enabled |
| MAINTENANCE | IPv6 Min Fragment | Enabled • |
| PING TEST TRACE ROUTE | Bytes | (1240) (0-65535) |
| FILE MANAGEMENT | ICMP Fragments | Enabled * |
| RESTART DEVICE | IPv4 Ping Max Size | Enabled |
| ADVANCED | IPv6 Ping Max Size | Enabled |
| PORT STATISTICS | Ping Max Size Setting | 512 Bytes (0-65535) |
| MULTICAST | Smurf Attack | Enabled |
| D STP | Netmask Length | 0 (0-32) |
| ▲ SECURITY | TCP Min Hdr Size | Enabled |
| PORT MIRRORING 802.1X | TCP Min Hdr Bytes | 20 (0-31) |
| RADIU S SERVER | TCP-SYN(SPORT<1024) | Enabled v |
| DOS PORT SECURITY | Null Scan Attack | Enabled |
| MAC ADDRESS FILTER | X-Mas Scan Attack | Enabled |
| RMON D QOS | TCP SYN-FIN Attack | Enabled |
| D ACL | TCP SYN-RST Attack | Enabled |
| ▷ SNMP LACP | 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 | | | | |
|-----------|---------------|----------------|--|--|--|
| (Q Search | 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.

| araknis | DODT | SECURITY | CLOUD SERVER: Connected | • System Time: 2016-03-02 09:21:26 | System Uptime: 1d 23:02:5 |
|--------------------|------|------------|-------------------------|------------------------------------|---------------------------|
| STATUS SYSTEM | Port | SECORITY | Max MAC Address | _ | _ |
| PORTS | 1 | Disabled • | 256 | | |
| SETTINGS SYSTEM | 2 | Disabled • | 256 | | |
| PORTS | 3 | Disabled • | 256 | | |
| VLANS | 4 | Disabled • | 256 | | |
| LINK AGGREGATION | c | Dischlod | | | |

- 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 |
|------------|--------------------------|

| araknis | | ESS FILTER | 📥 CLOUD SI | RVER: Connected | • System Time: 2016-03-02 09:21:59 | System Uptime: | 1d 23:03:22 |
|---------------------------|----------|------------|------------|-----------------|------------------------------------|----------------|-------------|
| STATUS SYSTEM PORTS | MAC ADDR | VID | | MAC Address | | Delete | |
| | IIIdex | 1 | • • | XXXXXXXXXXXXXXX | | | |
| PORTS | | | | | | Ade | 1 |
| VLANS | | | | | | Apply Cance | 1 |

- 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

| araknis | EVENTLIST | | CLOUD SE | RVER: Connected | System Time: 2016- | 03-02 09:22:30 | System Uptime: 1d 23 |
|---------------------------|-----------|------------|-----------|-----------------|--------------------|----------------|----------------------|
| STATUS SYSTEM PORTS | Index | Event Type | Community | Description | Last Time Sent | Owner | Delete |
| | 1 ~ 65535 | Log v | private v | char : 0 ~ 127 | | char : 0 ~ 32 | <u></u> |

- 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

| araknis | | CLOUD SERVER: C | onnected (System Time: 2016-03-0 | 2 09:22:59 O System Uptime: 1d 23:04:23 |
|---------------------------|-----------------|-----------------|----------------------------------|--|
| STATUS SYSTEM PORTS | EVENT LOG TABLE | 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

| araknis | ALAR | A LIST | | 📥 CI | LOUD SERVER: Co | nnected | 🕒 System Tin | ne: 2016-03-02 09 | 9:23:24 💽 S | ystem Upt | ime: 1d 23:04: |
|---------------------------------------|------|--------|--------------------|--------------------|-----------------|---------------------|----------------------|-------------------|---------------|-----------|----------------|
| STATUS SYSTEM PORTS | | | Sample Variable | Sample Interval | Sample Type | Rising Threshold | Falling Threshold | Rising Event | Falling Event | Owner | Delete |
| SETTINGS SYSTEM PORTS DOE | 1. | 1 | DropEv: • | 1 ~ 2147483 | Absolut | 0~214 | 0~214 | | | cha | لللاً Add |

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



RMON - History List

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

Figure 73. History List

| araknis | HISTORY LIST | | CLOUD SERVER: Connected | System Time: 2016-03 | -02 09:23:50 🕓 Syste | em Uptime: 1d 23:05:13 |
|------------------|--------------|-------------|-------------------------|----------------------|----------------------|------------------------|
| STATUS SYSTEM | Index | Sample Port | Bucket Requested | Interval | Owner | Delete |
| | 1 ~ 65535 | 1 • | 1~50 | 1 ~ 3600 | char : 0 ~ 32 | <u> </u> |
| SYSTEM | | ÷ | ak a | A. | ÷. | Add |

- 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

| | HISTORY LOG TABLE | CLOUD SERVER: Connecte | d O System Time: 2016-03-02 09:24:16 | () System Uptime: 1d 23:05:40 |
|------------------|----------------------|------------------------|---|-------------------------------|
| STATUS SYSTEM | Select History Index | none v | Refresh | |
| PORTS | | | | |

- 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

| araknis. | | CLOUD SERVER: Connected | • System Time: 2016-03-02 09:25:23 | System Uptime: 1d 23:06:40 |
|------------------|-------------------|-------------------------|------------------------------------|----------------------------|
| STATUS SYSTEM | GLOBAL SETTINGS | Enabled Oisabled | | |
| | Scheduling Method | Strict Priority * | | |
| SYSTEM | Trust Mode | 802.1p * | | |

- 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.





- 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.



| araknis | DSCP MAPPING | CLOUD SERVER: Connected | ⊙ System Time: 2016-03-02 09:26:39 | () System Uptime: 1d 23:08:02 |
|------------------|--------------|-------------------------|------------------------------------|-------------------------------|
| STATUS SYSTEM | DSCP | Queue | | |
| PORTS | 0 | | | |

- **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 | ble |
|------------------------------------|-----|
|------------------------------------|-----|

| Taraknis | PORT SETTINGS | | CLOUD SERVER: Connected | • System Time: 2016-03-02 09:27:10 | System Uptime: 1d 23:08:33 |
|------------------|---------------|-----------|-------------------------|------------------------------------|----------------------------|
| STATUS SYSTEM | Port | CoS Value | | Trust | |
| PORTS | 1 | | | 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.

| Bana Mathematic Control Table | Figure 79. | Bandwidth | Control | Table |
|-------------------------------|------------|-----------|---------|-------|
|-------------------------------|------------|-----------|---------|-------|

| araknis | BANDV | VIDTH CONTROL | CLOUD SERVER: Connect | ed Osystem Time: | 2016-03-02 09:27:38 | • System Uptime: 1d 23:09:07 |
|---------|-------|-------------------|-----------------------|-------------------|---------------------|------------------------------|
| | Port | Ingress | Ingress Rate (kbps) | Egress | Egress Rate (kbps) | |
| DODTO | FOIL | ingress | ingress rate (rups) | Lyless | Egress Rate (Rops) | |
| PORTS | 1 | Disabled v | Off | Disabled v | Off | |
| | 2 | Disphled - | lo# | Dischlod T | 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.



| NETWORKS | STORM | CONTROL | | | |
|--------------------------|-------|------------|------------------|--------------------------|------------------------|
| STATUS SYSTEM | Port | Status | Broadcast (kbps) | Unknown Multicast (kbps) | Unknown Unicast (kbps) |
| PORTS | 1 | Disabled T | Off (10000) | Off (10000) | Off (10000) |
| | 2 | Disabled T | Cff (10000) | □ Off (10000) | Off (10000) |
| PORTS | 3 | Disabled • | Off (10000) | Off (10000) | Off (10000) |
| POE | 4 | Disabled • | Off (10000) | = Off (10000) | Gff (10000) |
| LINK AGGREGATION | 5 | Disabled • | Off (10000) | Off (10000) | Off (10000) |
| ACCESS MANAGEMENT | 6 | Disabled • | Off (10000) | Off (10000) | Off (10000) |
| | 7 | Disabled • | Gff (10000) | □ Off (10000) |) (Off (10000) |
| PING TEST TRACE ROUTE | 8 | Disabled • | Off (10000) | C Off (10000) | 🗆 Off (10000) |
| FILE MANAGEMENT | SFP1 | Disabled • | Off (10000) | G (10000) | Gff (10000) |
| RESTART DEVICE | SFP2 | Disabled • | Off (10000) | Cff (10000) | 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.

| Ξ | Note - | The ACI | feature | is | only | found | in | 310 | series | switches. |
|---|--------|---------|---------|----|--------|-------|----|-----|--------|-------------|
| | | | | 13 | Officy | round | | 510 | 301103 | 3001001003. |

ACL - MAC ACL

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

Figure 81. MAC ACL List

| araknis | MAC AC | L | | CLOOD | SERVER: Connected | O system | Time: 2016-05- | 2 11.10.04 | | System Upti | 10. 00 |
|---|---------|---------------|----------|--------------------------|-------------------------|---------------------|--------------------|------------|-----------------|-------------|--------|
| STATUS SYSTEM PORTS | MAC AC | L List | | | | | | | | | |
| | Index | Name | | | | | | | | | Delete |
| SYSTEM | 1 | ACL1 | | | | | | | | | 匬 |
| PORTS | | char : 1 ~ 32 | | | | | | | | | Ŵ |
| VLANS LINK AGGREGATION ACCESS MANAGEMENT | MAC AC | E List | | | | | | | | 1 | Add |
| MAIN TENANCE | ACL Nar | ne Sequence | Action | Destination MAC Value | Destination MAC Mask | Source MAC Value | Source MAC Mask | VLAN ID | 802.1p Value | Ethertype | Delete |
| | | | | (| | Any | | | Any | (A= | 圎 |
| TRACE ROUTE FILE MANAGEMENT | ACL1 | | Permit • | Any | Any | Any | Any | Any | Any | Any | ш |
| TRACE ROUTE | ACL1 | <u>•</u> | Permit v | Any | Any | Any | Any | Any | Any | | Add |
| TRACE ROUTE FILE MANAGEMENT RESTART DEVICE | ACL1 | <u>•</u> | Permit 🔻 | Any | Any | Any | Any | Any | | | Add |
| TRACE ROUTE FILE MANAGEMENT RESTART DEVICE LOG OUT | ACL1 | <u> </u> | Permit 🔻 | Any | Any | Any | Any | Any | | | Add |

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 Edit | to |
|----------------------------------|----|
|----------------------------------|----|

| LINK AGGREGATION | MAC ACE Editor | | | |
|--------------------------|-------------------------|--------|---|-----------|
| ACCESS MANAGEMENT | | | | |
| MAIN TENANCE | ACL Name | ACL1 | • | |
| PING TEST TRACE ROUTE | Sequence | | (Range: 1 - 2147483647, 1 is first processed) | |
| FILE MANAGEMENT | Action | Permit |] | |
| RESTART DEVICE | Destination MAC Address | Any | <u>j</u> | |
| ADVANCED | Source MAC Address | Any |] | |
| PORT STATISTICS | VLAN ID | | (Range: 1 - 4094) | |
| D NEIGHBORS | 802.1p Value | |) (Range: 0 - 7) | |
| D MULTICAST | Ethertype Value (Hex) | | (Range: 0600~FFFF) | |
| D VLANS | | | | OK Cancel |
| > SECURITY | | | | ORCOARCE |

- 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.



| araknis | | _ | | | - | CLOUD SE | RVER: Conne | ected 🕓 S | ystem Tim | e: 2016-03-16 | 10:55:1 | 16 🤆 |) System | n Uptime | : 15d 23 |
|--|----------|----------------------|--------|----------|-------------------------|----------|---------------------------|------------------------|-------------------------|---------------------------|-------------|------|----------|--------------|---------------|
| STATU S SYSTEM PORTS | IPV4 AC | | | | | | | | | | | | | | |
| SETTINGS SYSTEM PORTS | Index | Name | 32 | | | | | | | | | | | | elete ÎÎÎ |
| POE | | | | | | | | | | | | | | 4 | Add |
| | IPv4 ACE | EList | | | - | - | | | - | | | | | | Add |
| POE VLANS LINK AGGREGATION | ACL | E List Sequence A | Action | Protocol | Source IP Address | | Destination IP Address | Destination IP Mask | Source Port Range | Destination Port Range | Flag Set | DSCP | | ICMP | Delete |
| POE VLANS LINK AGGREGATION ACCESS MANAGEMENT MAINTENANCE PING TEST TRACE ROUTE | ACL | | Action | Protocol | IP | IP | | | Port | Destination Port Range | Flag Set | DSCP | | ICMP Code | _ |
| POE VLANS LINK AGGREGATION ACCESS MANAGEMENT MAINTENANCE PING TEST | ACL | | Action | Protocol | IP | IP | | | Port | Destination Port Range | Flag Set | DSCP | ICMP | ICMP Code | Delete |

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

| VLANS | IPv4 ACE Editor | |
|---------------------------|----------------------------|---|
| LINK AGGREG ACCESS MAN | A OL NI | |
| 🧭 MAIN TENAN | CE Sequen | (Range: 1 - 2147483647, 1 is first processed) |
| PING TEST TRACE ROUTE | Acti | permit v |
| FILE MANAGE | IENT Protoc | ol Select from list v I IPv4:ICMP v |
| RESTART DEV LOG OUT | CE Source IP Addre | ss User Defined • |
| | Source IP Address Val | Je |
| PORT STATIST | CS Source IP Ma | sk [? |
| ▶ MULTICA ST | Destination IP Addre | ss User Defined v |
| D STP D VLANS | Destination IP Address Val | |
| > SECURITY | Destination IP Ma | sk 🛛 🕜 |
| ⊳ RMON ⊳ QOS | Type of Servi | CE DSCP to match • (Range: 0 - 63) |
| ▲ ACL | ICMP Typ | e: Select from list v Echo Reply v |
| MAC ACL • IPV4 ACL | ICMP Co | de User Defined v (Range: 0 - 255) |
| IPV6 ACL ACL BINDI | | ОКС |

- 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:Rout, IPv6Frag, RSVP, IPv6:ICMP, OSPF, PIM, or L2TP.
 - **Protocol ID -** Enter the identifier for the protocol.
- Source/Destination IP Address Select whether to monitor Any or a User Defined address.
- Source/Destination IP Address Value Enter the address to monitor. Only visible when monitoring a User Defined address.
- Source/Destination IP Mask Subnet mask to monitor. Use this field to filter multiple addresses within a range. Only visible when monitoring a User Defined address.
- Source/Destination Port/Port Range Enter a port or ports to monitor.
- **Type of Service -** Select Any or DSCP to match (then enter range).
- ICMP Type Select the IMCP type to monitor:
 - Any No ICMP monitoring.
 - Select from list Select the ICMP type to monitor. Options: EchoReply, Destination Unreachable, Source Quench, Echo Request, Router Advertisement, Router Solicitation, Time Exceeded, Timestamp, Timestamp Reply, or Traceroute.
 - Protocol ID Enter the identifier for the protocol
- ICMP Code
 - Any No ICMP code monitoring.
 - User Defined Enter the code value to be monitored.
- **OK -** Click to accept the new settings and return to the IPv4 ACL ACE List.
- Cancel Click to reject the new settings and return to the IPv4 ACL ACE List.



ACL - IPV6 ACL

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



| araknis | | | | | - | CLOUD S | ERVER: Conne | ected 🕑 9 | System Tin | ne: 2016-03-16 | 6 10 :55: | 51 (| Syste | m Uptim | e: 15d 23:3 |
|--|-------------------|-------------------|----|----------|-------------------------|----------------------------------|---------------------------|-----------|-------------------------|----------------|------------------|------|-------|---------|---------------|
| STATU S SYSTEM PORTS | IPV6 AC | | | | | | | | | | | | | | |
| SETTINGS SYSTEM PORTS POE VLANS LINK AGGREGATION ACCESS MANAGEMENT | Index IPv6 ACE | Name char:1~32 | | | | | | | | | | | | | Delete |
| ACCESS MANAGEMENT MAIN TENANCE PING TEST TRACE ROUTE FILE MANAGEMENT RESTART DEVICE | ACL Name | Sequence Act | on | Protocol | Source IP Address | Source IP Prefix Length | Destination IP Address | | Source Port Range | Destination | Flag Set | DSCP | ICMP | 17 | Delete Add |
| ADVANCED | | | | | | | | | | | | | Арр | oly Ca | ncel |

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

| POE | IPv6 ACE Editor | |
|--|---|---|
| VLANS LINK AGGREGATION ACCESS MANAGEMENT | ACL Name acl3 | Y |
| MAIN TENANCE | Sequence (Range | e: 1 - 2147483647, 1 is first processed) |
| PING TEST TRACE ROUTE | Action | |
| FILE MANAGEMENT | Protocol Select from list v TCP | · • |
| RESTART DEVICE LOG OUT | Source IP Address | |
| | Source IP Address Value | (XXCXXC::XXCXXX) |
| PORT STATISTICS | Source IP Prefix Length | (Range: 0 - 128) |
| NEIGHBORS MULTICAST | Destination IP Address User Defined | |
| ⊳ STP | Destination IP Address Value | (XXCXXCCXXX) |
| ▷ VLANS ▷ SECURITY | Destination IP Prefix Length | (Range: 0 - 128) |
| D RMON | Source Port: Range | (Range: 0 - 65535) |
| D QOS ACL | Destination Port: Range v | (Range: 0 - 65535) |
| MAC ACL IPV4 ACL | TCP Flags Urg Don't Care Ack Rst Don't Care Svn | Don't Care Psh Don't Care Fin Don't Care Fin Don't Care |
| IPV6 ACL ACL BINDING | Type of Service DSCP to match * | (Range: 0 - 63) |

- 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.



| araknis | | | | CLOUD SERVER: Connected | d 🕒 System Time: | 2016-03-16 10:57:01 | System Uptime: 15d 23 |
|---------------------------------------|------|---------|---|-------------------------|------------------|---------------------|-----------------------|
| STATU S | | NDING | | | | | |
| | Port | MAC ACL | | IPv4 ACL | | IPv6 ACL | |
| PORTS | 1 | (none) | * | (none) | * | (none) | • |
| SETTINGS SYSTEM | 2 | (none) | | (none) | • | (none) | • |
| PORTS POE | 3 | (none) | v | (none) | v | (none) | • |
| VLANS | 4 | (none) | • | (none) | * | (none) | • |
| LINK AGGREGATION ACCESS MANAGEMENT | 5 | (none) | * | (none) | * | (none) | * |
| MAIN TENANCE | 6 | (none) | * | (none) | • | (none) | • |
| PING TEST TRACE ROUTE | 7 | (none) | • | (none) | • | (none) | • |
| | 8 | (none) | • | (none) | * | (none) | • |
| RESTART DEVICE LOG OUT | SFP1 | (none) | * | (none) | * | (none) | v |

• 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 | | |
|------------|------------------|-----------------|--|---|
| 1 | araknis | GLOBAL SETTINGS | CLOUD SERVER: Connected O System Time: 2016-03-16 10:57 | 7:39 O System Uptime: 15d 23:39:39 |
| S | TATU S (STEM | Settings | | |
| | ORTS | SNMP State | Enabled Disabled | |
| S | ETTINGS (STEM | Engine ID | 8000B55303D46A9132F06E | Default |
| | ORTS DF | | (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.



| LINK AGGREGATION ACCESS MANAGEMENT | Trap Settings | | 2 | 15 | × | 12 | 5 | | |
|--|---------------|--------------|-------------|-------------------|-----------|-----|---------|-------|--------|
| MAIN TENANCE PING TEST | | SNMP Version | Notify Type | Community Name | User Name | UDP | Timeout | Retry | Delete |
| TRACE ROUTE FILE MANAGEMENT RESTART DEVICE | char : 1 ~ | <u>v1</u> | 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

| LOG OUT | Remote Engine ID List | | |
|--|-----------------------|------------------|--------|
| PORT STATISTICS | Server IP | Remote Engine ID | Delete |
| NEIGHBORS MULTICAST | x.x.x.x/xxixxiixxixx | 10~64 hex | |
| D STP | | | 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

| araknis | LISTS | 📥 CLOUD | SERVER: Connected | 🕒 System Time | 2016-03-16 11:06:5 | 5 🕒 System Upt | me: 15d 23:48:55 |
|---------------------------|---------------|---------------|-------------------|---------------|--------------------|----------------|------------------|
| STATUS SYSTEM PORTS | Group List | | | | | | |
| | Group Name | Security Mode | Security Level | Read View | Write View | Notify View | Delete |
| SYSTEM PORTS | char : 1 ~ 30 | v1 • | No Auth 🔻 | all 🔻 | None • | None • | Û |
| POE | | | | | | | Add |

- 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

| ACCESS MANAGEMENT | | | | | |
|--------------------------------|---------------|----------------|---------------|------------|--------|
| MAINTENANCE | View Name | Subtree OID | Subtree Mask | View Type | Delete |
| PING TEST | all | .1 | all | Included | |
| TRACE ROUTE FILE MANAGEMENT | char : 1 ~ 30 | max level : 20 | char : 1 ~ 20 | Included • |) 🛍 |

- 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 O (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

| PORT STATISTICS | Community Name | Community Mo | ode | Group Name | View Name | | Access Rights | | Delete |
|-------------------------|----------------|--------------|-----|------------|-----------|----|---------------|---|--------|
| NEIGHBORS MULTICAST | private | Basic | * | (v | all | •) | Read Write | * | Ŵ |
| D STP | public | Basic | • | Ţ. | all | • | Read Only | • | Ŵ |
| D VLANS | char : 1 ~ 20 | Basic | * | | all | • | Read Only | • | ŵ |

- 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

| GLOBAL SETTINGS | | | | Authenitication | Authenitication | Encryption | | |
|-----------------|--------------|------------|----------------|-----------------|-----------------|------------|----------------|--------|
| LISTS | User Name | Group Name | Privilege Mode | Protocol | Password | Protocol | Encryption Key | Delete |
| ACP | char: 4 ~ 30 | | No Auth | None 🔻 | char: 8 ~ 32 | None v | char : 8 ~ 64 | 匬 |

- 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.



| araknis, | | ETTINGS | CLOUD SERVER: Conner | System Time: 2016-03-16 11:08:44 | () System Uptime: 15d 23:50 |
|-----------------------------------|----------|---------|----------------------|--|-----------------------------|
| STATU S SYSTEM PORTS | Settings | | 32768 (1~ | | |
| SETTINGS SYSTEM PORTS | System | | 32/00 (1~ | 65535) | |
| POE | Port | Timeout | | | |
| VLANS LINK AGGREGATION | 1 | Slow | | | • |
| ACCESSMANAGEMENT | 2 | Slow | | | |
| MAIN TENANCE PING TEST | 3 | Slow | | | • |
| TRACE ROUTE | 4 | Slow | | | |
| FILE MANAGEMENT RESTART DEVICE | 5 | Slow | | | * |
| LOG OUT | 6 | Slow | | | • |
| | 7 | Slow | | | * |
| NEIGHBORS | 8 | Slow | | | ▼ |
| > MULTICAST > STP | SFP1 | Slow | | | • |
| VLANS | SFP2 | Slow | | | |
| SECURITY | | | | | |
| D RMON | | | | | |
| D QOS D ACL | | | | | Apply Cancel |

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.

| araknis | LOG | CLOUD SERVER: Connected | • System Time: 2016-03-16 11:09:44 | System Uptime: 15d 23:51:43 |
|-------------------|-----------------|-------------------------|------------------------------------|------------------------------------|
| STATU S SYSTEM | Settings | | | |
| PORTS | Logging Service | Enabled Disabled | | |

• 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

| POE | Local Logging | | | | | | | |
|------------------|---------------|-------|-------|-------|---------|--------|------|-------|
| VLANS | EMERG | ALERT | CRIT | ERROR | WARNING | NOTICE | INFO | DEBUG |
| LINK AGGREGATION | Yes • | Yes v | Yes • | Yes v | Yes v | No v | No v | No v |

• 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

| TRACE ROUTE | IP/Hostname | Server Port | EMERG | ALERT | CRIT | ERROR | WARNING | NOTICE | INFO | DEBUG | Facility | Delete |
|-----------------|---------------|-------------|-------|-------|------|-------|---------|--------|------|-------|----------|--------|
| FILE MANAGEMENT | char : 1 ~ 63 | 514 | N • | N • | N v | N * | No 🔻 | • | N . | N . | loc 🔻 | Ŵ |
| RESTART DEVICE | | | | | | | | | | | | Add |

- 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: localO-local7. Default: local O
- 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 | |
|------------|-------------------------------------|----|
| Figure 2. | Mounting Methods | |
| Figure 3. | Connection Diagram | |
| Figure 4. | EIA/TIA 568B Termination Pattern | 11 |
| Figure 5. | PoE Calculation Example | |
| Figure 6. | OvrC Operation Diagram | 13 |
| Figure 7. | Interface Layout | 19 |
| Figure 8. | Apply Button | 10 |
| Figure 9. | System Information and Port Status | 20 |
| Figure 10. | Events Log | 21 |
| Figure 11. | Port Status | |
| Figure 12. | System Information Settings | 23 |
| Figure 13. | IP Address Settings Menu | 24 |
| Figure 14. | Date and Time Settings, UPnP | 25 |
| Figure 15. | Recommended System Settings | 26 |
| Figure 16. | Jumbo Frame and Basic Port Settings | 27 |
| Figure 17. | Advanced Port Settings | 28 |
| Figure 18. | PoE Settings Menu | 29 |
| Figure 19. | PoE Settings Menu | |
| Figure 20. | VLAN Settings | |
| Figure 21. | Access and Trunk Port Selection | |
| Figure 22. | Configuring Ports in a VLAN | 32 |
| Figure 23. | Link Aggregation Settings Menu | 33 |
| Figure 24. | Access Management Menu Page | 35 |
| Figure 25. | Ping Test Page | 36 |
| Figure 26. | Successful Ping Test Result | 37 |
| Figure 27. | Failed Ping Test Result | 37 |
| Figure 28. | Trace Route Test Page | 38 |
| Figure 29. | Trace Route Result | 39 |
| Figure 30. | File Management Menu | |
| Figure 31. | Dual Image Menu | |
| Figure 32. | Restart Page | |
| Figure 33. | Log Out Page | 42 |
| Figure 34. | Detailed Port Statistics | 44 |
| Figure 35. | Neighbors MAC Address Table | 46 |
| Figure 36. | LLDP Information | 47 |
| Figure 37. | LLDP Settings | 48 |
| Figure 38. | LLDP Remote Device Menu | 48 |
| Figure 39. | IGMP Snooping Settings | 49 |
| Figure 40. | IGMP Snooping VLAN Settings | 49 |
| | | |



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



| MAC ACL ACE List Editor | |
|-------------------------------------|--|
| IPv4 ACL Menu Page | |
| IPv4 ACL ACE Editor | |
| IPv6 ACL Menu Page | |
| IPv4 ACL ACE Editor | |
| ACL Binding Menu Page | |
| SNMP Global Settings | |
| SNMP Trap Settings | |
| SNMP Remote Engine ID List Settings | |
| SNMP Group List | |
| SNMP View List | |
| SNMP Community List | 88 |
| SNMP User List | 88 |
| Advanced LACP Settings | |
| Log Settings | |
| Local Logging | |
| Remote Logging | |
| | IPv4 ACL Menu Page IPv4 ACL ACE Editor IPv6 ACL Menu Page IPv4 ACL ACE Editor ACL Binding Menu Page SNMP Global Settings SNMP Global Settings SNMP Trap Settings SNMP Remote Engine ID List Settings SNMP Group List SNMP View List SNMP View List SNMP Community List SNMP User List Advanced LACP Settings Log Settings Log Settings |

39 - AN-210-SW Specifications

| | | 210-8P | 210-16P | 210-24P |
|-----------------------------|---------------------------------|-----------|-----------|-----------|
| | Port | | | |
| 10/100/1000Base RJ-45 Ports | | 8 | 16 | 24 |
| 1000Base SFP | | 2 | 2 | 2 |
| PoE Ports | | 8 | 16 | 24 |
| | Physical Configuration | - | - | |
| Flash Memory | | 16MB | 16MB | 16MB |
| SDRAM | | 128MB | 128MB | 128MB |
| Packet Buffer | | 512KB | 512KB | 512KB |
| | ESD & Surge | 012110 | 012110 | 012110 |
| Cable ESD | 200 0 00.90 | 15Kv | 15Kv | 15Kv |
| Air ESD | | +/- 8Kv | +/- 8Kv | +/- 8Kv |
| Contact ESD | | +/- 6Kv | +/- 6Kv | +/- 6Kv |
| RJ-45 Surge | | +/- 1.6Kv | +/- 1.6Kv | +/- 1.6Kv |
| PSU Surge | | +/- 2.5Kv | +/- 2.5Kv | +/- 2.5Kv |
| | Performance | | | · · |
| MAC Address Table Size | | 8K | 8K | 8K |
| Switching Capacity | | 20Gbps | 36Gbps | 52Gbps |
| Forwarding Rate | | 14.8Mbps | 26.8Mbps | 38.7Mbps |
| | PoE Features | | | |
| 802.3af/at Compliant | | х | х | х |
| Max Power Output per Port | | 30W | 30W | 30W |
| PoE Power Budget | | 65W | 130W | 190W |
| PD Classification | | х | х | х |
| Power Management | Enable/Disable per port | х | х | х |
| C C | Priority Setting per port | х | х | х |
| | Overloading Protection per port | х | х | х |
| | Power level setting per port | х | х | х |
| | L2 Features | | , | |
| HOL Blocking | Head-of-line blocking | х | х | х |
| Flow Control | 802.3x, Back Pressure | X | x | X |
| Forwarding Mode | Store-and-forward | х | х | х |
| Energy Efficient Ethernet | IEEE 802.3az | х | х | х |
| Spanning Tree | 802.1D (STP) | x | x | x |
| | 802.1w (RSTP) | х | х | х |
| | 802.1s (MSTP) | х | х | х |
| VLAN | 802.1Q | х | х | х |
| | VLAN Group | х | х | х |
| | Port-based VLANs | х | х | х |
| | Private VLANs | - | - | - |
| | QinQ | - | - | - |
| | Protocol-based VLAN | - | - | - |
| | Voice VLAN | х | х | х |
| Link Aggregation | Static, 802.3ad LACP | х | х | х |
| | Max ports per group | 8 | 8 | 8 |
| | Max Group | 8 | 8 | 8 |
| Multicast Snooping | IGMP Snooping v1/v2/v3; MLD | х | х | x |
| | Snooping v1/v2 | | | |
| | IGMP Querier | х | х | х |
| | IGMP Immediate Leaxe | x | x | x |
| Storm Control | Broadcast/UnKnown Multi- | X | x | x |
| | cast/Unknown Unicast | | | |
| Jumbo Frame Support | | 9k | 9k | 9k |
| | | | | |



| | | 210-8P | 210-16P | 210-24P |
|--|----------------------------|-----------------------------|-----------------------------|----------------------|
| | QoS Features | | | |
| Number of priority queues | | х | х | х |
| Rate Limiting | Ingress | Х | х | х |
| 5 | Egress | х | х | х |
| DiffServ (RFC2474) | | x | x | x |
| Scheduling | WRR | x | x | x |
| Seriedaning | Strict | X | X | x |
| | Hybrid | - | - | - |
| CoS | 802.1p | х | х | x |
| | IP ToS Precedence | X | X | x |
| | IP DSCP | x | × | × |
| | Security | ~ | ~ | ~ |
| Dort Scourity (MAC based) | Security | × | , v | |
| Port Security (MAC-based) | | X | X | X |
| 802.1x | | Х | Х | X |
| ACL | L2 | - | - | - |
| | L3 | - | - | - |
| | L4 | - | - | - |
| IP Source Guard | | - | - | - |
| RADIUS | | х | х | х |
| TACACS+ | | - | - | - |
| HTTPS and SSL | | Х | х | х |
| SSH v2.0 | | Х | Х | х |
| MAC Filter | | Х | х | х |
| IP Filter | | - | - | - |
| | Management | | | |
| Management | CLI, Web, Telnet | х | х | х |
| Dual FW Images | | - | - | - |
| FW Upgrade | TFTP upgrade | х | х | х |
| | HTTP upgrade | X | X | x |
| Management Access Filtering | SNMP/Web/Telnet | X | X | x |
| SNMP | v1,v2c,v3 | x | × | × |
| | V1,V2C,V3 | | | |
| SNTP | | X | X | X |
| RMON (1,2,3 and 9 groups) | c | Х | Х | |
| DHCP | Server | - | - | |
| | Client | Х | Х | Х |
| | Relay | - | - | - |
| | Option82 | - | - | - |
| | Snooping | - | - | - |
| Exent log | local flash, remote serxer | Х | Х | Х |
| sFlow | | - | - | - |
| Port Mirroring | One to One, Many to One | Х | Х | х |
| Remote Ping | | Х | Х | х |
| LLDP (IEEE802.1ab) | | х | х | х |
| Cable Diagnostics | | х | х | х |
| UPnP | | X | x | x |
| | Environmental | | | |
| Dimensions | Inches (WxHxD) | 12.99 x 9.06 | 18.98 x 10.24 | 18.98 x 10.24 |
| | | x 1.75 | x 1.75 | x 1.75 |
| Davier Consult | | 100-240x | 100-240x | 100-240x |
| | | | | |
| Power Supply | | $A \subset E \cap / C \cap$ | $A \subset E \cap / E \cap$ | |
| Power Supply | | AC, 50/60 | AC, 50/60 | AC, 50/60 |
| | - b u u | AC, 50/60 Hz | AC, 50/60 Hz | AC, 50/60 Hz |
| Maximum Power Consumption | Watts | Hz | Hz | Hz |
| Maximum Power Consumption (Full PoE No PoE) | Watts | Hz 86.50 13.30 | Hz 162.08 21.31 | Hz 291.81 23.71 |
| Maximum Power Consumption | Watts | Hz | Hz | Hz |

40 - AN-310-SW Specifications

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

ପି

| | SPEC | 310-8P | 310-16P | 310-24P | 310-8 | 310-16 | 310-24 |
|-----------------------------------|---------------------------------------|--------------|--------------|-----------|--------------|--------------|-------------|
| | | | eatures | | | | |
| Number of priority queues | | x | x | x | х | х | Х |
| Rate Limiting | Ingress | х | x | X | X | X | х |
| | Egress | х | х | х | х | х | х |
| DiffSerx (RFC24 | 74) | х | х | х | х | х | х |
| Scheduling | WRR | х | х | х | х | х | х |
| | Strict | х | х | х | х | х | × |
| | Hybrid | - | - | - | - | - | - |
| CoS | 802.1p | х | х | х | х | х | х |
| | IP ToS Precedence | х | х | х | х | х | х |
| | IP DSCP | х | х | х | х | х | х |
| | | Sec | urity | | | | - |
| Port Security (M | AC-based) | х | х | х | х | х | х |
| 802.1x | | х | х | х | х | х | х |
| ACL | L2 | х | х | х | х | х | х |
| | L3 | x | х | х | х | х | х |
| | L4 | x | x | x | x | x | X |
| IP Source Guard | | - | - | - | - | - | - |
| | | × | × | × | × | × | × |
| RADIUS TACACS+ | | X | × - | × - | - X | X | - X |
| | | | | | | | |
| HTTPS and SSL | | x | x | x | x | X | X |
| SSH x2.0 | | x | × | x | × | X | X |
| MAC Filter | | х | х | х | х | х | х |
| IP Filter | | - | - | - | - | - | - |
| | | Manag | ement | - | | - | - |
| Management | CLI, Web, Telnet | х | х | х | х | х | х |
| Dual FW Images | | х | х | х | х | х | x |
| FW Upgrade | TFTP upgrade | х | х | х | х | х | х |
| | HTTP upgrade | х | х | х | х | х | х |
| Management | SNMP/Web/Telnet | х | х | х | х | х | х |
| SNMP | v1,v2c,v3 | х | х | х | х | х | х |
| SNTP | | х | х | х | х | х | х |
| RMON (1,2,3 and | 9 groups) | х | х | х | х | х | х |
| DHCP | Server | - | - | - | - | - | - |
| 2.101 | Client | x | x | x | x | х | х |
| | Relay | - | - | - | - | - | - |
| | Option82 | - | _ | - | - | - | _ |
| | · · · · · · · · · · · · · · · · · · · | - | | - | _ | _ | _ |
| E | Snooping | | | | | | |
| Event log | local flash, remote server | x | х | х | х | х | Х |
| sFlow | | - | - | - | - | - | - |
| Port Mirroring | One to One, Many to One | х | x | х | x | X | х |
| Remote Ping | | Х | х | х | x | х | × |
| LLDP (IEEE802.1ab) | | х | х | х | х | х | х |
| Cable Diagnostic | S | х | х | х | х | х | × |
| UPnP | | х | х | х | x | х | х |
| | | Enviror | nmental | | | | |
| Dimensions | Inches (WxHxD) | 12.99 x 9.06 | 18.98 x | 18.98 x | 12.99 x 9.06 | 18.98 x | 18.98 x |
| | | x 1.75 | 10.24 x 1.75 | | x 1.75 | 10.24 x 1.75 | 10.24 x 1.7 |
| | | | | | | | |
| Power Supply | | 100-240V | 100-240V | 100-240V | 100-240V | 100-240V | 100-240 |
| | | AC, 50/60 | AC, 50/60 | AC, 50/60 | AC, 50/60 | AC, 50/60 | AC, 50/60 |
| | | Hz | Hz | Hz | Hz | Hz | Hz |
| Maximum Power Consumption (Watts) | | 10.00 | 12.64 | 10 7 4 | 163.00 | 287.93 | 425.15 |
| (Full PoE No PoE) | | 10.22 | 12.64 | 18.34 | 12.70 | 22.24 | 38.75 |
| Operating | | | | | | | |
| Temperature | | 0-50°C | 0-50°C | 0-50°C | 0-50°C | 0-50°C | 0-50°C |
| - | <u> </u> | | | | | | L |
| | ondensing) | | | 1 | | | |
| Humidity (non-c | ondensing) | 10 - 90% | 10 - 90% | 10 - 90% | 10 - 90% | 10 - 90% | 10 - 90% |

41 - Appendix - Safety and Regulatory Information

FCC Warning

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

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

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

CE Warning

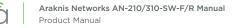
This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

UL Statement

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

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

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



42 - Warranty

2 Year Limited Warranty

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

Contact Information

Web: www.araknisnetworks.com

Phone: Technical Support - (866) 838.5052

Email: techsupport@araknisnetworks.com

