araknis NETWORKS

300 – SERIES NETWORK SWITCHES

Product Manual

Managed AV Rack Network Switches

CERTIFICATIONS AND WARNINGS

FCC Warning This device has been tested and found to comply with limits for a Class B digital device, pursuant to Parts 2 and 15 of 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 and radiates radio frequency energy and, if not installed and used in accordance with the user's manual, it may cause interference in which case users will be required to correct interference at their own expense.

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

UL This device is intended for indoor use only. It should not be connected to an Ethernet network with outside plant routing.

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. This manual was created expressly for electronic use, but has been formatted so that it may be printed and bound using either one-sided or front-and-back printing.

The symbols below are used in this manual to identify certain information. Review the definition of each symbol type to better understand notes later in the text.

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. Pro tips may also link to extra information that will provide a better understanding of application, technology or use of the product feature in question. These items are not required, but have been added for the convenience of this manual's target audience.

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. Notes may be located before or in the midst of the section they apply to, depending on the type of information. These items usually contain essential information, like the size or dimension of a separate part required, or a critical step in the process 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. Cautions are always provided before the information they relate to. 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. Warnings are always provided before the information they relate to. 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

Figures

Tables

1— INTRODUCTION

1.1— Welcome to Araknis® Networks

Thank you for choosing an Araknis® 300-series Network Switch. The 300-series managed network switch is an enterprise-class switch specifically designed for use in Ethernet applications within the residential market.

With front-facing indicators and rear-facing ports, the 300-series switch was designed for easy installation and high performance in an environment where traffic on the network and the number of users could increase continuously. The switch provides 10/100/1000Mbps capability on all ports and operates as a plug-and-play device, auto detecting connections to other switches and allowing straight-through patch cables throughout an installation. An intuitive GUI (Graphical User Interface) allows for quick and easy configuration of the switch's powerful features.

PoE models provide full PoE functionality. The PoE power budget in the AN-300-SW-R-8-POE / -16-POE / -24-POE provides 15W on each port simultaneously. This helps the systems integrators save time and effort calculating the available power budget as more PoE devices are added to the switch.

Note — Individual ports can provide up to 25W, but this will affect the available PoE budget for other ports. Each PoE model can provide 25W on half of the available ports at the same time.

This Installation Guide will guide you through the layout of the device, and show the basic steps for using the switch.

For more information, visit www.snapav.com.

1.1.1— Araknis® 300-Series Overview

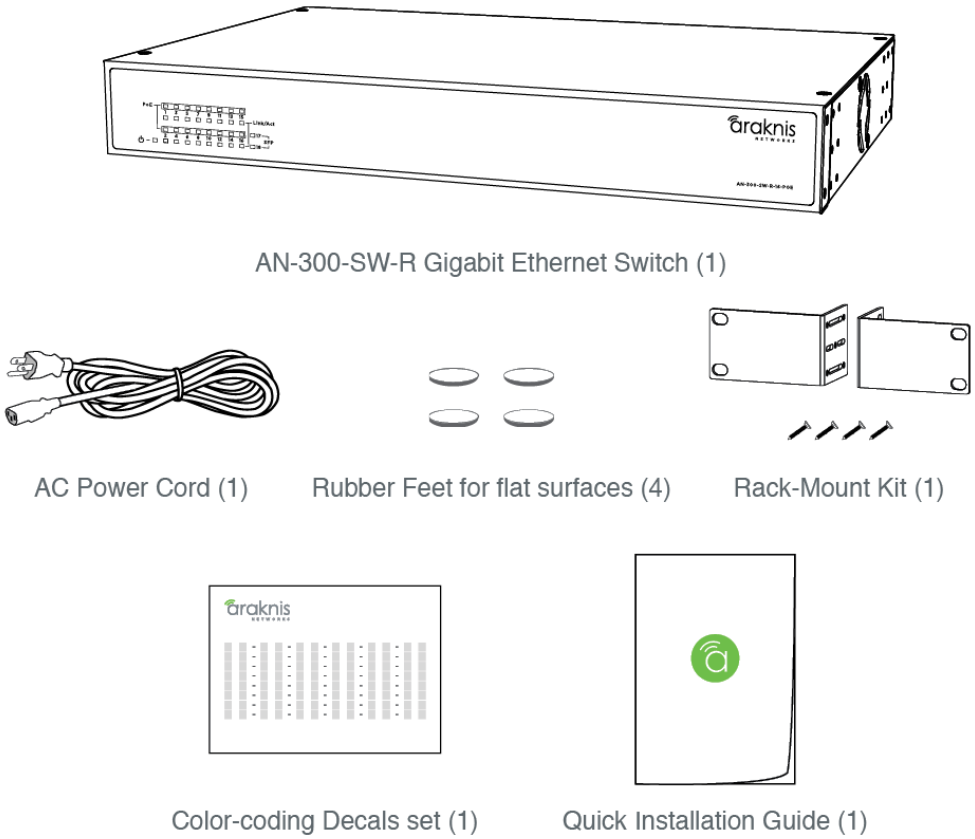
The following table lists the models available in the 300-series family of network switches.

Table 1. Series Overview

Model	Number of Ethernet Ports	Number of PoE Ports	Number of SFP Ports	Internal/External Power Supply
AN-300-SW-F/R-8	8	0	2	Internal
AN-300-SW-F/R-16	16	0	2	Internal
AN-300-SW-F/R-24	24	0	2	Internal
AN-300-SW-F/R-8-POE	8	8	2	Internal
AN-300-SW-F/R-16-POE	16	16	2	Internal
AN-300-SW-F/R-24-POE	24	24	2	Internal

1.2— Package Contents

Figure 1. Package Contents



1.3— Recommended for Installation

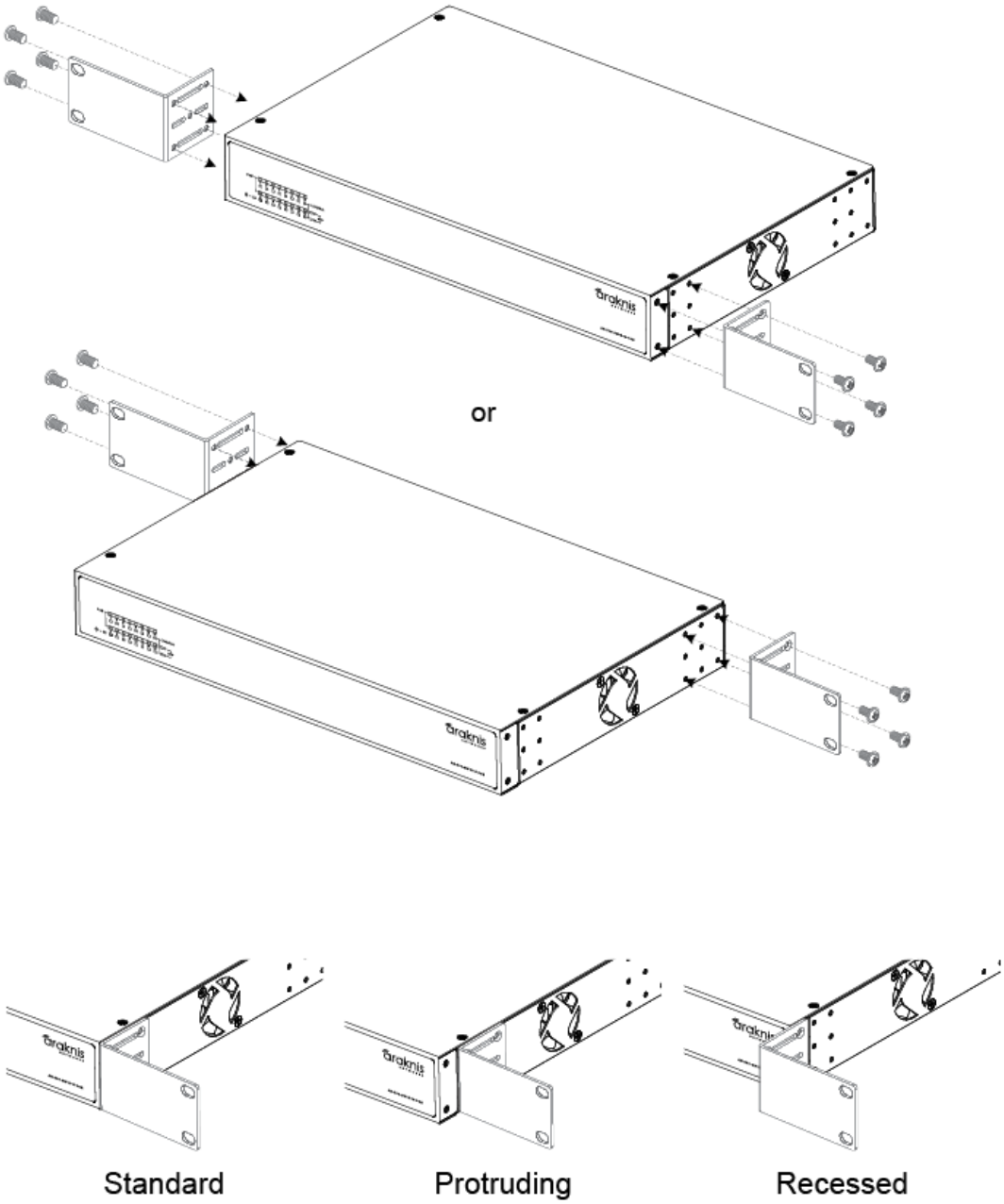
- #2 Phillips screwdriver (for mounting ear installation)
- Screws and anchors for wall-mount installation optional; use a material that is fastener rated, specified for use in the wall, and can safely hold the weight of the model in use
- Rack screws (optional; use screws designed for the rack in use)
- Drill (optional; for installation of wall-mount screws or anchors)

Note — For wall mounting, it is recommended to use #8x1-1/4 in. coarse phosphate-plated steel bugle-head Phillips drywall screws and anchors.

2.1— Mounting Options

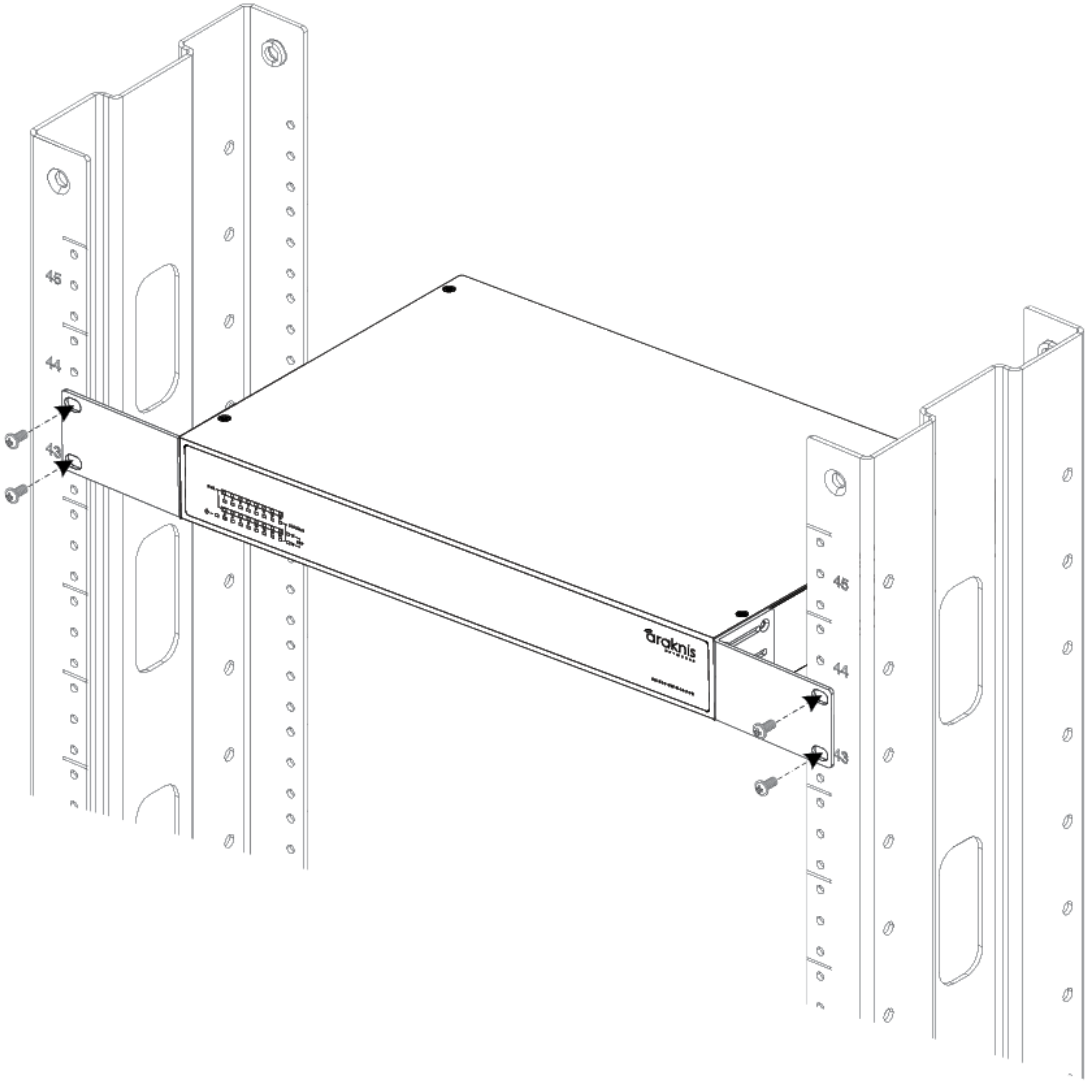
2.1.1— Rack Mounting

Figure 2. Rack Mounting Ears



Note — All product pictures in this manual feature AN-300-SW-R models as an example of the 300-series product line. Front-facing models are identical in operation.

Figure 3. Rack Mounting Options

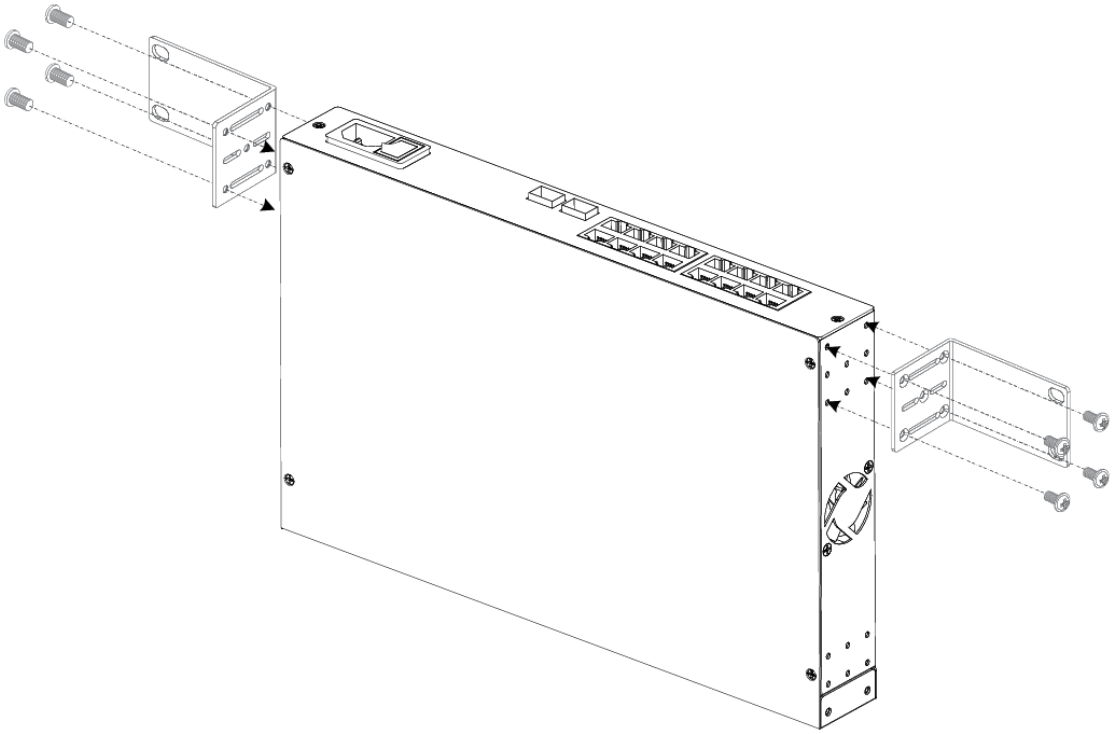


2.1.1.1— Rack Mounting Guidelines

- 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).

2.1.2— Wall Mounting

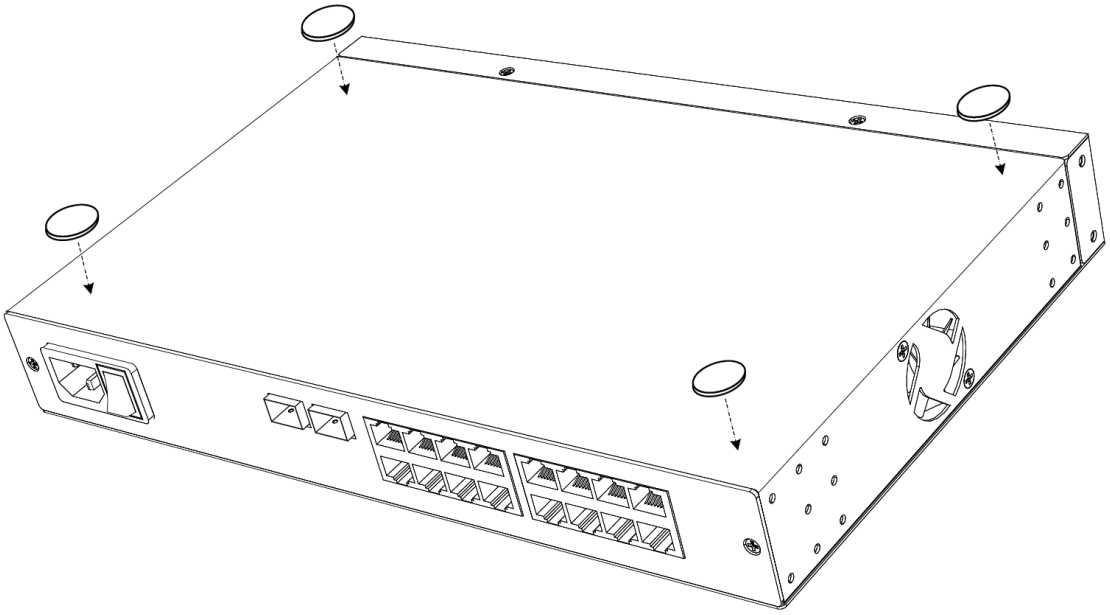
Figure 4. Wall Mounting



2.1.3— Shelf Mounting

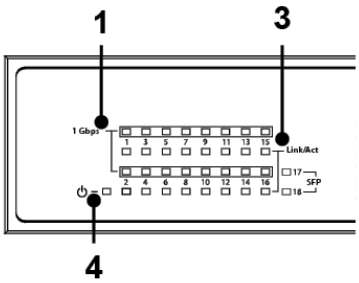
Warning! — Caution: Do not stack more than 4 switches together. Do not stack any other equipment on top of the network switch to avoid possible interference or damage.

Figure 5. Shelf Mounting



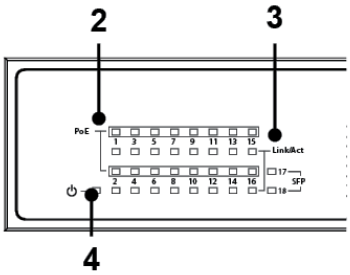
2.2— Front Panel Layout

Figure 6. Front Panel Layout



1. 1 Gbps LED Indicator (for non-PoE Models)

LED	Behavior	Description
1 Gbps	Off	No device is connected/ Connected device supports 10/100M speed
	On	Device is connected at 1Gbps speed



2. PoE LED Indicator (for PoE Models)

PoE LED Indicator (for PoE Models)	Off	No PoE device is connected
	On	PoE-enabled device is connected

3. Link/Act LED Indicator

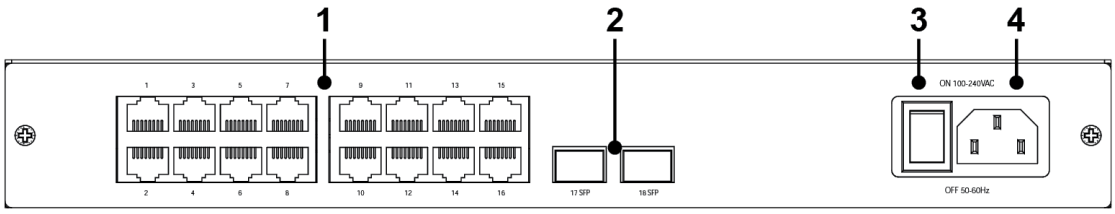
Behavior	Description
Off	No device is connected
Blinking	Device is connected and traffic is running

4. Power LED Indicator

Behavior	Description
Off	Power is off
On	Power is on

2.3— Rear Panel Layout

Figure 7. Rear Panel Layout

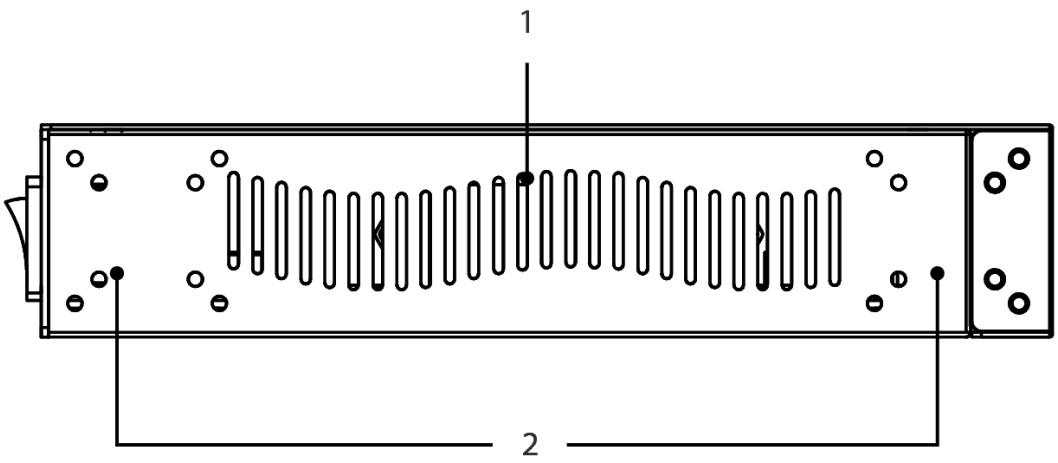


1. **Ethernet Ports (RJ45) —** Connect Ethernet network cables routed to equipment.
2. **SFP Ports —** Port for AN-ACC-SFP-E-100 or AN-ACC-SFP-MMF-350
3. **Master Power Switch —** Toggle Switch for master power control.
4. **Power Jack —** Attach an IEC power cable.

2.4— Side Panel Layout

2.4.1— Non-PoE Models

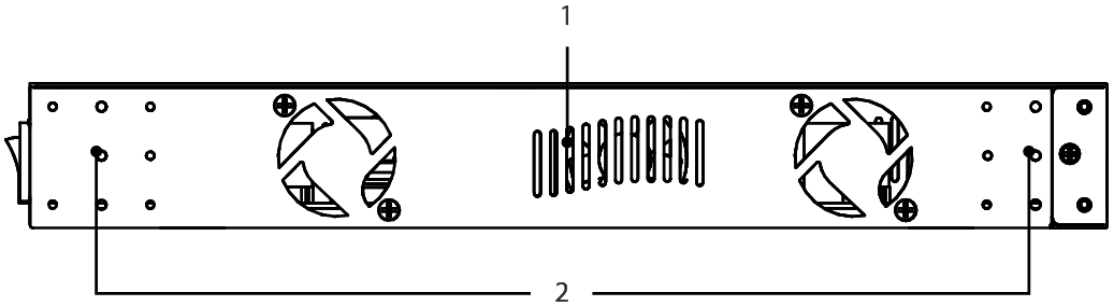
Figure 8. Non-PoE Models



1. **Ventilation Slots —** Allows airflow through the chassis to keep the device cool.
2. **Rack Mounting Holes —** The combination of threaded holes at the front and rear of each side allow for many variations in mounting options.

2.4.2— PoE Models

Figure 9. PoE Models

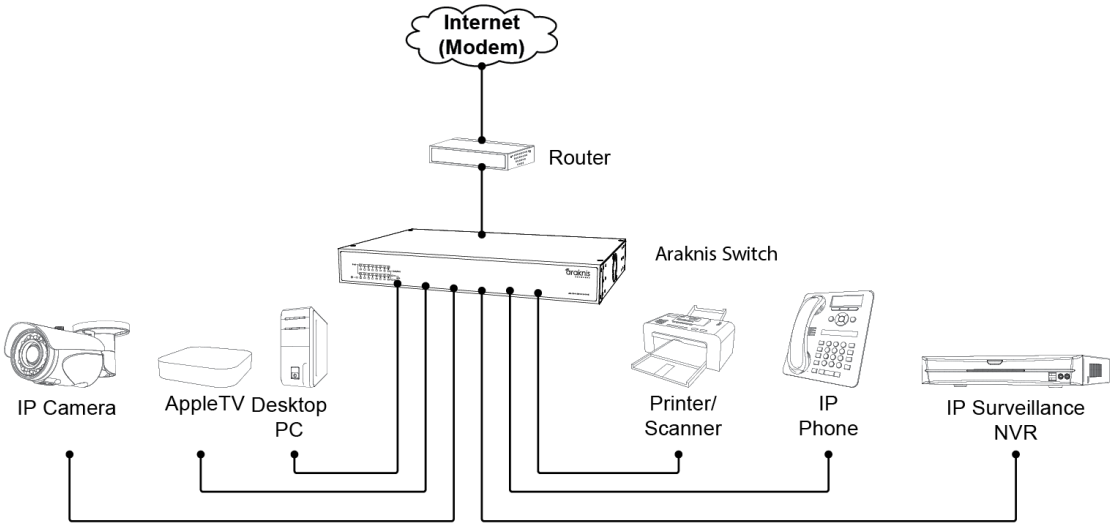


1. **Ventilation Slots —** Allows airflow through the chassis to keep the device cool.
2. **Rack Mounting Holes —** The combination of threaded holes at the front and rear of each side allow for many variations in mounting options.

Note — The PoE model shown above is for model AN-300-SW-R-24-POE. 8-port and 16-port models only have one fan.

2.5— Installation Diagram

Figure 10. Installation Diagram



2.6— Powering the Switch

Figure 11. Power Inlet

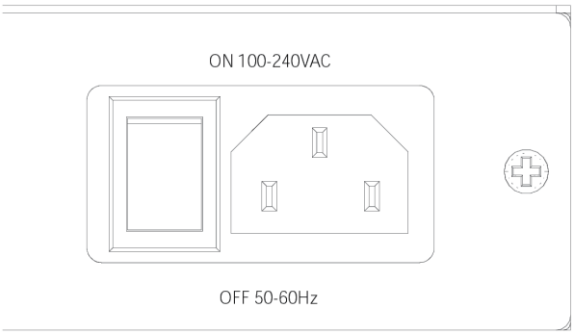


Table 2. Power Requirements

Input Voltage (AC Only)	100~240V AC, 50~60Hz

3— SOFTWARE CONFIGURATION

The Araknis® Managed switch provides a variety of basic and advanced features for Layer 2 switching, all available for access and modification through a convenient web interface. The default configuration that comes set out of the box was designed for quick integration into most applications without making any setting changes. To maximize the switch's performance however, there are changes that can be made to fully optimize the network.

3.1— Key Features

Table 3. Key Features

Feature	Description
Configuration Backup and Restore	Backup to management station using Web
Authentication	Telnet, Web – user name/password Web – HTTPS Telnet – SSH SNMP v1/2c – Community strings SNMP version 3 – MD5 or SHA password
General Security Measures	Private VLANs Port Authentication Port Security DHCP Snooping (with Option 82 relay information) IP Source Guard
DHCP	Client
DNS	Client and Proxy service
Port Configuration	Speed, duplex mode, flow control, MTU, response to excessive collisions, power saving mode
Rate Limiting	Input rate limiting per port
Port Mirroring	1 sessions, up to 10/18/26 source port to one analysis port per session
Link Aggregation	Supports up to 5/9/13 trunks – static or dynamic (LACP)
Address Table	8K MAC addresses in the forwarding table
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 4K using IEEE 802.1Q, port-based VLANs
Quality of Service	Supports Differentiated Services (DiffServ) and DSCP remarking
Multicast Filtering	Supports IGMP snooping and query, and Multicast VLAN Registration

3.2— Description of Software Features

The Araknis® Managed switch provides a variety of features that can help enhance your network's performance. Read about these features below.

Configuration Backup and Restore

You can fully backup the settings for this switch to a file on your PC. Once this is done, you have the ability to load this file back into the same switch or deploy it to another Araknis® 300-series switch.

Authentication

Access to the switch's web interface can be authenticated. You can provide usernames and passwords for different levels of access.

There are other choices for authentication that include HTTPS for secure management access via the web interface, SSH for secure management access via a Telnet connection, and SNMP version 2c/3.

Port Configuration

Unique configuration options are given for each individual port. These options include name configuration, speed and duplex mode, flow control, as well auto-negotiation to detect the connection settings in use for the device connected. Full-Duplex mode can be used on ports to double the throughput of those connections. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2002).

Port Mirroring

Traffic from one port can be mirrored to another target port. This gives the ability to enable a protocol analyzer on the port for traffic analysis and to conduct deep troubleshooting.

Link Aggregation

The switch can create an aggregate connection by combining ports. You have to option to set this up manually or automatically using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). Throughput may increase exponentially with the addition of each aggregated port, which will provide redundancy if the trunk port ever fails. The Araknis® switch can support up to 16 trunks.

IEEE 802.1D Bridge

The switch supports IEEE 802.1D transparent bridging. Data frames are analyzed from the source addresses to create an address table that can then filter or forward traffic based off of the analyzed traffic. The address table supports up to 8,000 addresses.

Store-And-Forward Switching

With this function the switch can copy each frame into memory before sending it to another port. This allows for the switch to check for errors. The switch will look to see that all frames are a standard size and verify the accuracy using the cyclic redundancy check(CRC). This is a great tool for preventing any bad frames from entering the network and causing trouble with bandwidth.

The switch provides 512 KB for frame buffering to avoid dropping frames on congested ports. Using this buffer will allow the switch to queue packets that are awaiting transmission on congested ports.

Spanning Tree Algorithm

The switch supports these spanning tree protocols:

- Spanning Tree Protocol (STP, IEEE 802.1D) – STP helps ensure a loop free topology within your network. In a large network with multiple physical links, loops can occur in the path back to the router. Using the STP algorithm, a single path will be chosen to disable all the others to ensure that only the most efficient path exists between two devices on the network. Using STP will prevent the introduction of network loops that can severely decrease bandwidth and even cause devices to not work. In the event that the chosen path were to fail, an alternate path will be used to maintain connection.
- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol adds new bridge port roles. This is done to speed up convergence following a link failure. It will speed up that convergence time to about 3 to 5 seconds, where it is at 30 seconds on the older IEEE 802.1D STP standard.
- Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s) – This protocol is a direct extension of RSTP. It will allow for an independent spanning to be used with different VLANs.

Virtual LANs

A Virtual LAN is a partition of a network that is its own broadcast domain that is isolated to allow packet pass through only on this specific VLAN through a router. The switch supports up to 4096 VLANs. Tagged VLANs based on the IEEE 802.1Q standard are supported. Switch ports can be manually assigned to a specific set of VLANs. By segmenting your network into VLANs, the following is possible:

- Broadcast Storms are possible in a flat network. VLANs will help prevent this.
- Data security is provided by restricting traffic to the original VLAN.
- VLANs will help in isolating devices that use multicast or broadcast in their own broadcast domain. With other devices not having to listen to and discard multicast and broadcast traffic, network performance will be increased.

Quality of Service (QoS)

QoS uses Differentiated Services (DiffServ) to provide a policy-based management mechanism used for prioritizing network resources. This allows the network to meet the requirements of specific traffic types on a per-hop basis. Each packet is prioritized based on the required level of service. This prioritization is completed using eight priority queues with strict or Weighted Round Robin queuing. Incoming traffic is prioritized based on input from the connected device to the switch port using IEE 802.1p and 802.1q tags. Independent priorities can be set for delay sensitive data (streaming video) and best-effort data (Internet browsing).

Multicast Filtering

You have the ability to assign Multicast traffic to its own VLAN so that it will not interfere with normal network traffic. Setting the required priority level for the designated VLAN guarantees real-time delivery. IGMP Snooping and Query are used to manage multicast group registration for IPv4 traffic.

3.3— System Defaults

The switch system defaults are provided in the “Factory_Default_Config.cfg” configuration file. The following table lists some of the basic system defaults. (See section 3.8.2—File Management on page 47 for information about using configuration files and restoring the switch to factory default settings.)

Table 4. System Defaults

Function	Parameter	Default Setting
Authentication	Admin User Name	“araknis”
	Admin Password	“araknis”
	HTTPS	Enabled
	SSH	Enabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Disabled
	HTTP Secure Server Redirect	Disabled
SNMP	SNMP Agent	Disabled
	Community Strings	“public” (read only)
		“private” (read/write)
	Traps	Global: Disabled
		Authentication traps: Enabled
		Link-up-down events: Enabled
	SNMP V3	View: default_view
		Group: default_rw_group
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Link Aggregation	Static	None
Spanning Tree Algorithm	Status	Enabled, RSTP
Address Table	Aging Time	300 seconds

Function	Parameter	Default Setting
Virtual LANs	Default VLAN	1
	PVID	1
	Acceptable Frame Type	All
	Ingress Filtering	Disabled
	Switchport Mode (Egress Mode)	Access
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	Strict
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: Disabled in strict mode
	Ethernet Type	Disabled
	VLAN ID	Disabled
	VLAN Priority Tag	Disabled
	ToS Priority	Disabled
	IP DSCP Priority	Disabled
	TCP-UDP Port Priority	Disabled
LLDP	Status	Enabled
IP Settings	Management VLAN	VLAN 1
	IP Address	192.168.20.254
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled Snooping: Disabled
	DNS	Proxy service: Disabled
Multicast Filtering	IGMP Snooping	Snooping: Disabled Querier: Disabled
	Multicast VLAN Registration	Disabled
System Log	Status	Enabled
NTP	Clock Synchronization	Disabled

3.4— Device Access Methods and Guidelines

3.4.1— Web Interface

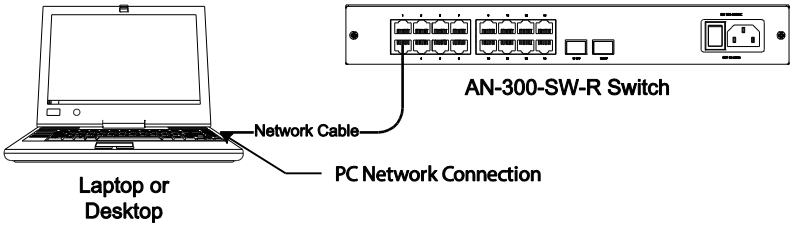
This section details how to connect to the switch through the web interface. To make the best use of the management features in your switch, it is highly recommended to configure it with an IP address in the same range as other equipment on the local network before permanently installing the switch.

3.4.1.1— Web Interface Access Setup

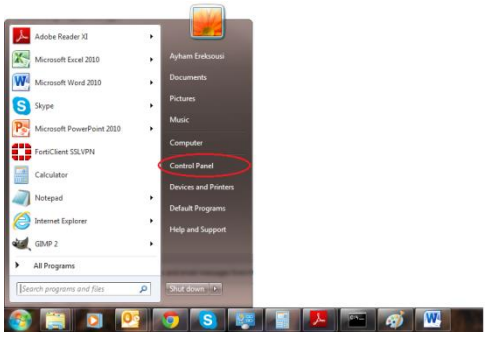
Follow this procedure to connect to the Web Interface:

3. Place the switch close to the PC that you intend to use for configuration. It helps if you can see the front panel of the switch while working on your computer.

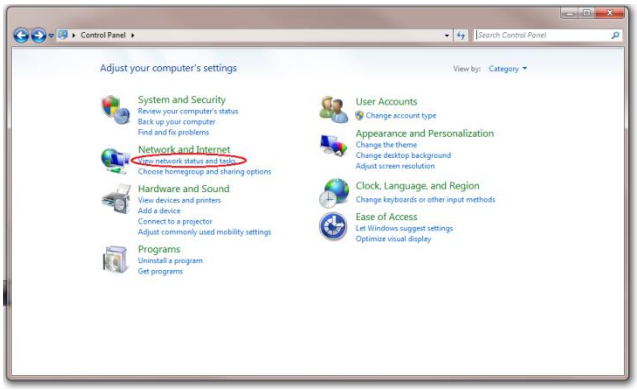
Figure 12. PC Connection for Web Interface



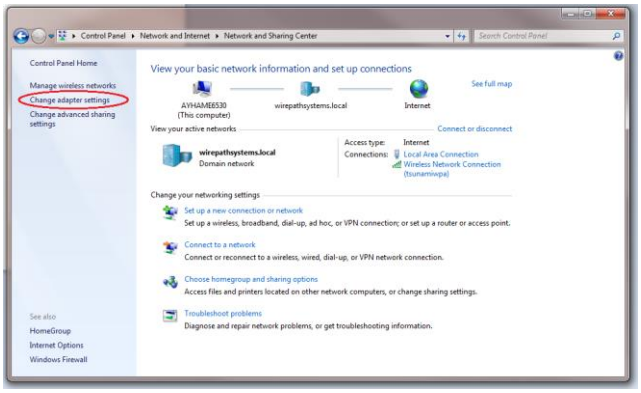
4. Connect the Ethernet port of your PC to any Ethernet port on the switch. Connect power to the switch and verify that you have a link by checking the front-panel LEDs.
5. Check that your PC has an IP address on the same subnet as the switch. The default IP address of the switch is **192.168.20.254 and the subnet mask is 255.255.255.0**. The PC and switch are on the same subnet if they both have addresses in the range, “192.168.20.x”. If the PC and switch are not on the same subnet, manually set the PC’s IP address to 192.168.20.x (where “x” is any number from 1 to 253):
   A. Click the Start button, and then “Control Panel”.



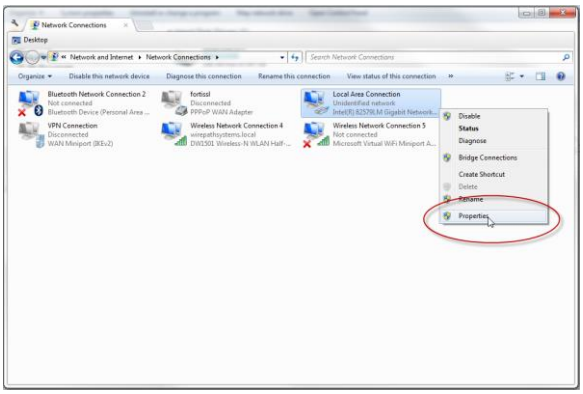
B. Click on “View network status and tasks” under “Network and Internet”.



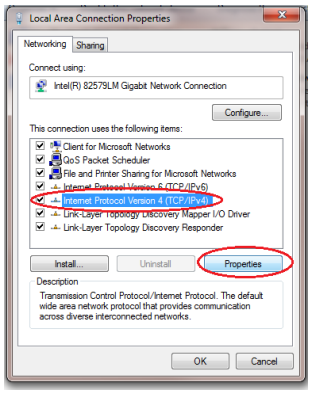
C. On the left panel, click on “Change Adapter Settings”.



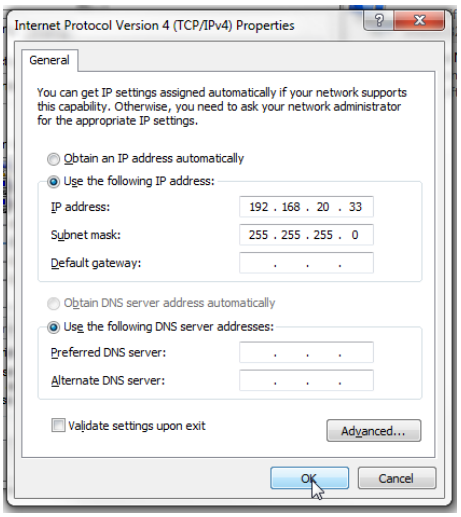
D. Right click on the local Ethernet adapter icon and click on “Properties”.



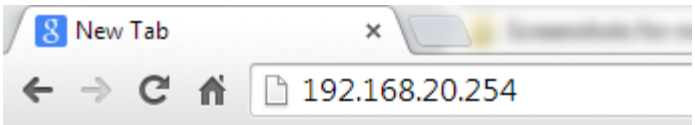
E. Click to highlight “Internet Protocol Version 4 (TCP/IPv4), then click “Properties”.



F. Enter the new static IP settings, and then click “OK”. Then, click “OK” on the Ethernet adapter properties window.



6. Open a web browser and enter the address http://192.168.20.254. If your PC is properly configured, you will see the login page for the switch. If you do not see the login page, repeat step 3.



7. Enter “araknis” for both the user name and password fields and then click the “Login” button.

8. From the menu, click SETTINGS->System. To request an address from a local DHCP Server, mark the DHCP Enabled check box. To configure a static address, enter the new IP Address, Subnet Mask, and other optional parameters for the switch, and then click on the “Apply” button.

After changing the IP address, connectivity will be lost, as the IP address is now different than before. Verify the new IP address of the switch within the settings of your router. Or, if you have statically assigned an IP address, simply type that IP address, gateway, and subnet into your LAN settings on your PC.

Note — No other configuration changes are required at this stage, but it is recommended that you change the administrator’s password before logging out.

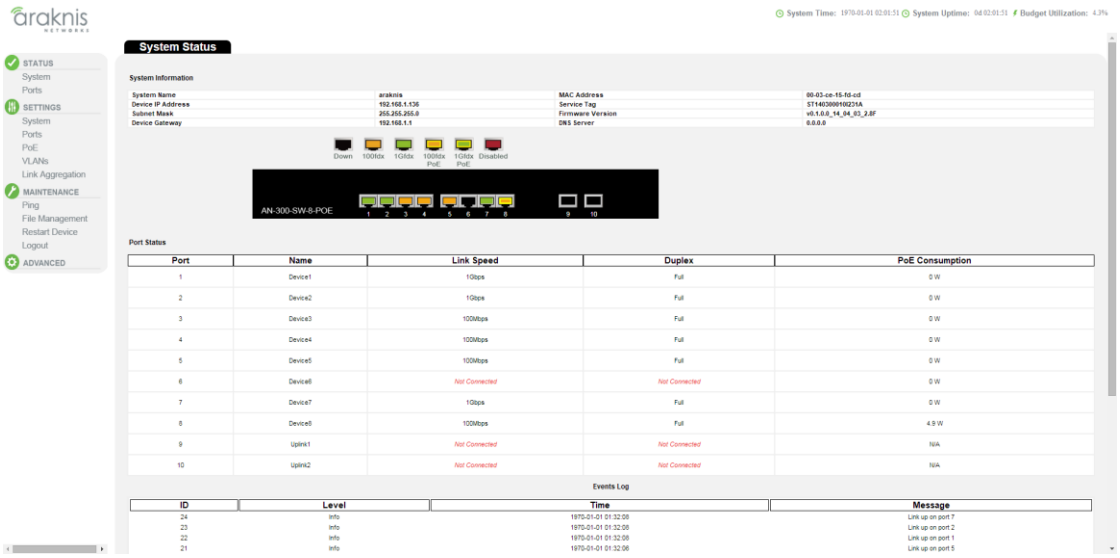
3.5— Navigating the Web Browser Interface

A username and password must be entered to access the web-browser interface. The default administrator user name and password is "**araknis**" for both fields. The administrator has Read/Write access to all configuration parameters and statistics.

3.5.1— Home Page (System Status)

After logging into the switch, the System Status page will appear (Figure 13). The navigation menu on the left side of the screen is used to access different screens on the management interface to monitor and configure the switch. The live status bar in the top-right corner displays the switch's current time, uptime, and PoE budget utilization (for PoE models only). The main window displays the system status or the option selected from the navigation menu, with the name of the menu selection being viewed in the black tab above.

Figure 13. Web Interface Home Page



3.5.2— Navigation Menu Overview

Basic configuration items in the menu are always visible. The Advanced menu is collapsed by default. Click “Advanced” to expand all Advanced settings.

Table 5. below briefly describes the selections available on the 300-series switch.

3.5.2.1— Navigation Menu Options

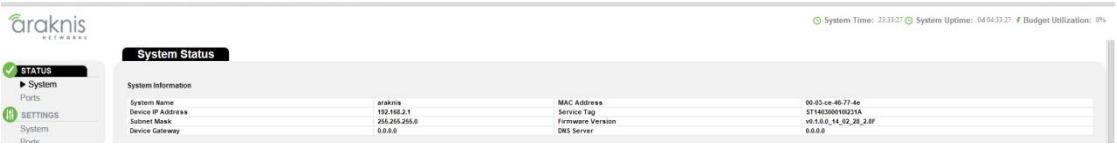
Table 5. Navigation Menu Options

- **Status**
  - System
  - Ports
- **SETTINGS**
  - System
  - Ports
  - PoE
  - VLANs
  - Link Aggregation
- **MAINTENANCE**
  - Ping
  - File Management
  - Restart Device
  - Logout
- **ADVANCED**
  - Ports (Detailed Port Statistics)
    - Port Statistics
    - Port Settings
  - LACP
  - Connected Devices
  - IGMP Snooping
  - Spanning Tree
    - Status
    - Bridge Settings
    - CIST Ports
  - VLANs
    - MAC-Based VLANs
    - Private VLANs
  - Security
    - SNMP
    - Access Management
    - DHCP Snooping
    - Loop Protection
    - Port Mirroring
  - Advanced QoS
    - Port Classification
    - Port Policing
    - Port Scheduler
    - Port Shaping
    - Port Tag Remarking
    - Port DSCP Configuration
    - DSCP-Based QoS
    - DSCP Translation
    - DSCP Classification
    - QoS Control List Configuration
    - Storm Control

3.6— Status Menu

3.6.1— System Status

Figure 14. System Status Menu



Path Status, System

3.6.1.1— System Information

The System Information table in Figure 14 displays basic global information about the switch:

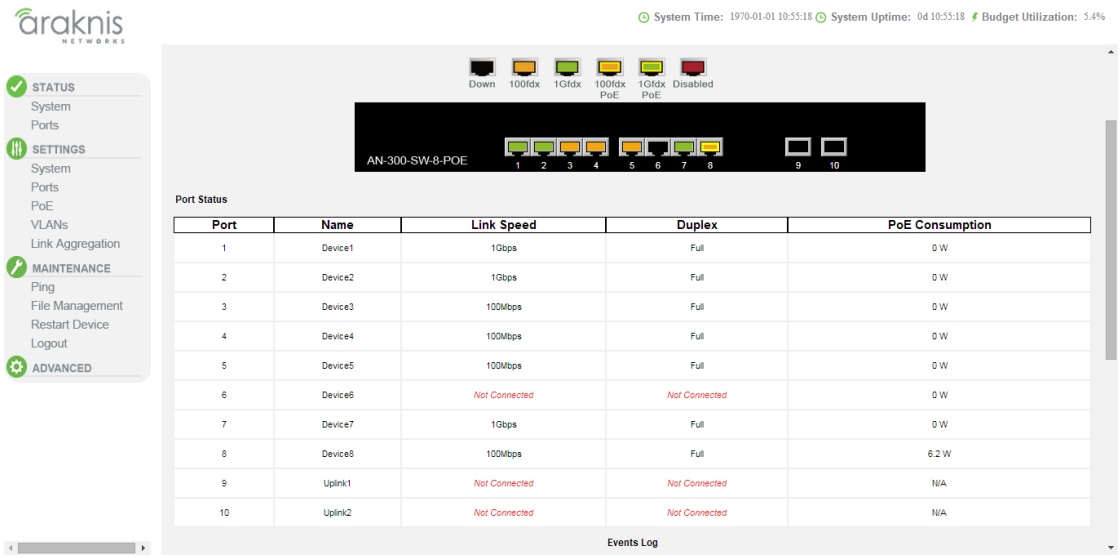
- **System Name** – Name assigned to the switch system.
- **Device IP Address** – Device management IP address.
- **Subnet Mask** – Management address subnet mask.
- **Device Gateway** – Management VLAN default gateway.
- **MAC Address** – Device Media Access Control (MAC) address.
- **Service Tag** – Araknis® Networks unique device identifier. Used to track individual devices for easy service and support.
- **Firmware Version** – Current running firmware version.
- **DHCP Server** – IP address of the DHCP server (if DHCP is enabled).

3.6.1.2— Port Status and Panel Display

The System Status page displays a live graphic of the switch with the current status of each port. Clicking on the image of a port opens the Advanced Port Statistics page of that port (4.1.1— Port Statistics on page 51)

Below the graphic, the Port Status table summarizes the Port, Name, Link Speed, Duplex Mode, and PoE consumption for each port so that essential information is visible immediately upon logging in.

Figure 15. Port Status (on system status page)



Port	Name	Link Speed	Duplex	PoE Consumption
1	Device1	1Gbps	Full	0 W
2	Device2	1Gbps	Full	0 W
3	Device3	100Mbps	Full	0 W
4	Device4	100Mbps	Full	0 W
5	Device5	100Mbps	Full	0 W
6	Device6	Not Connected	Not Connected	0 W
7	Device7	1Gbps	Full	0 W
8	Device8	100Mbps	Full	6.2 W
9	Uplink1	Not Connected	Not Connected	N/A
10	Uplink2	Not Connected	Not Connected	N/A

Path Status, System

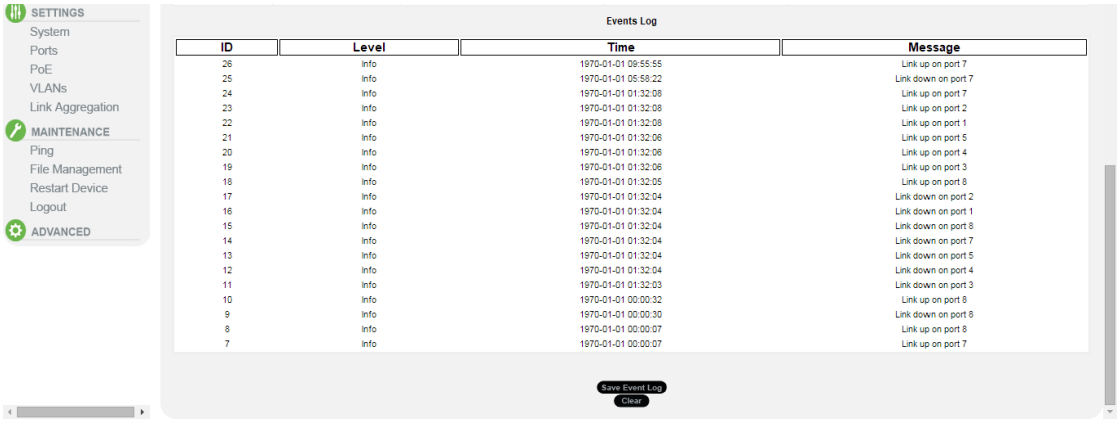
Parameters

- **Port** — The number of the port.
- **Name** — The assigned name of the port.
- **Link Speed** — The current negotiated speed of the port. Options include: 1Gbps, 100Mbps, 10Mbps, and Not Connected.
- **Duplex** — The current negotiated duplex setting with the connected device. Options include: Full and Half.
- **Port Consumption** — Watts being consumed by each PoE port.

3.6.1.3— Events Log

Use the Events Log to see messages about system events.

Figure 16. Events Log



ID	Level	Time	Message
26	Info	1970-01-01 09:55:55	Link up on port 7
25	Info	1970-01-01 05:58:22	Link down on port 7
24	Info	1970-01-01 01:32:08	Link up on port 7
23	Info	1970-01-01 01:32:08	Link up on port 2
22	Info	1970-01-01 01:32:08	Link up on port 1
21	Info	1970-01-01 01:32:06	Link up on port 5
20	Info	1970-01-01 01:32:06	Link up on port 4
19	Info	1970-01-01 01:32:06	Link up on port 3
18	Info	1970-01-01 01:32:05	Link up on port 8
17	Info	1970-01-01 01:32:04	Link down on port 2
16	Info	1970-01-01 01:32:04	Link down on port 1
15	Info	1970-01-01 01:32:04	Link down on port 8
14	Info	1970-01-01 01:32:04	Link down on port 7
13	Info	1970-01-01 01:32:04	Link down on port 5
12	Info	1970-01-01 01:32:04	Link down on port 4
11	Info	1970-01-01 01:32:03	Link down on port 3
10	Info	1970-01-01 00:00:32	Link up on port 8
9	Info	1970-01-01 00:00:30	Link down on port 8
8	Info	1970-01-01 00:00:07	Link up on port 8
7	Info	1970-01-01 00:00:07	Link up on port 7

Path Status, System

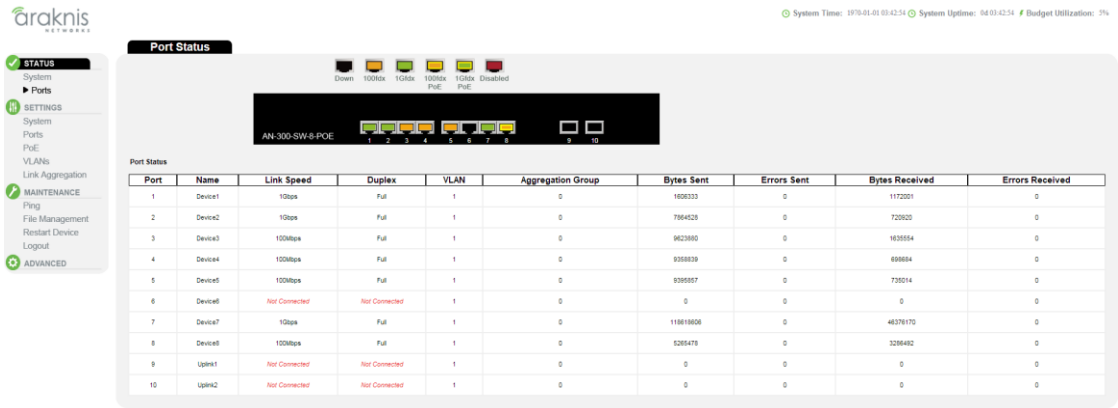
Parameters

- **ID** — Log entry identifier.
- **Level** — Shows the level of the log message. Options include Info, Warning, and Error.
- **Time —** Time stamp of the log entry.
- **Message** — Summary of the event log entry.

3.6.2— Ports

Use the Port Status table to display a summary of basic information on each port.

Figure 17. Ports Status Page



Port	Name	Link Speed	Duplex	VLAN	Aggregation Group	Bytes Sent	Errors Sent	Bytes Received	Errors Received
1	Device1	1Gbps	Full	1	0	1606333	0	1172001	0
2	Device2	1Gbps	Full	1	0	7864526	0	720920	0
3	Device3	100Mbps	Full	1	0	9623880	0	1635554	0
4	Device4	100Mbps	Full	1	0	9358839	0	698684	0
5	Device5	100Mbps	Full	1	0	9395857	0	735014	0
6	Device6	Not Connected	Not Connected	1	0	0	0	0	0
7	Device7	1Gbps	Full	1	0	118618606	0	46376170	0
8	Device8	100Mbps	Full	1	0	5265478	0	3286482	0
9	Uplink1	Not Connected	Not Connected	1	0	0	0	0	0
10	Uplink2	Not Connected	Not Connected	1	0	0	0	0	0

Parameters The following parameters are displayed:

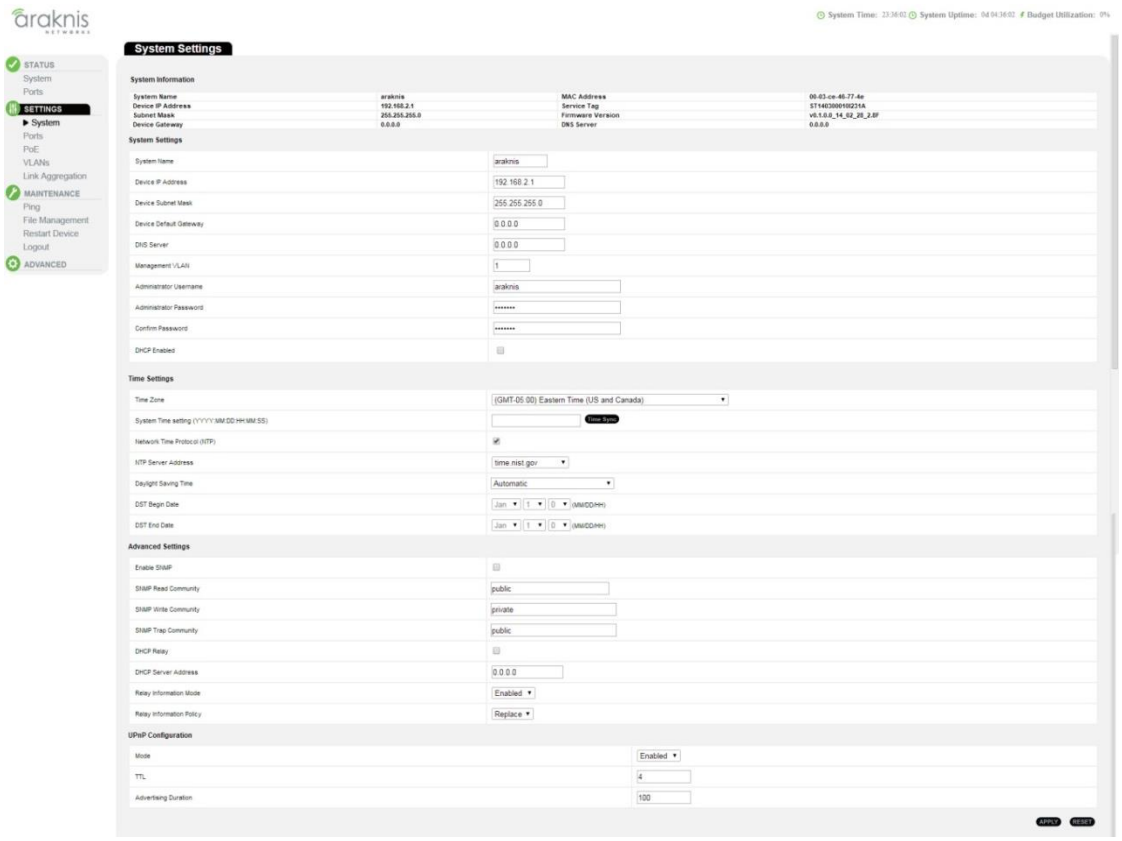
- **Port** – The number of the port.
- **Name** – The assigned name of the port.
- **Link Speed** – The current speed of the port based off of the connected device in use. Options include: 1Gbps, 100Mbps, 10Mbps, and Not Connected.
- **Duplex** – The current negotiated duplex setting with the connected device. Options include: Full and Half.
- **VLAN** – The VLAN ID of which the port is a member. All ports are members of VLAN ID = 1 by default.
- **Aggregation Group** – The aggregation group the port is member of. All ports are not members of any aggregation group by default.
- **Bytes Sent** – A live counter of the number of Bytes being transmitted on a specific port.
- **Errors Sent** – A live counter of the number of errors being 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 counter of the number of Bytes being received on a specific port.
- **Errors Received** – A live counter of the number of Errors being received on a specific port. Use this number to determine whether there is a problem with the physical interface of the port.

3.7— Settings Menu

3.7.1— System Settings

The System Settings page is used to configure basic settings such as System Name, IP Address, Date/Time Settings. Some advanced settings can be configured such as SNMP, DHCP Relay, and UPnP. The current settings are displayed in the System Information table at the top of the page.

Figure 18. Settings Menu



3.7.1.1— Changing the System Name

The system name is assigned to the switch for easy identification. (Maximum length: 10 characters)

Figure 19. System Name

Path Settings, System

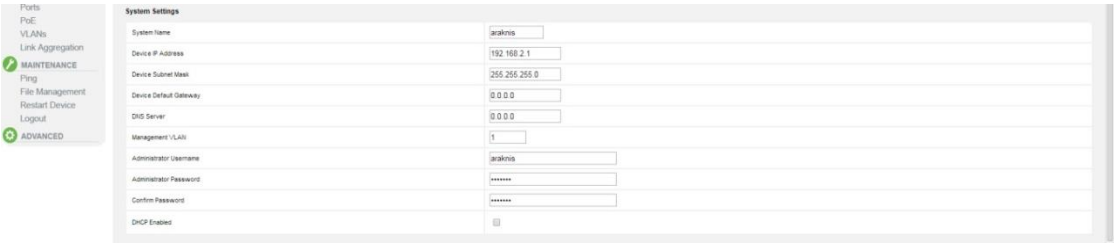
Configuration Instructions To configure System Name:

1. Click Settings, System.
2. Enter the new name in the System Name field.
3. Click Apply.

3.7.1.2— Changing the IP Address and Network Access Settings

The system settings section can be used to configure the IP address of the switch. The IP address for the switch can be obtained via DHCP or configured manually. To manually configure an IP address, you need to change the switch's default settings to values that are compatible with your network. In case you need to access the web interface of the switch from an outside network or you want to use Network Time Protocol (NTP) server, you need to configure a Default Gateway for the switch that is on the same subnet as the switch configured IP address.

Figure 20. IP Settings



Path Settings, System, System Settings

Parameters These parameters are displayed:

IP Configuration

- **Device IP Address –** Valid IP addresses consist of four decimal numbers represented in dot-decimal notation, 0 to 255, separated by periods. (Default: 192.168.20.254)
- **Device Subnet Mask –** This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **Device Default Gateway –** The IP address to the gateway (Typically the IP Address of the Router) the switch uses to access the Internet or other VLANs on the network.
- **DNS Server –** Enter the same DNS Server IP Address that is listed in the router on site, or use the IP address of the router itself.
- **Management VLAN –** ID of the management VLAN. By default, all ports on the switch are members of VLAN 1. The web interface can be configured for access from a specific VLAN after that VLAN is configured. Changing the default management VLAN ID will result in a loss of connection until your PC is physically connected to a switch port that is a member of the newly assigned management VLAN ID. (Range: 1-4095; Default: 1)
- **Administrator Username –** See Section 3.7.1.3
- **Administrator Password –** See Section 3.7.1.3
- **DHCP Client –** If DHCP is enabled, the web interface will not be accessed until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP values can include the IP address, subnet mask, and default gateway. (Default: Disabled)

Configuration Instructions To configure an IP address:

1. Click Settings, System.
2. Specify the IPv4 settings.
3. Click Apply.

3.7.1.3—Changing Admin Username and Password

It is recommended to change the default username and password in order to keep the network secure.

Figure 21. Administrator Credentials

Path Settings, System, System Settings

Parameters

- **Administrator Username –** Change the default username of the admin (default: araknis).
- **Administrator Password –** Change the default password for the admin account (default: araknis).

Configuration Instructions To change Admin Username and Password:

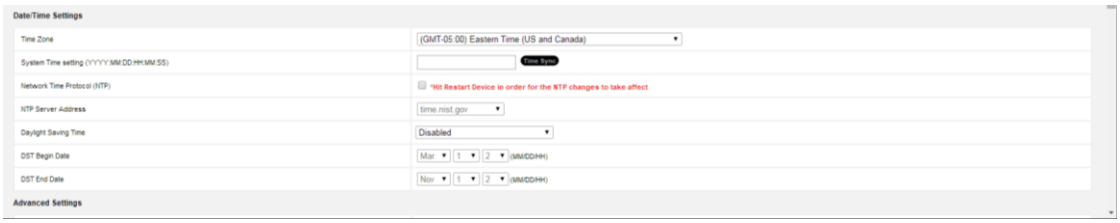
1. Click Settings, System.
2. Specify the new admin credentials.
3. Click Apply.

3.7.1.4— Configuring Time Settings

Use the Time Settings section to specify the Network Time Protocol (NTP) servers to query for the current time. NTP allows the switch to set its internal clock based on periodic updates from an NTP time server. Recording meaningful dates and times in the event log is essential for troubleshooting the switch and maintaining the system time will ensure that this log is correct. If the clock is not set, the switch will only record the time since the factory default was reset during the last boot-up.

NTP is disabled by default. When the NTP client is enabled, the switch periodically sends a request for a time update to a configured time server. Select a server from the preconfigured list, or enter a custom NTP server address.

Figure 22. Time Settings Menu



In the Time Settings section, you can manually change the Time Zone of the switch to ensure that your times match up with the region that the switch is installed in. Daylight Savings Time may also be set to Disabled, Automatic, or Manual. By selecting Manual Daylight Savings Time, you can manually set the date of Daylight Savings Time (DST) begin and end. The Automatic option adheres to DST rules in the continental U.S. only. If you are planning to use the device outside the U.S., manually change DST settings to match the country you are in.

Time settings may also be configured manually in the format “YYYY:MM:DD:HH:MM:SS” , or by pressing "Sync Time" to automatically pull settings from your PC.

Note — Once the NTP server is configured, make sure the device has a Default Gateway and DNS set and then restart the device from Maintenance -> Restart menu. This will force the switch to trigger an NTP request.

Path Settings, System, Time Settings

Parameters

- **Time Zone** – Manually configure Time Zone settings for the switch. (Default: Eastern Standard Time (EST)).
- **Network Time Protocol (NTP)** – Enables or disables NTP client requests.
- **NTP Server Address** – Sets the IP address for a time server. The switch attempts to update the time from the server.

Configuration Instructions

To configure the NTP server:

1. Click Settings, System.
2. Enable NTP then select a server from the list.
3. Select your DST settings.
4. Click Apply.
5. Make sure “Default Gateway” and “DNS Server” options are configured correctly.
6. Click on Maintenance, Restart
7. Restart the device to force an NTP request (see section 3.8.3—Restart Device on page 50).

3.7.1.5—Configuring SNMP System and Trap Settings

Simple Network Management Protocol (SNMP) is an internet protocol for network management. It is used for collecting information from various devices on the network. Devices that typically support SNMP include routers, switches, printers and more. It will monitor these attached devices for notifications that require troubleshooting.

SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.

Table 6. SNMP Table

Model	Level	Community String	Group	Read View	Write View	Security
v1	noAuth NoPriv	public	default_ro_group	default_view	none	Community string only
v1	noAuth NoPriv	private	default_rw_group	default_view	default_view	Community string only
v1	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v2c	noAuth NoPriv	public	default_ro_group	default_view	none	Community string only
v2c	noAuth NoPriv	private	default_rw_group	default_view	default_view	Community string only
v2c	noAuth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	Community string only
v3	noAuth NoPriv	*user defined*	default_rw_group	default_view	default_view	
v3	Auth NoPriv	*user defined*	*user defined*	*user defined*	*user defined*	
v3	Auth Priv	*user defined*	*user defined*	*user defined*	*user defined*	Provides user authentication via MD5 or SHA algorithms and data privacy using DES 56-bit encryption

The switch contains a software “agent” that supports SNMP locally on the switch. This includes SNMP version 1, 2c, and 3. “Managed Objects” are variables that are defined and maintained by the SNMP agent that is managing the device. The Management Information Base (MIB) defines each “object” and provides a standard outline of the information controlled by the “agent”.

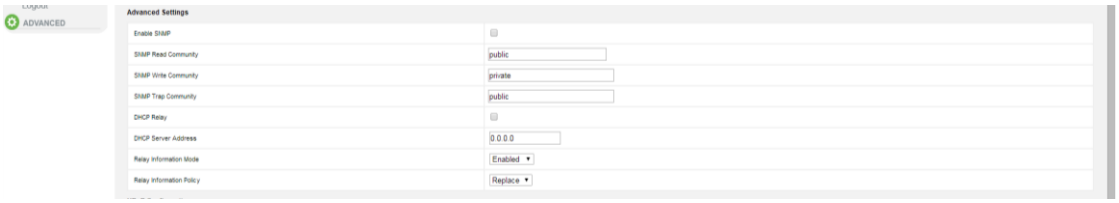
This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management software like ihiji can access this information. Community strings control the access to the onboard agent via SNMP v1 and v2c. The management software must first submit a valid community string for authentication before it can communicate with the switch.

The predefined default “groups” and “view” can be deleted from the system. Once deleted, you can then define customized groups and views for the SNMP clients that require access.

Use the Advanced Settings section to configure basic settings and traps for SNMP. You must first enable the protocol and configure the basic access parameters before you can manage the switch with SNMP. Trap messages can also be enabled but you first must enable the trap function and have a destination host specified before it will actually issue a message.

Path Settings, System, Advanced Settings

Figure 23. SNMP Configuration



Parameters

SNMP System Configuration:

- **Enable SNMP —** Enables or disables SNMP service. (Default: Enabled – SNMP v2c)
- **SNMP Read Community —** The community used for read-only access to the SNMP agent. (Range: 0-255 characters, Default: public)

  This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. For SNMPv3 settings, please go to Advanced->Security->SNMP.
- **Write Community —** The community used for read/write access to the SNMP agent. (Range: 0-255 characters, Default: private)

  This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy. For SNMPv3 settings, please go to Advanced->Security->SNMP.
- **SNMP Trap Community** — Specifies the community access string to use when sending SNMP trap packets. (Range: 0-255 characters, Default: public)

Configuration Instructions

To configure SNMP system and trap settings:

1. Click Settings, System.
2. In the Advanced Settings section, check Enable SNMP to enable SNMP service on the switch, and change the community access strings if required.
3. Click Apply.

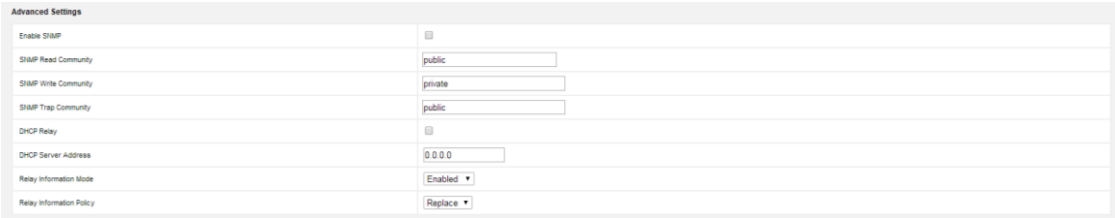
3.7.1.6— Configuring DHCP Relay and Option 82 Information

Use the DHCP Relay section to configure DHCP relay service for attached host devices. If a subnet does not include a DHCP server, you can relay DHCP client requests to a DHCP server on another subnet.

When the feature is enabled and the switch sees a DHCP request broadcast, it puts its own IP address into the request so that the DHCP server knows the subnet of the client, and then the switch forwards the packet to the DHCP server. When the server receives the DHCP request, it issues an IP address for the client from its defined DHCP range for the client's subnet, and sends a DHCP response back to the switch. The switch sends the DHCP response to the client.

DHCP Option 82 provides a way to send information about the switch and its DHCP clients to the DHCP server. This mechanism allows DHCP servers that support Option 82 to use the information when assigning IP addresses.

Figure 24. DHCP Relay and Option 82



With DHCP Relay Option 82, clients can be identified by the VLAN and switch port to which they are connected, rather than just MAC address. Thus, DHCP client-server messages are forwarded directly between the server and client without flooding the entire VLAN.

Path Settings, System, Advanced Settings

Parameters

- **DHCP Relay** — Enables or disables the DHCP relay function. (Default: Disabled)
- **DHCP Server Address** — IP address of DHCP server to be used by the switch's DHCP relay agent.
- **Relay Information Mode** — Enables or disables the DHCP Relay Option 82 support. Note that Relay Mode must also be enabled for Relay Information Mode to take effect. (Default: Enabled)
- **Relay Information Policy** — Sets the DHCP relay policy for DHCP client packets that include Option 82 information.
  - Replace — Overwrites the DHCP client packet information with the switch's relay information. (This is the default.)
  - Keep — Retains the client's DHCP information.
  - Drop — Drops the packet when it receives a DHCP message that already contains relay information.

Configuration Instructions To configure DHCP Relay:

1. Click Settings, System.
2. Enable the DHCP relay function, specify the DHCP server's IP address, enable Option 82 information mode, and set the method by which to handle relay information found in client packets.
3. Click Apply.

3.7.1.7— Configuring UPnP

Universal Plug and Play (UPnP) is a set of protocols that allows devices to connect seamlessly, and simplifies the deployment of home and office networks.

When a device is added to the network, the UPnP discovery protocol allows that device to broadcast its services to other UPnP devices on the network.

Once an UPnP control has discovered a device, it learns more about the device and its capabilities by requesting a description from the URL provided by the device in the discovery message. Then, it can send actions to the device's service.

Figure 25. UPnP Settings

Path Settings, System, UPnP Configuration

Parameters

- **Mode —** Enables/disables UPnP on the device. (Default: Disabled)
- **TTL —** Sets the time-to-live (TTL) value for UPnP messages transmitted by the switch. (Range: 4-255; Default: 4)
- **Advertising Duration —** The duration, carried in Simple Service Discover Protocol (SSDP) packets. Informs a control point or control points how often a SSDP advertisement message should be received from this switch. (Range: 100-86400 seconds; Default: 100 seconds)

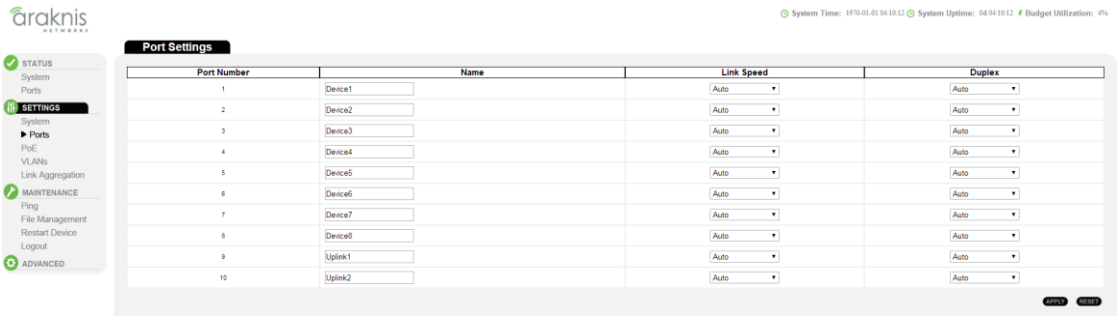
Configuration Instructions To configure UPnP:

1. Click Configuration, UPnP.
2. Enable or disable UPnP, then set the TTL and advertisement values.
3. Click Save.

3.7.2— Ports

Use the Port Settings page to configure the connection parameters for each port.

Figure 26. Port Settings Menu



3.7.2.1— Configuring Port Settings

By default, all ports support auto-negotiation for both speed and duplex. You can manually set the speed and duplex mode, disable specific ports, and change the name of an individual port.

Path Settings, Ports

Parameters

- **Port Number** – Lists the physical port number.
- **Port Name –** Change port name for each switch port. This feature can help better document and manage connected devices to the switch.
- **Link Speed** – Sets the port speed mode using auto-negotiation or manual selection. (Default Settings: Auto-negotiation enabled; advertised capabilities for RJ-45 ports: 1000BASE-T – 10half, 10full, 100half, 100full, 1000full; SFP: 1000BASE-SX/LX/LH – 1000full) The following options are supported:
  - Disabled – Disables the port. You can disable a port due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved by selecting Auto.
  - Auto – Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated with the connected devices based on that device's capabilities.
  - 1Gbps – Forces 1Gbps operation
  - 100Mbps – Forces 100Mbps operation
  - 10Mbps – Forces 10Mbps operation
- **Duplex** – Sets the port duplex mode using auto-negotiation or manual selection. The following options are supported:
  - **Auto** — Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities.
  - **Full** — Supports full duplex operation
  - **Half** — Supports half duplex operation

Caution! — It is highly advisable to leave duplex and speed settings at "Auto". In situations where it is necessary to force a certain setting on a port, make sure the other port is using the same settings.

The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

Configuration Instructions To configure port connection settings:

1. Click Settings, Ports.
2. Make any required changes to the connection settings.
3. Click Apply.

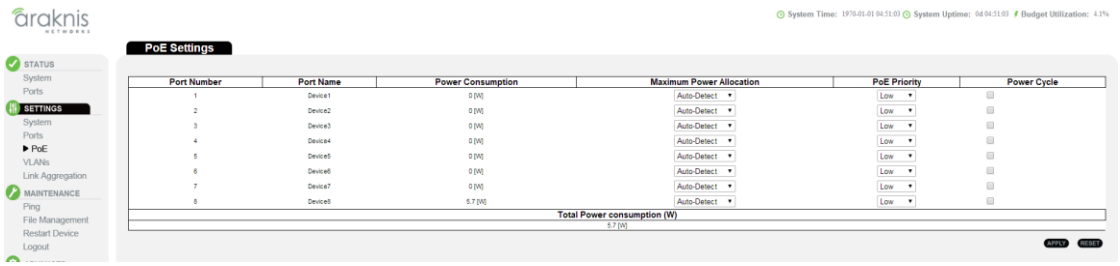
3.7.3— Power over Ethernet (for PoE Models Only)

Use the Power over Ethernet (PoE) Settings page to check Power Consumption on each port (as well as the entire system). Set Maximum Power Allocation for each port, shut down power on individual ports, power cycle individual or multiple ports, and set power allocation priority. If the power demand from devices connected to the switch exceeds the power budget, the switch uses port PoE Priority settings to limit the supplied power.

The switch can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. By default, an automatic detection process is initialized by the switch when a PoE-capable device is connected to any of the switch ports. Detection and authentication prevent damage to non-compliant devices (IEEE 802.3af or 802.3at).

This switch supports both the IEEE 802.3af PoE and IEEE 802.3at-2009 PoE Plus (PoE+) standards. To ensure that the correct power is supplied to Powered Devices (PD) compliant with these standards, the first detection pulse from the switch is based on 802.3af to which the 802.3af PDs will respond normally. It then sends a second PoE Plus pulse that causes an 802.3at PD to respond as a Class 4 device and draw Class 4 current. Afterwards, the switch exchanges information with the PD such as duty-cycle, peak and average power needs.

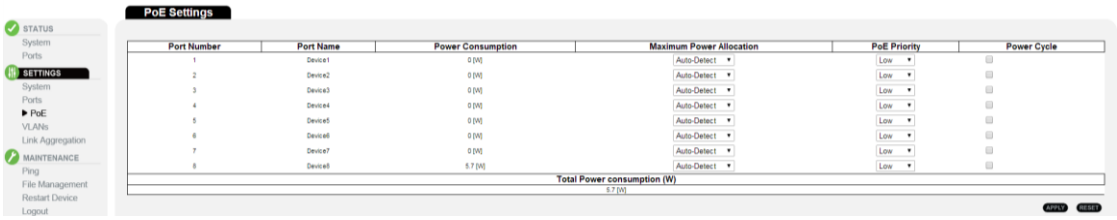
Figure 27. PoE Settings



Individual Port power can be turned on and off, and a per-port power priority can be set so that the switch never exceeds its power budget. When a device is connected to a switch port, its power requirements are detected by the switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied. Since the end device is still connected, it will attempt to establish a connection. This results in a behavior that looks like a constant reset on the port.

Ports can be set to one of three power priority levels, high, medium, or low. Ports set at high to medium priority have power enabled in preference to those ports set at low priority. For example, when a device connected to a port is set to critical priority, the switch supplies the required power, if necessary, by denying power to ports set for a lower priority during boot-up.

Figure 28. PoE Settings



Path Settings, PoE

Parameters These parameters are displayed:

- **Port Number** – Port identifier.
- **Port Name** – Port name.
- **Power Consumption** – Live counter of current power consumption in Watts for the port.
- **Maximum Power Allocation** – The PoE operating mode for a port includes these options:
  - **Disabled** – PoE is disabled for the port.
  - **AutoDetect** – The port automatically determines how much power to reserve according to the class to which the connected PD belongs, and reserves power accordingly. Three different classes exist, including 7, 15.4, or 30 Watts.
  - **7W** – Forces 7W maximum power allocated for this port.
  - **15.4W (PoE)** – Enables PoE IEEE 802.3af (Class 4 PDs limited to 15.4W)
  - **30.0W (PoE+)** – Enables PoE+ IEEE 802.3at (Class 4 PDs limited to 34.2W)
- **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.
- **Power Cycle** – A check mark to power cycle PoE on that specific port. You can select multiple ports or all ports at the same time.

Caution! — It is highly advisable to leave the “Maximum Power Allocation” setting on AutoDetect. Improper configuration (e.g. connecting a 9W device on a 7W port) will result in power reset every time the connected device requests more than the Maximum Allocated Power.

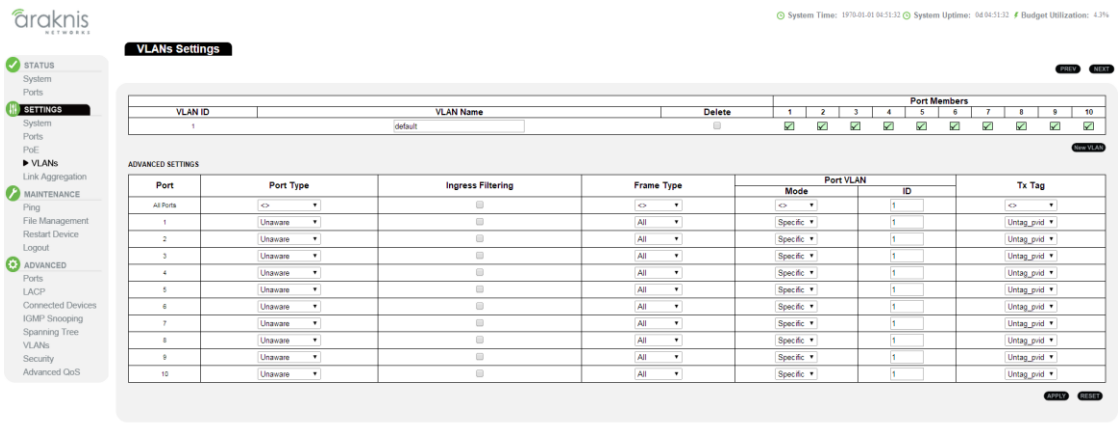
Configuration Instructions To configure port-specific PoE settings:

1. Click Settings, PoE.
2. Specify the port maximum power allocation and priority.
3. Click Apply.

3.7.4— VLANs

The Virtual Local Area Network (VLAN) technology allows you to divide physical ports to different logical groups. Each group is a virtual LAN, the clients within the VLAN are a broadcast domain. If clients in different VLANs need to communicate, connect the VLAN to an additional upper router (or a L3 device).

Figure 29. VLANs Settings Page



VLANs provide greater network efficiency and reduce broadcast traffic by isolating multicast and broadcast into their originating VLANs.

This switch supports the following VLAN features:

- Up to 4,095 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- Port overlapping, allowing a port to participate in multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices

3.7.4.1— Creating New VLANs

By default, all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs.

Use the VLANs Settings page to enable VLANs for this switch by assigning each port to the VLAN group(s) in which it will participate.

Figure 30. VLAN Settings – Assigning Ports

Path Settings, VLANs

Parameters These parameters are displayed:

- **VLAN ID** — VLAN Identifier. (Range: 1-4095)
- **VLAN Name** — The name of a VLAN. (Range: 1-32 alphanumeric characters)
- **Delete —** Delete an existing VLAN with all port membership associations.
- **Port Members** — Add ports to a VLAN by simply clicking on the check mark associated with that port.
  - To include a port in a VLAN, check the box as shown ✓.
  - To include a port in a forbidden port list, check the box as shown ✗.
  - To remove or exclude the port from the VLAN, make sure the box is unchecked.

Pro Tip – If you implement VLANs that do not overlap but still need to communicate, you must connect them through a router or a L3 device.

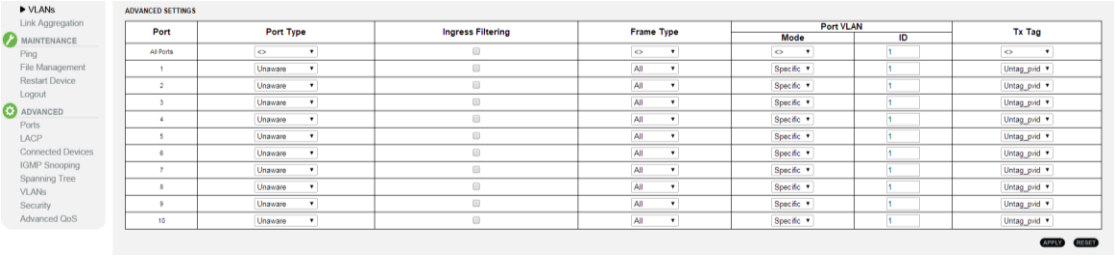
Configuration Instructions To configure IEEE 802.1Q VLAN groups:

1. Click Settings, VLANs.
2. Change the ports assigned to the default VLAN (VLAN 1) if required.
3. To configure a new VLAN, click New VLAN, enter the VLAN ID, the VLAN name, and then mark the ports to be assigned to the new group.
4. Click Apply.

3.7.4.2— Configuring VLAN Attributes For Port Members

Use the Advanced Settings section to configure VLAN attributes for specific ports, including enabling ingress filtering, setting the accepted frame types, and configuring the default VLAN identifier (PVID).

Figure 31. VLAN Settings — Configuring Attributes



Path Settings, VLANs

Parameters These parameters are displayed:

- **Port** — Port identifier.
- **Port Type** — Configure how a port processes the VLAN ID in ingress frames. (Default: Unaware)
  - **C-port** — For customer ports, each frame is assigned to the VLAN indicated in the VLAN tag, and the tag is removed.
  - **S-port** — For service ports, the EtherType of all received frames is changed to 0x88a8 to indicate that double-tagged frames are being forwarded across the switch. The switch will pass these frames on to the VLAN indicated in the outer tag. It will not strip the outer tag, nor change any components of the tag other than the EtherType field.
  - **S-custom-port** — For custom service ports, the EtherType of all received frames is changed to value set in the Ethertype for Custom S-ports field to indicate that double-tagged frames are being forwarded across the switch. The switch will pass these frames on to the VLAN indicated in the outer tag. It will not strip the outer tag, nor change any components of the tag other than the EtherType field.
  - **Unaware** — All frames are classified to the Port VLAN ID and tags are not removed.
- **Ingress Filtering** — Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Disabled)

  Ingress filtering only affects tagged frames.

  If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be dropped.

  If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports.
- **Frame Type** — Set the interface to accept all frame types, including tagged or untagged frames, only tagged frames, or only untagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. When set to receive only tagged frames, all untagged frames received on the interface are discarded. (Options: All, Tagged, Untagged; Default: All)
- **Port VLAN Mode** — Determine how to process VLAN tags for ingress and egress traffic. (Options: None, Specific; Default: Specific)
  - **None** — The ID for the VLAN to which this frame has been assigned is inserted in frames transmitted from the port. The assigned VLAN ID can be based on the ingress tag for tagged frames, or the default PVID for untagged ingress frames. Note that this mode is normally used for ports connected to VLAN-aware switches.
  - **Specific** — A *Port VLAN ID* can be configured (as described below). Untagged frames received on the port are classified to the Port VLAN ID. If Port Type is Unaware, all frames received on the port are classified to the Port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the Port VLAN ID, a VLAN tag with

the classified VLAN ID is inserted in the frame.

- When forwarding a frame from this switch along a path that contains any VLAN-aware devices, the switch should include VLAN tags. When forwarding a frame from this switch along a path that does not contain any VLAN-aware devices (including the destination host), the switch should first strip off the VLAN tag before forwarding the frame.

- **Port VLAN ID** — VLAN ID assigned to untagged frames received on the interface. The port must be a member of the same VLAN as the Port VLAN ID. (Range: 1-4095; Default: 1)
- **Tx Tag** — Determines egress tagging for a port:
  - **Untag_pvid —** All VLANs except for the native VLAN (the one using the PVID) will be tagged**.**
  - **Tag_all** — All VLANs are tagged.
  - **Untag_all —** All VLANs are untagged.

Configuration Instructions

To configure attributes for VLAN port members:

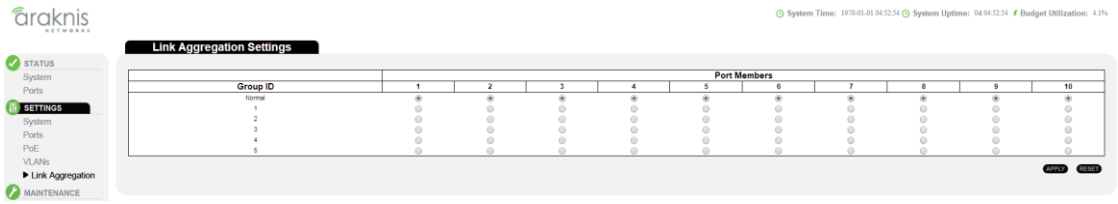
1. Click Settings, VLANs.
2. Configure in the required settings for each interface.
3. Click Apply.

3.7.5— Link Aggregation

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

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

Figure 32. Link Aggregation Settings



Path Settings, Link Aggregation

Parameters

- **Group ID** – Link Aggregation Group Identifier
- **Port Members** – Port Identifier

Configuration Instructions To configure static Link Aggregation Groups (LAGs):

1. Click Settings, Link Aggregation.
2. Select one or more port members to each Link Aggregation Group.
3. Click Apply.
4. Make sure that port members on the other side of the LAG are members of the same Group ID.

Pro Tip — To avoid creating a loop in the network, be sure to add a static trunk using the configuration interface before connecting physical ports. Also, disconnect physical ports before removing a static trunk via the interface.

3.8— Maintenance Menu

3.8.1— Pinging an IP Address

The Ping page is used to send ICMP echo request packets to another device on the network to determine if it can be reached.

Figure 33. ICMP Ping

Path Maintenance, Ping

Parameters These parameters are displayed on the Ping page:

- **IP Address** – IP address of the host.
  An IPv4 address consists of 4 numbers, 0 to 255, separated by periods.
- **Ping Size** – The payload size of the ICMP packet. (Range: 8 - 1400 bytes)

Configuration Instructions

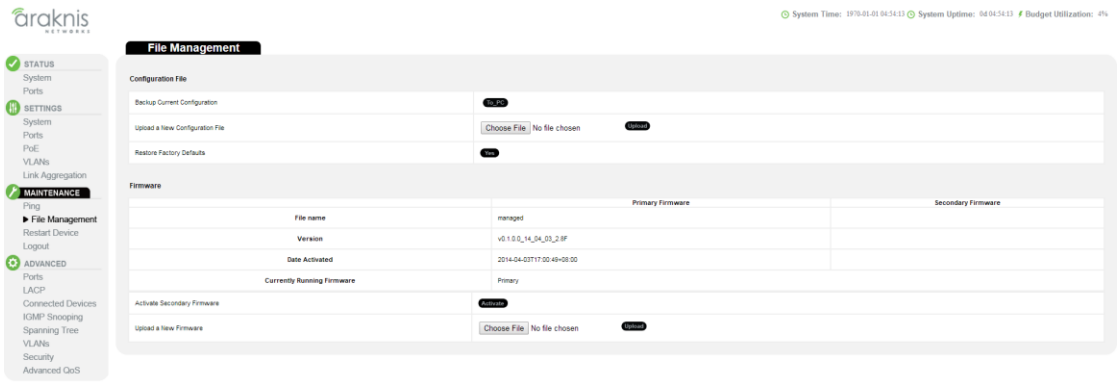
1. To ping another device on the network:
2. Click Maintenance, Ping.
3. Enter the IP address of the target device.
4. Specify the packet size.
5. Click Apply.

After you press Start, five ICMP packets are transmitted, and the sequence number and round-trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

3.8.2— File Management

Use the File Management Page to make backups of your configuration, load configuration files, and manage firmware updates and versions.

Figure 35. File Management Page



3.8.2.1— Saving Configuration Settings

Use the Back Current Configuration option to save the current configuration settings to a file on your local management station.

Path Maintenance, File Management, Configuration File

Configuration Instructions To save your current configuration settings:

1. Click Maintenance, File Management.
2. Click the “To_PC” button next to “Back Current Configuration”.

The configuration file is in XML format. The configuration parameters are represented as attribute values. When saving the configuration from the switch, the entire configuration including syntax descriptions is included in the file. The file may be modified using an editor and loaded to a switch.

3.8.2.2— Restoring Configuration Settings

Use the Upload a New Configuration File option to restore previously saved configuration settings to the switch from a file on your local management station.

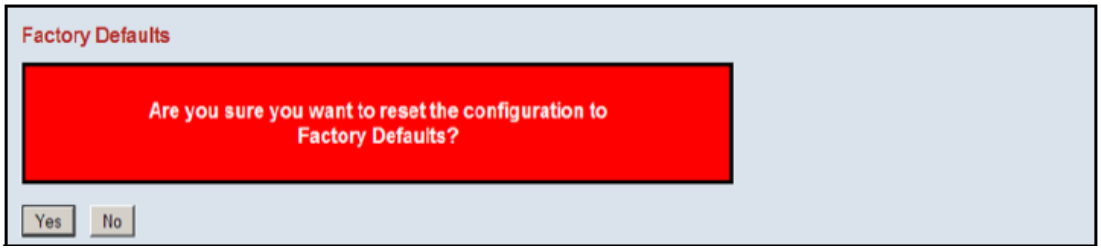
Path Maintenance, File Management, Configuration File

Configuration Instructions To restore your current configuration settings:

1. Click Maintenance, File Management.
2. Click the “Choose File” button next to “Upload a New Configuration File,” and select the configuration file.
3. Click the Upload button to restore the switch’s settings.

3.8.2.3— Restoring Factory Defaults

Figure 36. Restore Factory Defaults



Use the Configuration File section to restore the original factory settings. Note that the LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory defaults.

Path Maintenance, File Management, Configuration File

Configuration Instructions To restore factory defaults:

1. Click Maintenance, File Management.
2. Click Yes next to “Restore Factory Defaults.”

The factory defaults are immediately restored. No reboot is necessary.

3.8.2.4— Hardware Factory Default

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

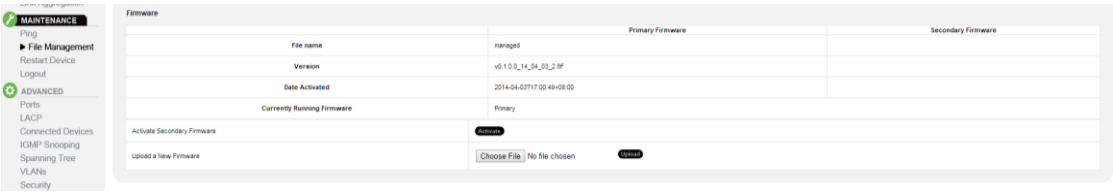
Configuration Instructions To perform a hardware reset:

1. Using the same Ethernet cable, plug one end into Port 1 and the other end into Port 2.
2. Power the switch off, wait a couple of seconds and then power switch back on.
3. Wait until the activity lights activate on Ports 1 and 2, then remove the Ethernet cable.
4. Restart the setup process.

3.8.2.5— Activating a Secondary Firmware

There are two images saved within the switch: Primary and Secondary. This page provides information about the active and alternate (Secondary) firmware images in the device, and allows you to revert to the alternate image. The web page displays two tables with information about the active and alternate firmware images.

Figure 37. Firmware Menu



Path Maintenance, File Management, Firmware

Configuration Instructions Click on Activate to revert to the Secondary image.

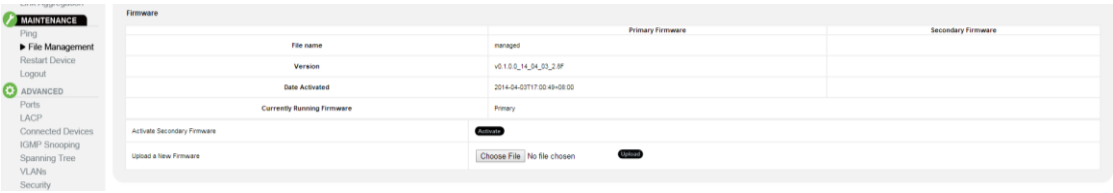
Pro Tip

- In case the active firmware image is the alternate image, only the "Active Image" table is shown. In this case, the Activate Alternate Image button is also disabled.
- If the alternate image is active (due to a corruption of the primary image or by manual intervention), uploading a new firmware image to the device will automatically use the primary image slot and activate this.
- The firmware version and date information may be empty for older firmware releases. This does not constitute an error.

3.8.2.6— Upgrading Firmware

Use the Firmware section to upgrade the switch's system firmware using a file provided by Araknis® Networks.

Figure 38. Firmware Update



Path Maintenance, File Management, Software Image

Caution! — Do not reset or power off the device during firmware upgrade or the switch may fail to function afterwards.

Configuration Instructions To upgrade firmware:

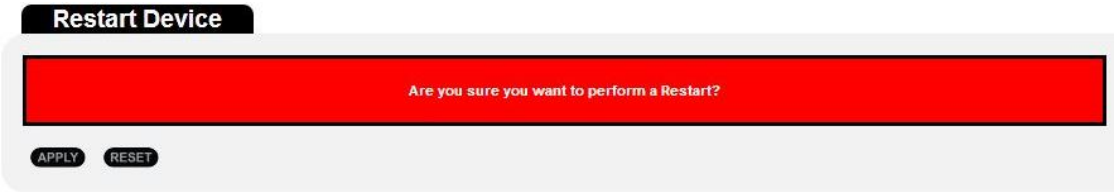
1. Click Maintenance, File Management.
2. Click the Choose File button next to "Upload a New Software Image," and select the firmware file.
3. Click the Upload button to upgrade the switch's firmware.

After the software image is uploaded, a page announces that the firmware update has been initiated. After about a minute, the firmware is updated and the switch is rebooted.

3.8.3— Restart Device

Use the Restart Device page to restart the switch.

Figure 39. Restart Device



Path Maintenance, Restart Device

Configuration Instructions To restart the switch:

1. Click Maintenance, Restart Device.
2. Click Yes.
3. The restart is complete when the user interface displays the login page again.

4.1— Ports

The Advanced Ports menu has two sub-menus: Ports Statistics and Port Settings. Use Port Statistics page to view detailed counters for each port. Use Port Settings to view advanced features for each port on the switch such as Maximum Frame Size.

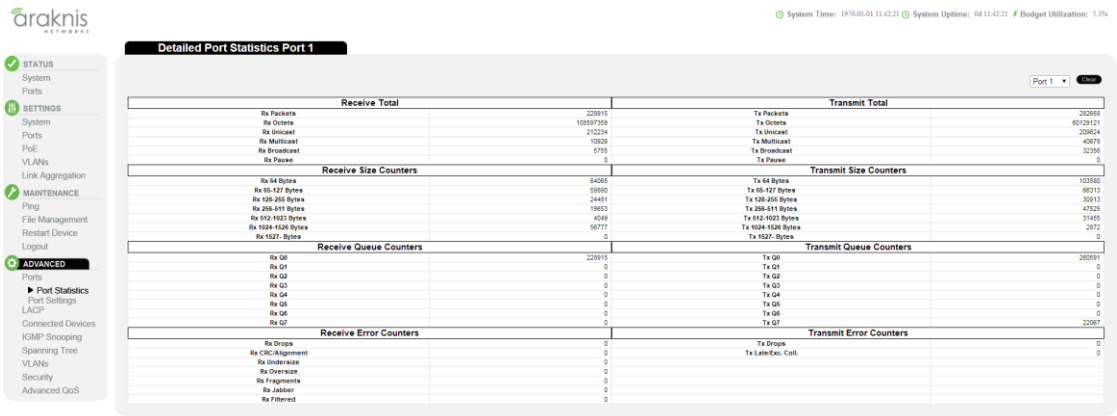
4.1.1— Port Statistics

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 certain switch port to view.
- Press the “Clear” button to reset the statistics for the selected port.

Path Advanced, Port, Port Statistics

Figure 40. Detailed Port Statistics



Parameters

- **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/Transmit 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.

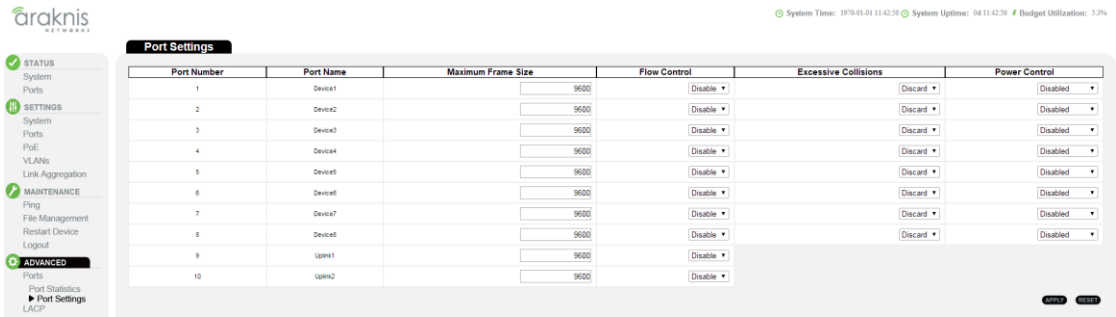
(continued on next page)

- **Receive Error Counters**
  - **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.
  - **Rx Undersize** – The total number of frames received that were less than 64 octets long excluding framing bits, but including FCS octets.
  - **Rx Oversize** – The 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** – The 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.
  - **Rx Jabber** – The 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 Filtered** – The number of frames received filtered by the forwarding process. The switch support Store-and-Forward forwarding process.
- **Transmit Error Counters**
  - **Tx Drops** – The number of dropped frames due to output buffer overload.
  - **Tx Late/Exc. Coll.** – The number of dropped frames due to late or excessive collisions.

4.1.2— Configuring Advanced Port Settings

Use the Port Settings menu to configure the advanced parameters for each port. This page includes options for setting the maximum frame size, enabling flow control, specifying the behavior in response to excessive collisions, or enabling power-saving mode.

Figure 41. Advanced Port Settings



Path Advanced, Ports, Port Settings

Parameters

- **Port Number —** Lists the physical port number.
- **Port Name —** Displays the name of the port.
- **Maximum Frame Size** — Sets the maximum transmit unit (MTU) for traffic going through the switch. Received packets that exceed the maximum frame size configured on the switch port are dropped. (Range: 1518-9600 bytes; Default: 9600 bytes). 9600 bytes maximum frame size is also referred to as Jumbo Frame.
- **Excessive Collision Mode —** Sets the behavior of the switch when excessive transmit collisions are detected on a specific port. The following behaviors are available to be configured for each switch port.
  - **Discard —** Discards a frame after 16 collisions (default).
  - **Restart —** Restarts the back-off algorithm after 16 collisions.
- **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)

When auto-negotiation is used (enabled by default), this parameter indicates the flow control capability advertised to the connected device. When the speed and duplex mode are manually configured, the Current Rx field indicates whether PAUSE frames are followed by this port (i.e. received from the connected device), and the Current Tx field indicates if PAUSE frames are sent from this port.

- **Power Control** — Adjusts the power provided to ports based on the length of the cable used to connect to other devices. When enabled, only sufficient power to maintain a connection is used. Enabling power-saving mode can significantly reduce power used for cable lengths of 20 meters or fewer whereas the IEEE 802.3 standard power requirements are specified for cable lengths of 100 meters.

  The following options are available:

  - **Disabled** – All power-savings mechanisms disabled (default).
  - **ActiPHY** – Link down power savings enabled.
  - **PerfectReach** – Link up power savings enabled.
- **Enabled** – Both link up and link down power savings enabled.

Configuration Instructions

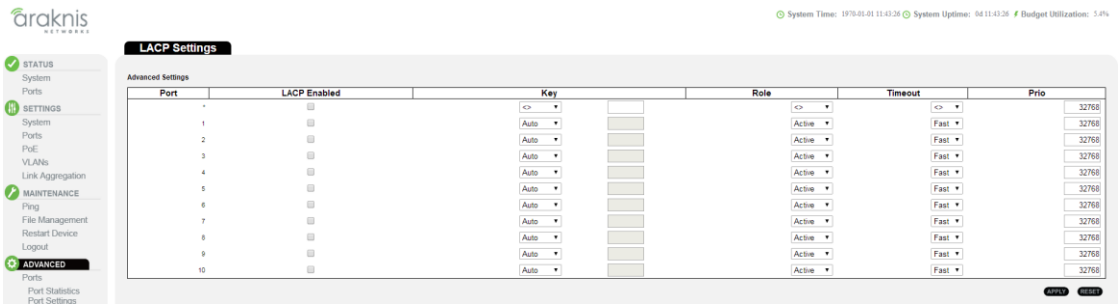
To configure port connection settings:

1. Click Settings, Ports.
2. Make any required changes to the connection settings.
3. Click Apply.

4.2— LACP

Use the Link Aggregation Control Protocol (LACP) menu to enable dynamic Link Aggregation (LACP) on selected ports, configure the administrative key, and the protocol initiation mode.

Figure 42. LACP Settings



Path Advanced, LACP

Parameters

- **Port** – Port identifier.
- **LACP Enabled** – Enables/Disables LACP on a particular switch port.
- **Key** – The LACP administration key must be set to the same value for ports that belong to the same Link Aggregation Group (LAG). (Range: 0-65535; Default: Auto). The following options are available.
  - **Specific —** Manually configure a key.
  - **Auto –** Automatically set the key based on the actual link speed, where 10Mbps = 1, 100Mbps = 2, and 1Gbps = 3.
- **Role** – Configures active or passive LACP initiation mode. Use Active option to initiate LACP negotiation on a port (one initiation packet each second). Use Passive option to make the port wait until it receives an LACP initiation packet from the connected device before beginning to establish a LAG.
- **Timeout –** Sets the timeout for the LACP session. The timeout value is the amount of time that a port waits for a LACPDU from the connected device before the LACP session is terminated. The default time out value is Fast (3 seconds); Slow is 90 seconds.
- **Priority –** Specifies the priority for the physical interface in LACP negotiation. Value range is from 1 to 65535. The higher the number, the lower the priority. (Default is 32768)

Configuration Instructions To configure a dynamic trunk:

1. Click Advanced, LACP.
2. Enable LACP on all of the ports to be used in an LAG.
3. Specify the LACP Admin Key to restrict a port to a specific LAG.
4. Set at least one of the ports in each LAG to Active initiation mode, either at the near end or far end of the trunk.
5. Click Apply.

Pro Tip

- To avoid creating a loop in the network, be sure you enable LACP before physically connecting the ports, and also physically disconnect the ports before disabling LACP.
- If the paired switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- All ports on both ends of an LACP trunk must be configured for full duplex, either manually

or auto-negotiation.

- Ports assigned to a common link aggregation group (LAG) must meet the following criteria:
  - Ports must have the same LACP Admin Key. Using Auto option of the Admin Key will avoid this problem.
  - One of the ports at either the near end or far end must be set to active initiation mode.

4.3— Connected Devices

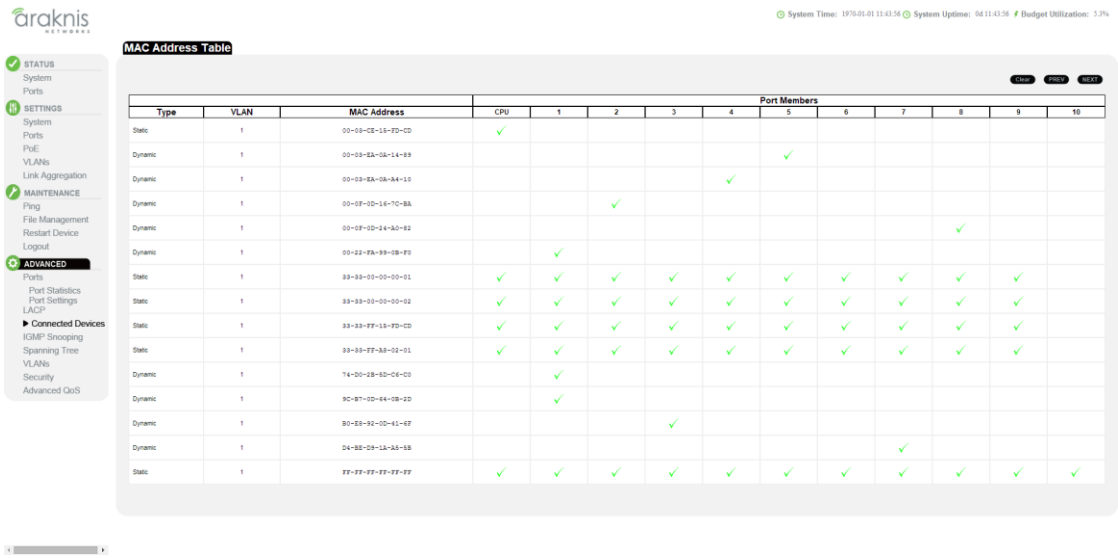
Link Layer Discovery Protocol (LLDP) is used to discover basic information about other devices in the same broadcast domain (i.e. VLAN). Advertised information is defined in IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings.

4.3.1— MAC Address Table

Use the MAC Address Table to display dynamic and static address entries associated with the CPU and each port.

Path Advanced, Connected Devices

Figure 43. MAC Address Table



Type	VLAN	MAC Address	Port Members										
			CPU	1	2	3	4	5	6	7	8	9	10
Static	1	00-03-CE-16-FD-CD	✓										
Dynamic	1	00-03-EA-0A-14-89						✓					
Dynamic	1	00-03-EA-0A-A4-10					✓						
Dynamic	1	00-0F-0D-16-7C-BA			✓								
Dynamic	1	00-0F-0D-24-A0-82									✓		
Dynamic	1	00-22-FA-99-0B-F0		✓									
Static	1	33-33-00-00-00-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Static	1	33-33-00-00-00-02	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Static	1	33-33-FF-16-FD-CD	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Static	1	33-33-FF-A8-02-01	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Dynamic	1	74-DC-2B-5D-C6-C0		✓									
Dynamic	1	9C-B7-0D-64-0B-2D		✓									
Dynamic	1	B0-E8-92-0D-41-6F				✓							
Dynamic	1	D4-BE-D9-1A-A5-5B								✓			
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Parameters

- **Type** – Indicates whether the entry is static or dynamic. Dynamic MAC addresses are learned by monitoring the source address for traffic entering the switch.
- **VLAN** – The VLAN containing this entry.
- **MAC Address** – Physical address associated with this interface.
- **Port Members** – The ports associated with this entry.

4.4— IGMP Snooping

Multicasting is used to support real-time applications like control systems or streaming audio. Using multicast, a server does not have to establish individual connections with each target client. The server broadcasts its service to the network, and any client that wants to receive the multicast stream simply subscribes to the multicast service with their connected switch.

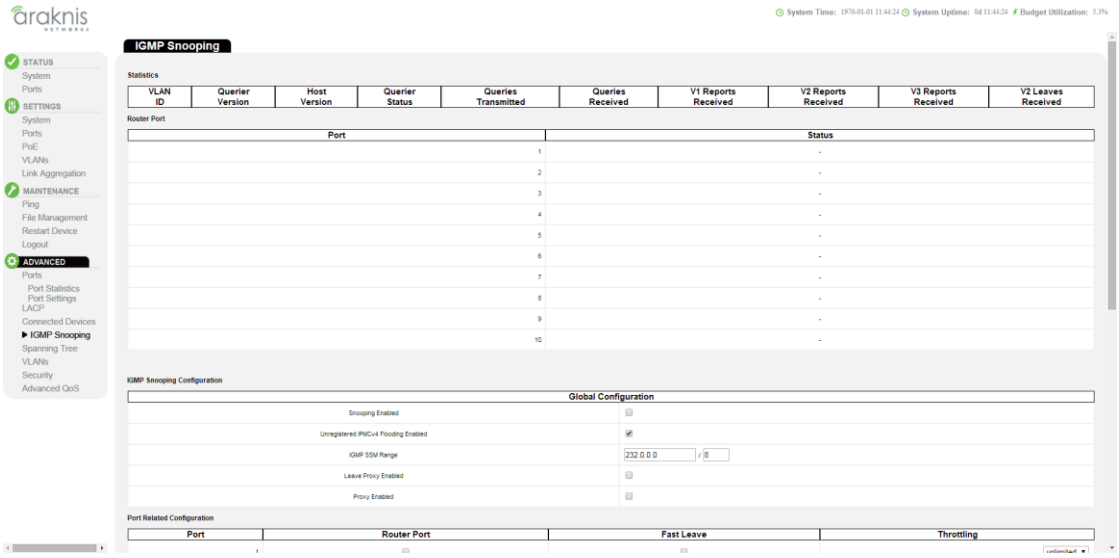
This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor exchanges between connected clients and an IGMP-enabled multicast server. Therefore, the switch can discover the clients that want to join a multicast group, and set its filters accordingly.

The goal of multicast filtering is to optimize network performance, so multicast packets will only be forwarded to those ports that connect multicast group clients or multicast switches, instead of flooding traffic to all ports in the subnet (VLAN).

IGMP Query can be used to actively ask the connected clients if they want to receive a specific multicast service. Then, IGMP Query identifies the ports containing clients requesting to join the service and sends multicast data to those ports only. 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.

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.

Figure 44. IGMP Snooping Page



4.4.1— IGMP Snooping Statistics

Use the IGMP Snooping page to display IGMP querier status, snooping statistics for each VLAN carrying IGMP traffic, and the ports connected to an upstream multicast router/switch.

Figure 45. IGMP Snooping Statistics

Path Advanced, IGMP Snooping

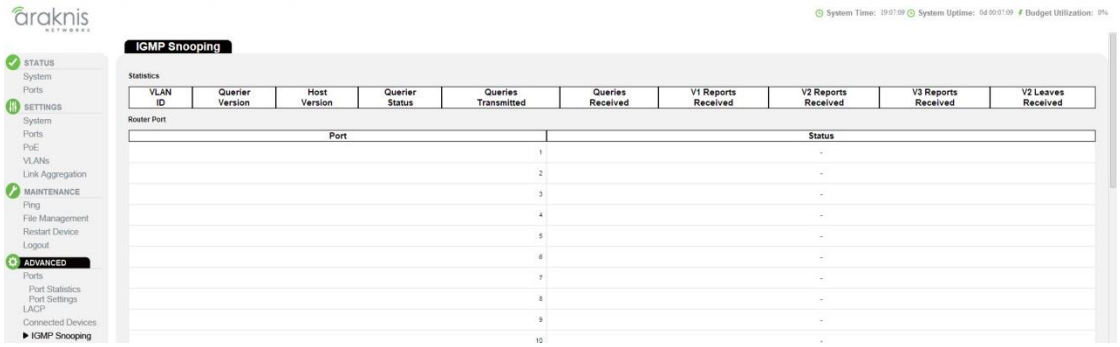
Parameters

- **VLAN ID** – VLAN Identifier.
- **Querier Version** – IGMP version used by the switch when acting as the IGMP querier.
- **Host Version** – IGMP version used this switch when acting as a host in IGMP proxy mode.
- **Querier Status** – Shows the Querier status as “ACTIVE” or “IDLE.” When enabled, the switch can be the Querier for IGMP traffic and becomes responsible for asking clients if they want to subscribe to multicast service.
- **Querier Transmitted** – The number of Querier messages sent.
- **Querier Received** – The number of Querier messages received.
- **V1 Reports Received** – The number of IGMP Version 1 reports received.
- **V2 Reports Received** – The number of IGMP Version 2 reports received.
- **V3 Reports Received** – The number of IGMP Version 3 reports received.
- **V2 Leaves Received** – The number of IGMP Version 2 leave reports received.

4.4.2— Router Port Status

This table displays current status of IGMP router ports.

Figure 46. IGMP Snooping Ports



Path Advanced, IGMP Snooping

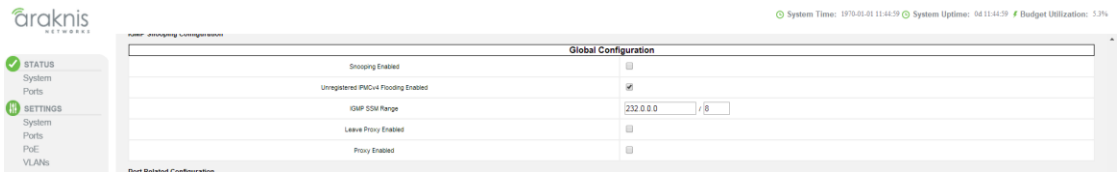
Parameters

- **Port** – Port Identifier.
- **Status** – Ports connected to multicast servers may be dynamically discovered or statically assigned to a port on this switch.

4.4.3— Configuring Global Settings for IGMP Snooping

Use the IGMP Snooping Configuration table to configure global settings that control the forwarding of multicast traffic. When enabled, the switch forwards traffic only to the ports that request multicast traffic as opposed to the switch broadcasting the traffic to all ports and possibly disrupting network performance.

Figure 47. IGMP Snooping Configuration



Path Advanced, IGMP Snooping

Parameters

- **Snooping Enabled** — When enabled, the switch monitors network traffic passing through it to determine which connected clients want to receive multicast traffic. (Default: Disabled)
- **Unregistered IPMC Flooding Enabled** – Floods unregistered multicast traffic into the same VLAN. (Default: Enabled)
- **Leave Proxy Enabled** – Discards IGMP leave messages unless received from the last member port in the group. (Default: Disabled)

  Leave proxy is also included in the general proxy function described below. Therefore if Leave Proxy Enabled is not selected, but Proxy Enabled is selected, leave proxy will still be performed.
- **Proxy Enabled** – Enables IGMP Snooping with Proxy Reporting. (Default: Disabled)

  When proxy reporting is enabled, the switch performs report suppression, last leave, and query suppression.

  Report suppression summarizes IGMP reports coming from connected clients. Last leave sends out a proxy query when the last member leaves a multicast group. Query suppression means that neither specific queries nor general queries are forwarded from the multicast server to connected multicast group members.

  When proxy reporting is disabled, all IGMP reports received by the switch are forwarded to the multicast server.

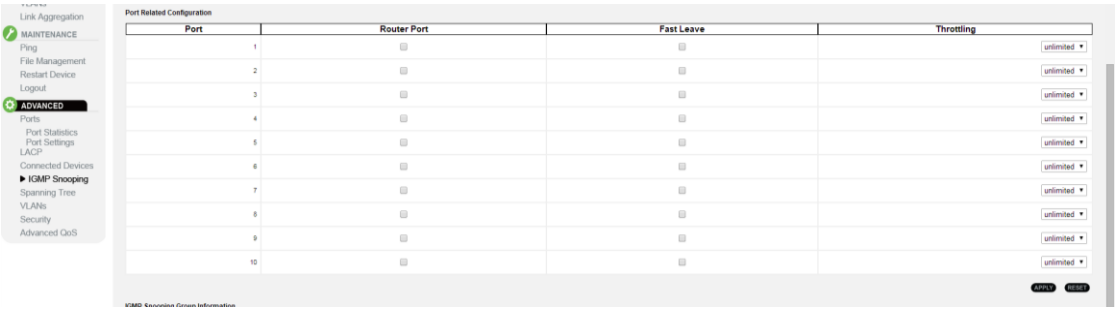
Configuration Instructions To configure global settings for IGMP Snooping:

1. Click Advanced, IGMP Snooping.
2. Adjust the IGMP settings as required.
3. Click Apply.

4.4.4— Configuring Port Related Settings for IGMP Snooping

Use this page to configure port related IGMP Snooping settings.

Figure 48. IGMP Port Related Configuration



Path Advanced, IGMP Snooping

Parameters

- **Port** — Port identifier.
- **Router Port** — Sets a port to function as a router port, which connects to a Layer 3 multicast server or IGMP querier. (Default: Disabled)

  If IGMP snooping cannot automatically locate the IGMP querier, you can manually configure a port connected to a known IGMP querier (i.e., a multicast server). This port will then join all the current multicast groups supported by the attached multicast server/switch to ensure that multicast traffic is forwarded to all subscribed ports within the switch.
- **Fast Leave** — Immediately deletes a member port of a multicast service if a leave packet is received at that port. (Default: Disabled)

  If Fast Leave is not used, a multicast server (or querier) will send a GS-query message when an IGMPv2/v3 group leave message is received. The server/querier stops forwarding traffic for that group only if no host replies to the query within the specified timeout period.

  Fast Leave can improve network performance for a network that frequently experiences many IGMP host add and leave requests.
- **Throttling** — Limits the number of multicast groups that a port can be a member of at the same time. When the maximum number of groups is reached on a port, any new IGMP join reports will be dropped. (Range: 1-10; Default: unlimited)

Configuration Instructions To configure global and port-related settings for IGMP Snooping:

1. Click Advanced, IGMP Snooping.
2. Adjust the IGMP settings as required.
3. Click Apply.

4.4.5— Showing IGMP Snooping Group Information

Use the IGMP Snooping Group Information section to display the port members of each service group.

Figure 49. IGMP Snooping Group Information

Path Advanced, IGMP Snooping

Parameters These parameters are displayed:

- **VLAN ID** – VLAN Identifier.
- **Groups** – The IP address for a specific multicast service.
- **Port Members** – The ports assigned to the listed VLAN, which broadcasts a specific multicast service.

4.4.6— Configuring IGMP Filtering

Use the IGMP Snooping Port Group Filtering Configuration section to filter specific multicast traffic. In certain switch applications, the network administrator may want to control the multicast services that are available to end users. IGMP filtering enables denying access to specified multicast services on a switch port.

Figure 50. Configuring IGMP Filtering

Path Advanced, IGMP Snooping

Parameters These parameters are displayed:

- **Delete** – Delete a certain Filtering Group.
- **Port** – Port identifier.
- **Filtering Groups –** Multicast groups that are denied on a port. When filter groups are defined, all IGMP join reports received on a port are checked against these groups. If a requested multicast group is denied, the IGMP join report is dropped.

4.4.6.1— Showing IGMP SSM Information

Use the IGMP SSM Information section to display IGMP Source-Specific Information including group, filtering mode (include or exclude), source address, and type (allow or deny).

Figure 51. Showing IGMP SSM Information

Path Advanced, IGMP Snooping

Parameters

- **VLAN ID** – VLAN Identifier.
- **Group** – The IP address of a multicast group detected on this interface.
- **Port** – Port identifier.
- **Mode** – The filtering mode per VLAN ID, port number, and Group Address. It can be either Include or Exclude.
- **Source Address** – IP Address of the source. Currently, the system limits the total number of IP source addresses for filtering to 128.

  Different source addresses belonging to the same group are treated as single entry.
- **Type** –May be set to either Allow or Deny.

4.5— Spanning Tree

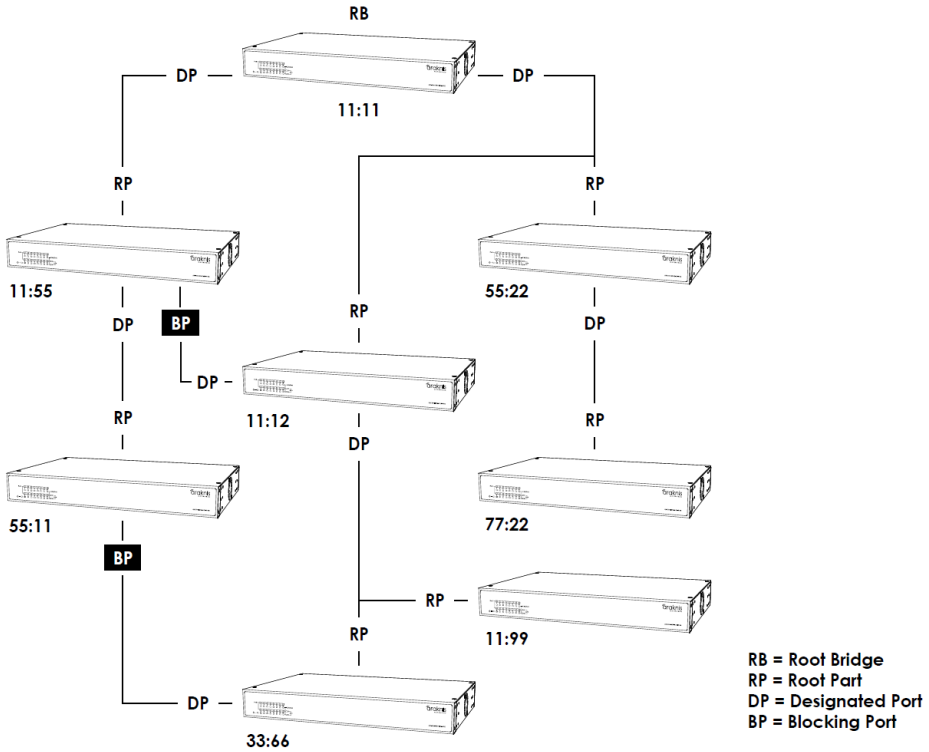
The Spanning Tree Protocol (STP) can be used to detect and eliminate network loops. This allows the switch to communicate with other switches in the network to ensure only one route exists between any two end devices, and provide backup routes which automatically take over when a primary route goes down.

The spanning tree protocol supported by this switch includes these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a switch that serves 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. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

Figure 52. STP 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 and make the network stable again.

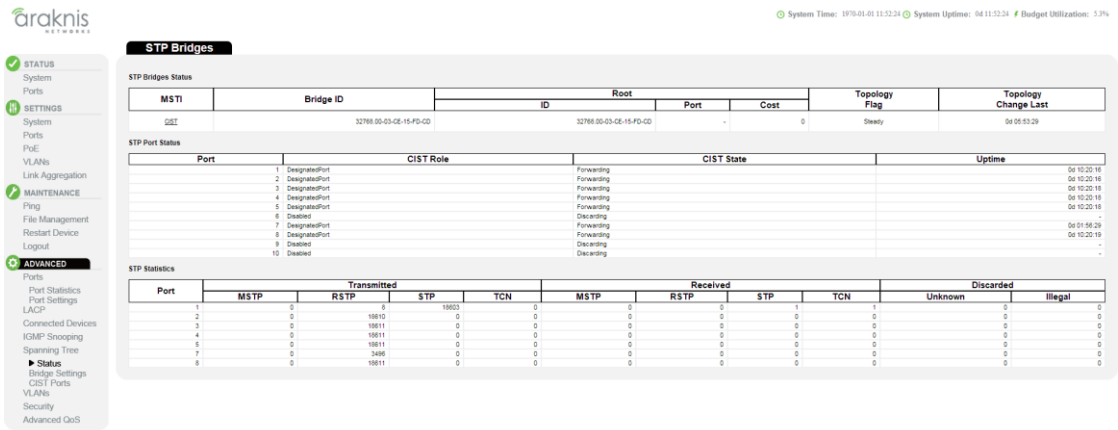
RSTP — RSTP is an enhancement on the slower, legacy STP. RSTP is also included in MSTP. RSTP performs faster reconfiguration when topology change is detected (1 to 3 seconds for RSTP, compared to 30 seconds or more for STP).

MSTP – MSTP is 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).

4.5.1— Status

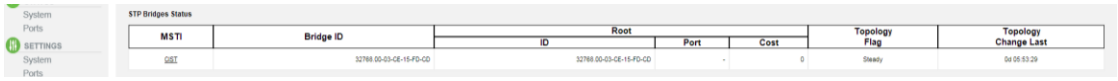
Use the Status Page for Spanning Tree to display information on spanning tree bridge status, the functional status of participating ports, and statistics on spanning tree protocol packets.

Figure 53. STP Bridges Status



4.5.1.1— STP Bridges Status

Figure 54. STP Bridges Status



Path Advanced, Spanning Tree, Status

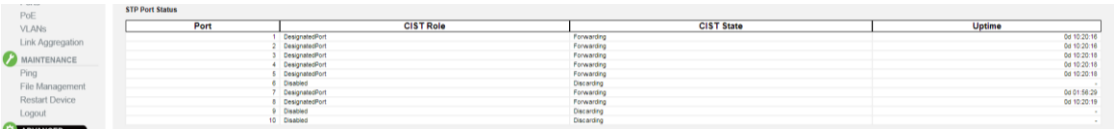
Parameters

- **MSTI** – The Bridge Instance.
- **Bridge ID** – A unique identifier for this switch, consisting of the bridge priority, and MAC address of the switch.
- **Root ID** – The Bridge ID of the Root Bridge in the current topology.
- **Root Port** – The port number on this switch that has the lowest path cost to the Root Bridge. This switch communicates with the root device through this port. If there is no root port, then this switch is the Root Bridge of the current topology.
- **Root Cost** – The path cost from the root port on this switch to the Root Bridge. For the Root Bridge this is zero. For all other switches, it is the sum of the port path costs on the lowest path to the Root Bridge.
- **Topology Flag** – The current state of the Topology Change Notification flag (TCN) for this bridge instance.
- **Topology Change Last** – Time since the Spanning Tree Algorithm was last performed.
- **Uptime** – The time since the bridge port was last initialized.

4.5.1.2— STP Port Status

Use the Port Status section to display the STP functional status of participating ports.

Figure 55. STP Port Status



Port	CIST Role	CIST State	Uptime
1	DesignatedPort	Forwarding	0d 10:20:16
2	DesignatedPort	Forwarding	0d 10:20:16
3	DesignatedPort	Forwarding	0d 10:20:16
4	DesignatedPort	Forwarding	0d 10:20:16
5	DesignatedPort	Forwarding	0d 10:20:16
6	Disabled	Discarding	-
7	DesignatedPort	Forwarding	0d 01:56:29
8	DesignatedPort	Forwarding	0d 10:20:19
9	Disabled	Discarding	-
10	Disabled	Discarding	-

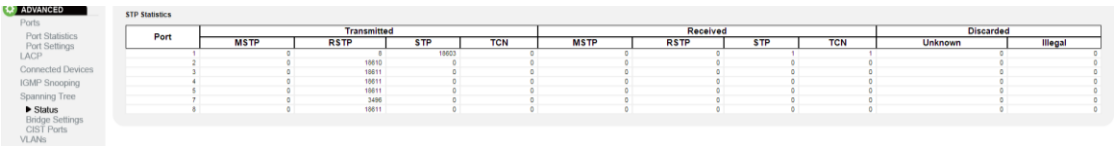
Path Advanced, Spanning Tree, Status

Parameters

- **Port** – Port Identifier.
- **CIST Role** – Port roles can be either: a part of the active topology connecting to the root bridge (i.e., root port), connecting a LAN segment through the switch to the root bridge (i.e., designated port), or is an alternate or backup port that may provide connectivity if the Spanning Tree topology changes.
- **CIST State** – Displays current state of this port within the Spanning Tree negotiation.
  - **Blocking** – Port receives STA configuration messages, but does not forward packets.
  - **Learning** – Port has transmitted configuration messages for a predefined period (Forward Delay) without receiving contradictory information.
  - **Forwarding** – Port forwards packets, and continues learning addresses in case of a topology change.
- **Uptime** – The time since the bridge port was last initialized.

4.5.1.3— STP Statistics

Figure 56. STP Statistics



Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	6	19603	0	0	0	1	1	0	0
2	0	19610	0	0	0	0	0	0	0	0
3	0	19611	0	0	0	0	0	0	0	0
4	0	19611	0	0	0	0	0	0	0	0
5	0	19611	0	0	0	0	0	0	0	0
7	0	3496	0	0	0	0	0	0	0	0
8	0	19611	0	0	0	0	0	0	0	0

Path Advanced, Spanning Tree, Status

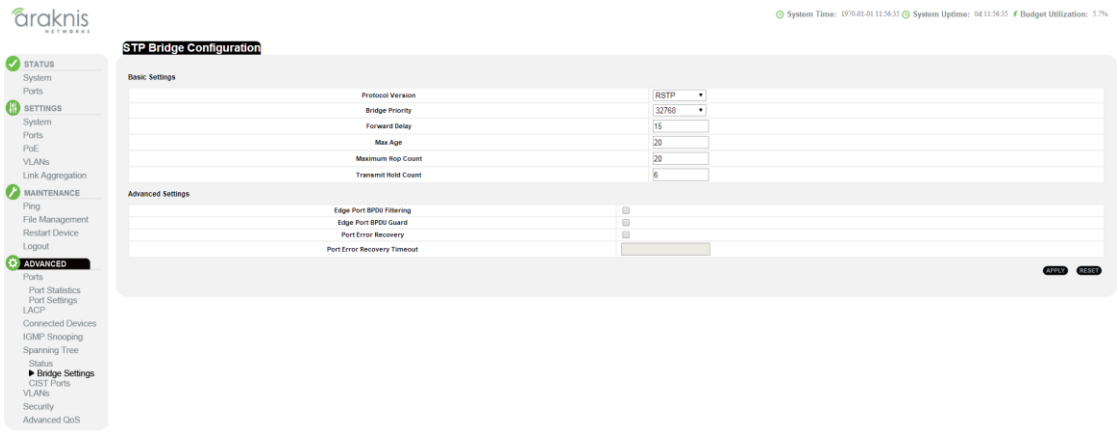
Parameters

- **Port** – Port Identifier.
- **MSTP** – The number of MSTP Configuration BPDU's received/sent on a port.
- **RSTP** – The number of RSTP Configuration BPDU's received/sent on a port.
- **STP** – The number of legacy STP Configuration BPDU's received/sent on a port.
- **TCN** – The number of (legacy) Topology Change Notification BPDU's received/sent on a port.
- **Discarded Unknown** – The number of unknown Spanning Tree BPDU's received and discarded on a port.
- **Discarded Illegal** – The number of illegal Spanning Tree BPDU's received and discarded on a port.

4.5.2— STP Bridge Settings

Use the STP Bridge Settings page to configure settings for STP that apply globally to the switch.

Figure 57. STP Bridge Configuration



Path Configuration, Spanning Tree, Bridge Settings

Parameters **Basic Settings**

- **Protocol Version —** Specifies the type of spanning tree used on this switch. (Options: STP, RSTP, MSTP; Default: MSTP)
  - **STP —** Spanning Tree Protocol (IEEE 802.1D); i.e., the switch will use RSTP set to STP forced compatibility mode.
  - **RSTP —** Rapid Spanning Tree (IEEE 802.1w)
  - **MSTP —** Multiple Spanning Tree (IEEE 802.1s); This is the default.
- **Bridge Priority —** Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
  - **Default —** 128
  - **Range —** 0-240, in steps of 16
  - **Options —** 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240
- **Forward Delay –** The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
  - **Minimum —** The higher of 4 or [(Max. Message Age / 2) + 1]
  - **Maximum —** 30
  - **Default —** 15
- **Max Age —** The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (Note that references to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
  - **Minimum —** The higher of 6 or [2 x (Hello Time + 1)]
  - **Maximum —** The lower of 40 or [2 x (Forward Delay - 1)]
  - **Default —** 20

- **Transmit Hold Count —** The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. (Range: 1-10; Default: 6)
- **Max Hop Count —** The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 6-40; Default: 20)

  An MST region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MST region is never changed. However, each spanning tree instance within a region, and the common internal spanning tree (CIST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

Advanced Settings

- **Edge Port BPDU Filtering —** BPDU filtering allows you to avoid transmitting BPDUs on configured edge ports that are connected to end nodes. By default, STA sends BPDUs to all ports regardless of whether administrative edge is enabled on a port. BDPU filtering is configured on a per-port basis. (Default: Disabled)
- **Edge Port BPDU Guard —** This feature protects edge ports from receiving BPDUs. It prevents loops by shutting down an edge port when a BPDU is received instead of putting it into the spanning tree discarding state. In a valid configuration, configured edge ports should not receive BPDUs. If an edge port receives a BPDU, an invalid configuration exists, such as a connection to an unauthorized device. The BPDU guard feature provides a secure response to invalid configurations because an administrator must manually enable the port. (Default: Disabled)
- **Port Error Recovery —** Controls whether a port in the error-disabled state will be automatically enabled after a certain time. If recovery is not enabled, ports have to be disabled and re-enabled for normal STA operation. The condition is also cleared by a system reboot.
- **Port Error Recovery Timeout —** The time that has to pass before a port in the error-disabled state can be enabled. (Range: 30-86400 seconds or 24 hours)

Configuration Instructions

To configure Basic and Advanced STP Bridge Settings:

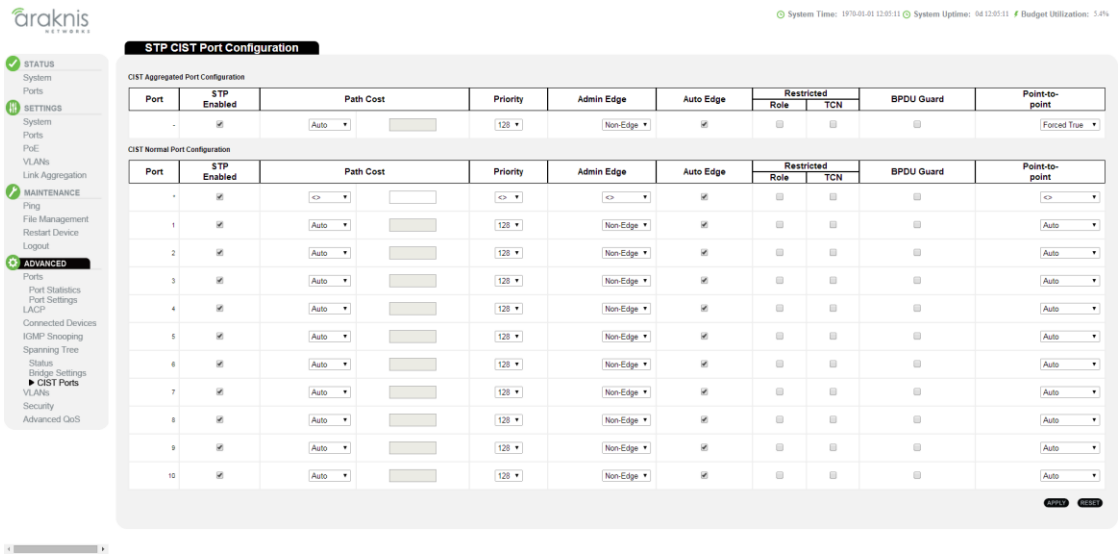
1. Click Configuration, Spanning Tree, Bridge Settings.
2. Modify the required attributes.
3. Click Save.

Pro Tip — Spanning Tree Protocol uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, we recommend selecting the MSTP option.

4.5.3— CIST Ports

Use the CIST Ports Configuration page to configure STA settings for individual ports when the spanning tree mode is configured to STP or RSTP, or for interfaces in the CIST. STA port settings include path cost, port priority, edge port (for fast forwarding), automatic detection of an edge port, and point-to-point link type.

Figure 58. STP CIST Port Configuration



Path Advanced, Spanning Tree, CIST Ports

Parameters

- **Port** – Port identifier.
- **STP Enabled** – Sets the interface to enable STA, disable STA, or disable STA with BPDU transparency. (Default: Enabled)

  BPDU transparency allows a port that is not participating in the spanning tree to forward BPDU packets to other ports instead of discarding these packets or attempting to process them.
- **Path Cost** – Determine the best path between devices. Lower values are assigned to faster ports and higher values are assigned to slower ports (e.g. 1Gbps links have lower path cost than 100Mbps).

  By default, the switch automatically detects the speed and duplex mode for each port, and the path cost is automatically populated for each port.
- **Priority** – If the path cost for all ports on a switch is the same, the port with the highest priority (i.e., lowest value) will be a designated port. If more than one port is assigned the same priority value, the port with lowest port identifier value will be elected as designated port (Range: 0-240, in steps of 16; Default: 128).
- **Admin Edge** – You can enable this option if the port is connected to an end device instead of another switch/router. Since end devices cannot cause network loops, they can go directly to the spanning tree forwarding state (Default: Enabled).
- **Auto Edge** – When enabled, the switch can determine that a switch port is connected to an end device if no BPDU's are received on the port (Default: Enabled).
- **Restricted TCN** – If enabled, the port does not communicate received topology change notifications and topology changes to other switches in the network.
- **Restricted Role** – If enabled, the port cannot be selected as Root Port for the CIST or any MSTI, even if it has the lowest path to the Root Bridge. The port will be selected as an Alternate Port after the Root Port has been selected. If enabled, this can cause a lack of spanning tree connectivity. This feature is also known as Root Guard.
- **BPDU Guard** – This feature can prevent loops by shutting down a port when a BPDU is received instead of putting it into the spanning tree discarding state.

(Default: Disabled)

- **Point-to-Point** – Transition to the forwarding state is faster for point-to-point links than for shared media. Available options include:
  - **Auto** – The switch automatically determines if the interface is attached to a point-to-point link or to shared medium (Default).
    - When automatic detection is selected, the switch determines the link type based on duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
  - **Forced True** – A point-to-point connection to exactly one other bridge.
  - **Forced False** – A shared connection to two or more bridges.

Configuration Instructions

To configure settings for STP/RSTP/CIST interfaces:

1. Click Advanced, Spanning Tree, CIST Ports.
2. Modify the required attributes.
3. Click “Apply”.

4.6— Advanced VLANs

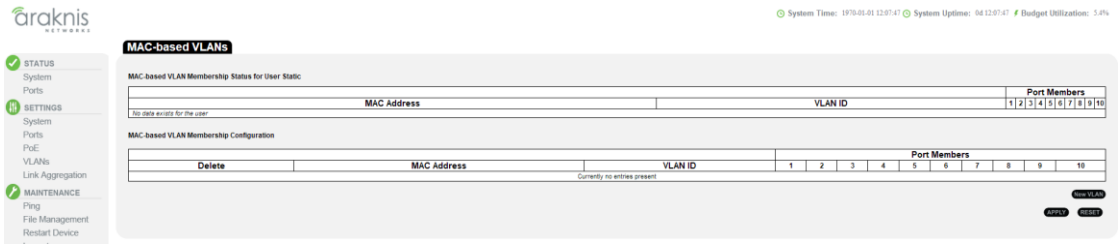
Advanced VLANs allows you to configure MAC-based VLANs and Private VLANs.

4.6.1— MAC-based VLANs

MAC-based VLANs group VLAN members by MAC address. With MAC-based VLANs configured, the device adds a VLAN tag to an untagged frame according to its source MAC address. MAC-based VLANs are mostly used in conjunction with security technologies such as 802.1X to provide secure, flexible network access for terminal devices.

Use the MAC-based VLAN Membership Configuration page to display the MAC address to VLAN map entries.

Figure 59. MAC-based VLAN



4.6.1.1— MAC-based VLANs Status

Figure 60. MAC-based VLANs Status

Path Advanced, VLANs, MAC-based VLANs

Parameters

- **MAC Address** – A source MAC address that is mapped to a specific VLAN.
- **VLAN ID** – VLAN to which ingress traffic matching the specified source MAC address is forwarded.
- **Port Members** – The ports assigned to this VLAN.

4.6.1.2— Configuring MAC-based VLANs

When MAC-based VLAN classification is enabled, untagged frames received by a port are assigned to the VLAN, which is mapped to the frame's source MAC address. When no MAC address is matched, untagged frames are assigned to the receiving port's native Port VLAN ID (PVID).

Figure 61. MAC-Based VLAN Configuration

Path Advanced, VLANs, MAC-based VLANs

Parameters

- **MAC Address** – A source MAC address that is to be mapped to a specific VLAN. The MAC address must be specified in the format xx-xx-xx-xx-xx-xx.
- **VLAN ID** – VLAN to which ingress traffic matching the specified source MAC address is forwarded (Range: 1-4093).
- **Port Members** – The ports currently assigned to this VLAN.

Configuration Instructions

To map a MAC address to a VLAN:

1. Click Advanced, Advanced VLANs, MAC-based VLANs.
2. Enter an address in the MAC Address field.
3. Enter an identifier in the VLAN field. Note that the specified VLAN need not already be configured.
4. Specify the ports assigned to this VLAN.
5. Click Apply.

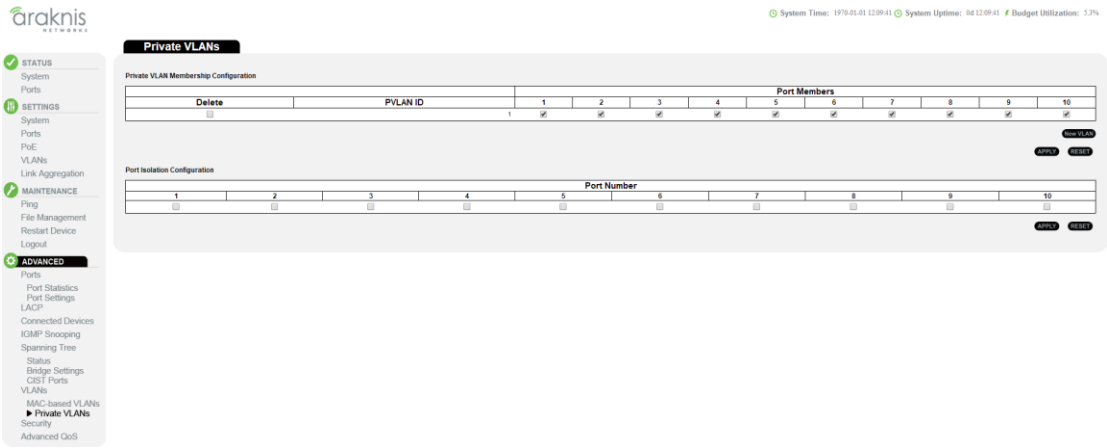
Pro Tip

- Source MAC addresses can be mapped to only one VLAN ID.
- Configured MAC addresses cannot be broadcast to multicast addresses.

4.6.2— 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.

Figure 62. Private VLANs



4.6.2.1— Configuring Private VLANs

Use the Private VLAN Membership Configuration section to assign port members to private VLANs.

Path Advanced, Advanced VLANs, Private VLANs

Parameters These parameters are displayed:

- **PVLAN ID** – Private VLAN identifier. (Range: 1-10)

  By default, all ports are configured as members of VLAN 1 and PVLAN 1. Because all of these ports are members of 802.1Q VLAN 1, isolation cannot be enforced between the members of PVLAN 1.
- **Port Members** – Port identifier.

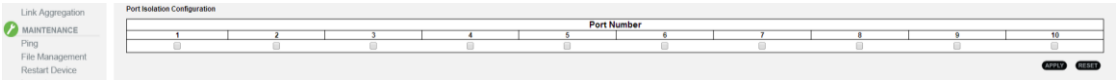
Configuration Instructions To configure VLAN port members for private VLANs:

1. Click Advanced, VLANs, Private VLANs.
2. Add or delete members of any existing PVLAN, or click Add New Private VLAN and mark the port members.
3. Click Apply.

4.6.2.2— Using Port Isolation

An isolated port cannot forward any unicast, multicast, or broadcast traffic to any other ports in the same PVLAN. Ports within a private VLAN (PVLAN) are isolated from other ports that are not in the same PVLAN. Port Isolation can be used to block communications between ports within the same PVLAN.

Figure 63. Port Isolation Settings



Path Advanced, VLANs, Private VLANs

Parameters These parameters are displayed:

- **Port Number** – Port identifier.

Configuration Instructions To configure isolated ports:

1. Click Advanced, VLANs, Private VLANs.
2. Mark the ports that are to be isolated from each other.
3. Click Apply.

4.7— Security

4.7.1— SNMP

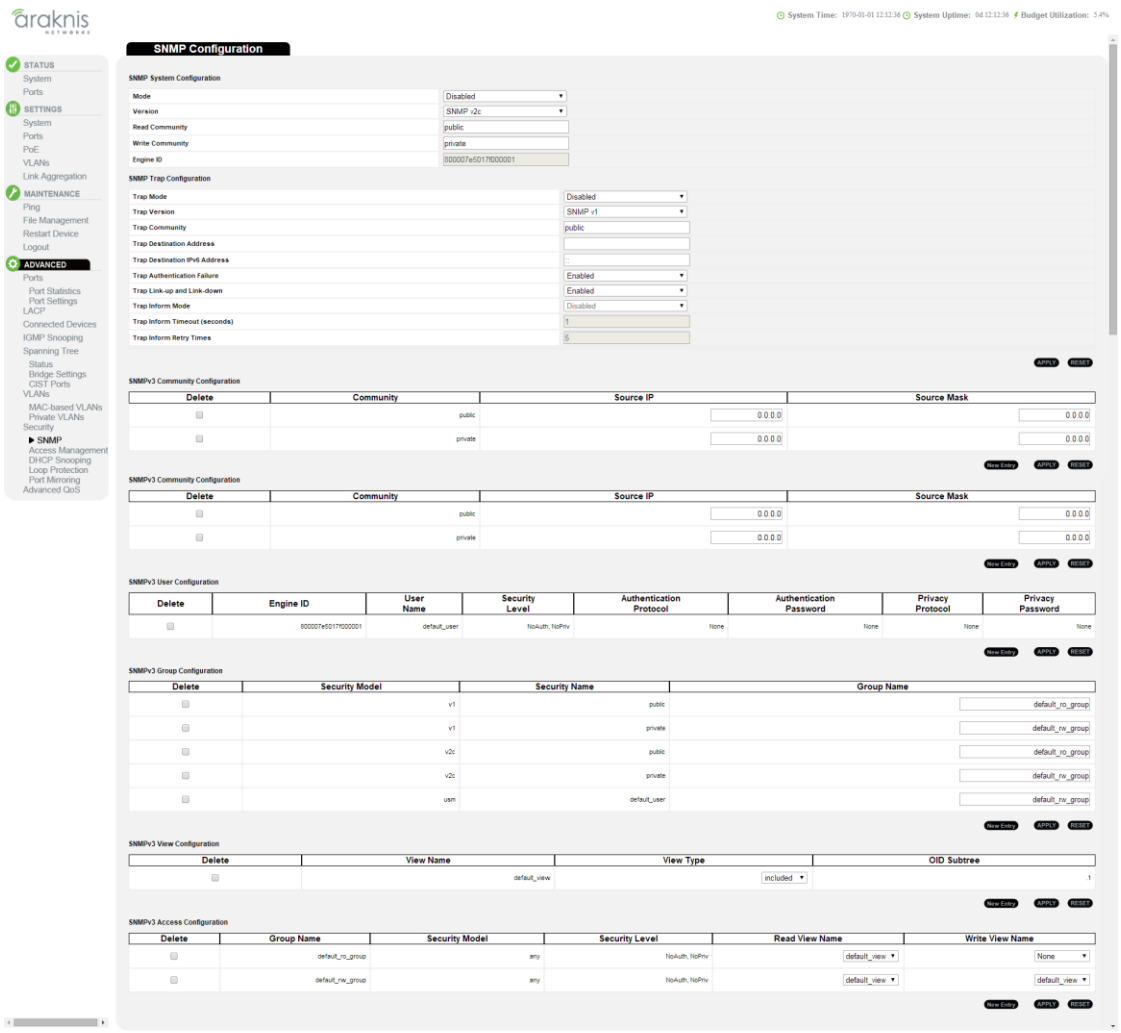
Simple Network Management Protocol (SNMP) is a communication protocol designed to manage devices on a network.

Managed devices that support SNMP contain a local agent, which is software that runs locally on the device. 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 300-series switch includes an SNMP agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. SNMP client software can access the switch SNMP agent from 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.

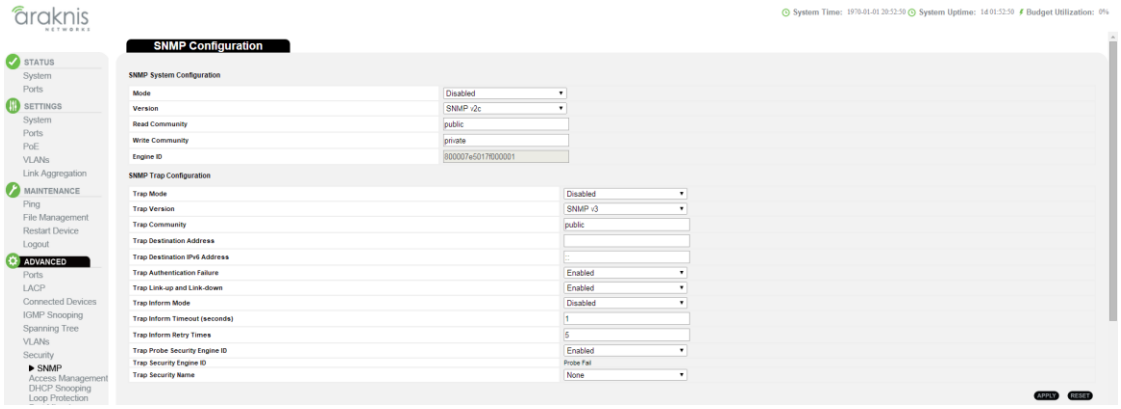
Figure 64. SNMP Configuration Page



4.7.1.1—Configuring SNMP System and Trap Settings

To manage the switch through SNMP, you must first enable the protocol and configure basic access parameters. To issue trap messages, the trap function must be enabled, and the destination host specified.

Figure 65. SNMP Configuration



Path Advanced, Security, SNMP

Parameters

SNMP System Configuration

- **Mode** – Enables or disables SNMP service (Default: Disabled).
- **Version** – Specifies the SNMP version to use (Options: SNMP v1, SNMP v2c, SNMP v3; Default: SNMP v2c).
- **Read Community** – The community used for read-only access to the SNMP agent (Range: 0-255 characters; Default: public).
  - This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy.
- **Write Community** – The community used for read/write access to the SNMP agent (Range: 0-255 characters; Default: private).
  - This parameter only applies to SNMPv1 and SNMPv2c. SNMPv3 uses the User-based Security Model (USM) for authentication and privacy.
- **Engine ID** – The SNMPv3 engine ID (Range: 10-64 hex digits, excluding a string of all 0s or all Fs; Default: 800007e5017f000001).
  - An SNMPv3 engine is an independent SNMP agent that resides on the switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
  - A local engine ID is automatically generated that is unique to the switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all local SNMP users will be cleared. You will need to reconfigure all existing users.

SNMP Trap Configuration

- **Trap Mode** – Enables or disables SNMP traps. (Default: Disabled)
  - SNMP traps should be enabled so that key events are reported by this switch to your management station. Traps indicating status changes can be issued by the switch to the specified trap manager by sending authentication failure messages and other trap messages.
- **Trap Version** – Indicates if the target user is running SNMP v1, v2c, or v3. (Default: SNMP v1)
- **Trap Community** – Specifies the community access string to use when sending SNMP trap packets (Range: 0-255 characters; Default: public).

- **Trap Destination Address** – IPv4 address of the management station to receive notification messages.
- **Trap Destination IPv6 Address** – IPv6 address of the management station to receive notification messages. An IPv6 address must be formatted according to RFC 2373 “IPv6 Addressing Architecture,” using 8 colon-separated 16-bit hexadecimal values. One double colon may be used to indicate the appropriate number of zeros required to fill the undefined fields.
- **Trap Authentication Failure** – Issues a notification message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled).
- **Trap Link-up and Link-down** – Issues a notification message whenever a port link is established or broken (Default: Enabled).
- **Trap Inform Mode** – Enables or disables sending notifications as inform messages. Note that this option is only available for version 2c and 3 hosts (Default: traps are used).
- **Trap Inform Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message (Range: 0-2147 seconds; Default: 1 second).
- **Trap Inform Retry Times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt (Range: 0-255; Default: 5).

Note — The SNMPv3-related settings below are not visible in the menu unless SNMP System Configuration Version has been set to “SNMPv3”.

- **Trap Probe Security Engine ID (SNMPv3)** – Specifies whether or not to use the engine ID of the SNMP trap probe in trap and inform messages. (Default: Enabled)
- **Trap Security Engine ID (SNMPv3) –** Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When “Trap Probe Security Engine ID” is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. (Range: 10-64 hex digits, excluding a string of all 0s or all Fs)

Note — The Trap Probe Security Engine ID must be disabled before an engine ID can be manually entered into this field.

Trap Security Name (SNMPv3) – Indicates the SNMP trap security name. SNMPv3 traps and “informs” use USM for authentication and privacy. A unique security name is needed when SNMPv3 traps or informs are enabled.

Note — To be able to select a name from this field, enter an SNMPv3 user with the same Trap Security Engine ID in the SNMPv3 Users Configuration section.

4.7.1.2— Setting SNMPv3 Community Access Strings

Use the SNMPv3 Community Configuration page to set community access strings. All community strings used to authorize access by SNMP v1 and v2c clients should be listed in the SNMPv3 Communities Configuration table. For security reasons, you should consider removing the default strings.

Figure 66. SNMPv3 Community Access Strings

Path Advanced, Security, SNMP

Parameters

- **Community –** Specifies the community strings that allow access to the SNMP agent. (Range: 1-32 characters, Default: public, private)

  For SNMPv3, these strings are treated as a Security Name, and are mapped as an SNMPv1 or SNMPv2 community string in the SNMPv3 Groups Configuration table.
- **Source IP –** Specifies the source address of an SNMP client.
- **Source Mask –** Specifies the address mask for the SNMP client.

Configuration Instructions To configure SNMPv3 Community Access Strings:

1. Click Advanced, Security, SNMP.
2. Set the IP address and mask for the default community strings. Otherwise, you should consider deleting these strings for security reasons.
3. Add any new community strings required for SNMPv1 or v2 clients that need to access the switch, along with the source address and address mask for each client.
4. Click Apply.

4.7.1.3— Configuring SNMPv3 Users

Use the SNMPv3 User Configuration table to define a unique name and remote engine ID for each SNMPv3 user. Users must be configured with a specific security level, and the types of authentication and privacy protocols to use.

Figure 67. SNMPv3 User Configuration

Note — Any user assigned through this page is associated with the group assigned to the USM Security Model on the SNMPv3 Groups Configuration, and the views assigned to that group in the SNMPv3 Access Configuration.

Path Configuration, Security, Switch, SNMP, Users

Parameters

- **Engine ID –** The engine identifier for the SNMP agent on the remote device where the user resides (Range: 10-64 hex digits, excluding a string of all 0s or all Fs).
- **User Name –** The name of user connecting to the SNMP agent (Range: 1-32 characters, ASCII characters 33-126 only).
- **Security Level –** The security level assigned to the user:
  - **NoAuth, NoPriv –** There is no authentication or encryption used in SNMP communications (This is the default for SNMPv3.).
  - **Auth, NoPriv –** SNMP communications use authentication, but the data is not encrypted.
  - **Auth, Priv –** SNMP communications use both authentication and encryption.
- **Authentication Protocol –** The method used for user authentication (Options: None, MD5, SHA; Default: MD5).
- **Authentication Password –** A plain text string identifying the authentication pass phrase (Range: 1-32 characters for MD5, 8-40 characters for SHA).
- **Privacy Protocol –** The encryption algorithm used for data privacy; only 56-bit DES is currently available (Options: None, DES; Default: DES).
- **Privacy Password –** A string identifying the privacy pass phrase (Range: 8-40 characters, ASCII characters 33-126 only).

Configuration Instructions To configure SNMPv3 users:

1. Click Advanced, Security, SNMP.
2. Click “Add new user” to configure a user name.
3. Enter a remote Engine ID of up to 64 hexadecimal characters.
4. Define the user name, security level, authentication, and privacy settings.
5. Click Apply.

4.7.1.4— Configuring SNMPv3 Groups

Use the SNMPv3 Group Configuration table to configure SNMPv3 groups. An SNMPv3 group defines the access policy for assigned users. You can use the pre-defined default groups, or create a new group and the views authorized for that group.

Figure 68. SNMPv3 Groups

Path Advanced, Security, SNMP

Parameters

- **Security Model –** The user security model. (Options: SNMP v1, v2c, or the User-based Security Model – USM).
- **Security Name –** The name of a user connecting to the SNMP agent. (Range: 1-32 characters)

  The options displayed for this parameter depend on the selected Security Model. For SNMP v1 and v2c, the switch displays the names configured on the SNMPv3 Communities Configuration menu. For USM (or SNMPv3), the switch displays the names configured with the local engine ID in the SNMPv3 Users Configuration table. To modify an entry for USM, the current entry must first be deleted.
- **Group Name –** The name of the SNMP group. (Range: 1-32 characters)

Configuration Instructions To configure SNMPv3 groups:

1. Click Advanced, Security, SNMP.
2. Click “Add new group” to set up a new group.
3. Select a security model.
4. Select the security name.
5. Enter a group name. Note that the views assigned to a group must be specified on the SNMP Accesses Configuration table.
6. Click Apply.

4.7.1.5—Configuring SNMPv3 Views

Use the SNMPv3 View Configuration table to define views that restrict user access to specified portions of the MIB tree. The predefined view “default_view” allows access to the entire MIB tree.

Figure 69. SNMP View Configuration

Path Advanced, Security, SNMP

Parameters

- **View Name –** The name of the SNMP view. (Range: 1-32 characters, ASCII characters 33-126 only).
- **View Type –** Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.
- **OID Subtree –** Object identifiers of branches within the MIB tree. The first character **must** be a period (.). Wild cards can be used to mask a specific portion of the OID string using an asterisk. (Length: 1-128)

Configuration Instructions To configure SNMPv3 views:

1. Click Advanced, Security, SNMP.
2. Click “Add new view” to set up a new view.
3. Enter the view name, view type, and OID subtree.
4. Click Apply.

4.7.1.6— Configuring SNMPv3 Group Access Rights

Use the SNMPv3 Access Configuration page to assign portions of the MIB tree to which each SNMPv3 group is granted access. You can assign more than one view to a group to specify access to different portions of the MIB tree.

Figure 70. SNMP View Configuration

Path Advanced, Security, SNMP

Parameters

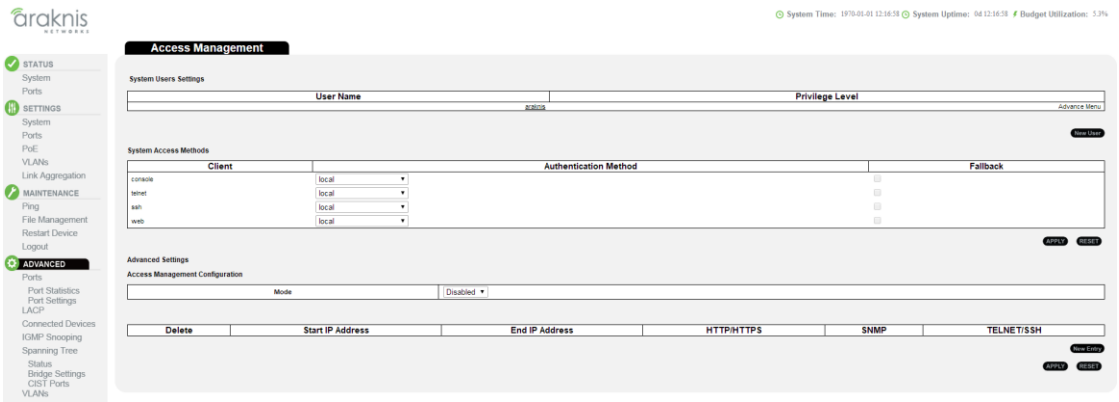
- **Group Name –** The name of the SNMP group (Range: 1-32 characters).
- **Security Model –** The user security model (Options: any, v1, v2c, or the User-based Security Model – usm; Default: any).
- **Security Level –** The security level assigned to the group:
  - NoAuth, NoPriv – There is no authentication or encryption used in SNMP communications (This is the default for SNMPv3.).
  - Auth, NoPriv – SNMP communications use authentication, but the data is not encrypted.
  - Auth, Priv – SNMP communications use both authentication and encryption.
- **Read View Name –** The configured view for read access (Range: 1-32 characters).
- **Write View Name –** The configured view for write access (Range: 1-32 characters).

Configuration Instructions To configure SNMPv3 Group Access Rights

1. Click Advanced, Security, SNMP.
2. Click Add New Access to create a new entry.
3. Specify the group name, security settings, read view, and write view.
4. Click Apply.

4.7.2— Access Management

Figure 71. Access Management



4.7.2.1— Configuring Security

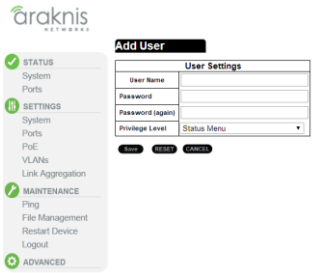
You can configure this switch to authenticate users logging into the system for management access or to control client access to the data ports.

Management access to the switch can be controlled through local authentication of user names and passwords stored on the switch. Additional authentication methods include Secure Shell (SSH), Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), static configuration of client addresses, and SNMP.

4.7.2.2— Configuring User Accounts

Use the Access Management page to control management access to the switch based on manually configured user names and passwords.

Figure 72. New User



Parameters Advanced, Security, Access Management, New User

Parameters

- **User Name –** The name of the user (Maximum length: 8 characters; maximum number of users: 16).
- **Password –** Specifies the user password (Range: 0-8 characters plain text, case sensitive).
- **Password (again) –** Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the password if these two fields do not match.
- **Privilege Level** – Specifies the user level. The default settings provide four access levels:
  - **Status Menu –** Access to Status menu as well as Advanced → Ports → Port Statistics, and Advanced → Spanning Tree → Status.
  - **Settings Menu –** Access to Status and Settings menus as well as Advanced → Ports → Port Statistics, and Advanced → Spanning Tree → Status.
  - **Maintenance Menu –** Access to Status, Settings, and Maintenance menus as well as Advanced → Ports → Port Statistics, and Advanced → Spanning Tree → Status.
  - **Advanced Menu –** Admin access to the switch.

Note –

- The default administrator name is “araknis” with the password “araknis”.
- It is highly recommended to assign a new administrator password as soon as possible, and store it in a safe place.

Configuration Instructions To configure user accounts:

1. Click Advanced, Security, Access Management.
2. Click New User.
3. Type user name, password and select privilege level associated with the new account.
4. Click Apply.

Note — To edit or delete an existing user, click the user name in the System Users Settings list to load the Edit User page.

4.7.2.3— Configuring SSH

Use the Access Management page to enable access to the Secure Shell (SSH) management interface. SSH provides remote management access to this switch as a secure replacement for Telnet.

Figure 73. System Access Methods Menu (SSL)

Path Advanced, Security, Access Management

Parameters

- **SSH —** Allows you to enable/disable SSH service on the switch. (Default: Enabled)

Configuration Instructions To configure SSH:

1. Click Advanced, Security, Access Management.
2. Enable SSH if required.
3. Click Apply.

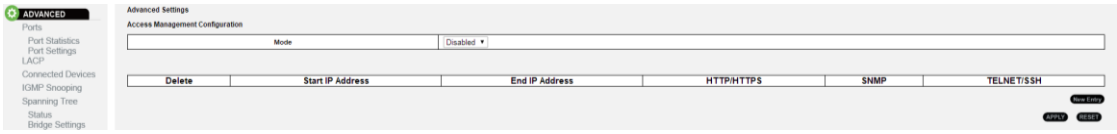
Pro Tip –

- You need to install an SSH client on the management station to access the switch for management via the SSH protocol. The switch supports both SSH Version 1.5 and 2.0 clients.
- The SSH service on the switch supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

4.7.2.4— Filtering IP Addresses For Management Access

Use the Access Management Configuration section to create a list of up to 16 IP addresses or IP address groups that are allowed management access to the switch through the web interface, or SNMP, or Telnet.

Figure 74. Access Management Configuration



Note — The management interfaces are open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses. If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection.

Path Advanced, Security, Access Management

Parameters

Delete – Delete an access management rule entry.

Start IP Address – The starting address of a range.

End IP Address – The ending address of a range.

HTTP/HTTPS – Filters IP addresses for access to the web interface over standard HTTP, or over HTTPS, which uses the Secure Socket Layer (SSL) protocol to provide an encrypted connection.

SNMP – Filters IP addresses for access through SNMP.

TELNET/SSH – Filters IP addresses for access through Telnet, or through Secure Shell, which provides authentication and encryption.

Configuration Instructions

To configure addresses allowed access to management interfaces on the switch:

1. Click Advanced, Security, Access Management.
2. Click “New Entry”.
3. Enter the start and end of an address range.
4. Mark the protocols to restrict based on the specified address range.
5. Click Apply.

4.7.3— DHCP Snooping

DHCP snooping ensures IP integrity in a domain. It works with information from a DHCP server to:

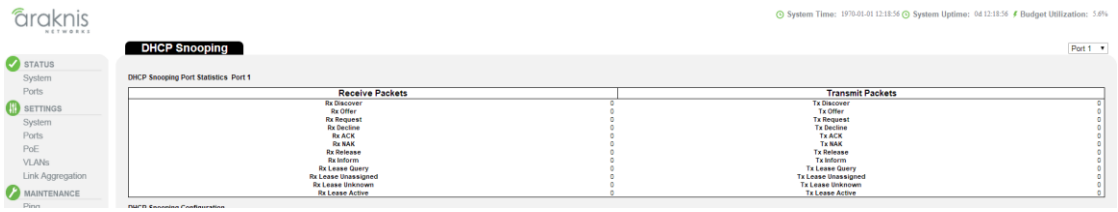
- Track the physical location of hosts.
- Ensure that hosts only use the IP addresses assigned to them.
- Ensure that only authorized DHCP servers are accessible.

With DHCP snooping, only an approved list of IP addresses may access the network. The list is configured at the switch port level, and the DHCP server manages the access control. Therefore, only specific IP addresses with specific MAC addresses on specific ports may access the network. DHCP Snooping is also an important defense mechanism against Rogue-DHCP and ARP Spoofing attacks.

4.7.3.1— DHCP Snooping Port Statistics

Use the DHCP Snooping Port Statistics section to show statistics for various types of DHCP protocol packets.

Figure 75. DHCP Snooping



Path Advanced, Security, DHCP Snooping, DHCP Snooping Port Statistics

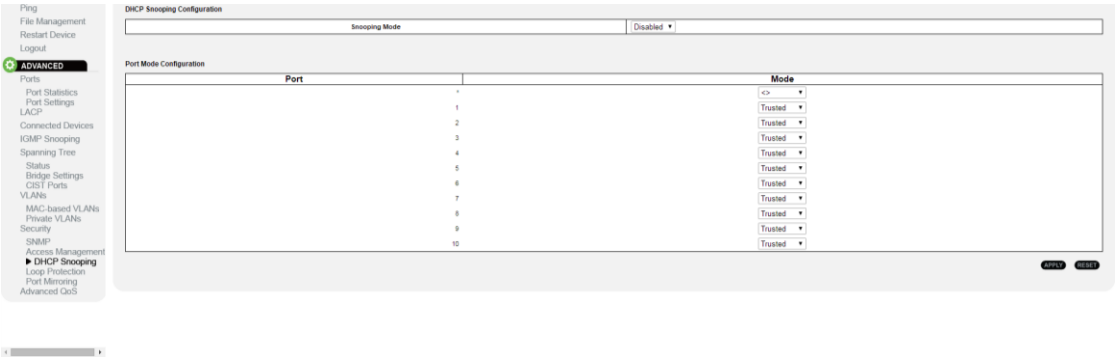
Parameters These parameters are displayed:

- **Rx/Tx Discover** – The number of discover (option 53 with value 1) packets received and sent.
- **Rx/Tx Offer** – The number of offer (option 53 with value 2) packets received and sent.
- **Rx/Tx Request** – The number of request (option 53 with value 3) packets received and sent.
- **Rx/Tx Decline** – The number of decline (option 53 with value 4) packets received and sent.
- **Rx/Tx ACK** – The number of ACK (option 53 with value 5) packets received and sent.
- **Rx/Tx NAK** – The number of NAK (option 53 with value 6) packets received and sent.
- **Rx/Tx Release** – The number of release (option 53 with value 7) packets received and sent.
- **Rx/Tx Inform** – The number of inform (option 53 with value 8) packets received and sent.
- **Rx/Tx Lease Query** – The number of lease query (option 53 with value 10) packets received and sent.
- **Rx/Tx Lease Unassigned** – The number of lease unassigned (option 53 with value 11) packets received and sent.
- **Rx/Tx Lease Unknown** – The number of lease unknown (option 53 with value 12) packets received and sent.
- **Rx/Tx Lease Active** – The number of lease active (option 53 with value 13) packets received and sent.

4.7.3.2— DHCP Snooping Configuration

Use the DHCP Snooping Configuration menu to filter IP traffic on insecure ports for which the source address cannot be identified via DHCP snooping. The addresses assigned to DHCP clients on insecure ports can be carefully controlled using the dynamic bindings registered with DHCP Snooping.

Figure 76. DHCP Snooping Menu



Path Advanced, Security, DHCP Snooping, DHCP Snooping Configuration

Parameters These parameters are displayed:

- **Snooping Mode** – Enables DHCP snooping globally. When DHCP snooping is enabled, DHCP request messages will be forwarded to trusted ports, and reply packets only allowed from trusted ports (Default: Disabled).
- **Port** – Port identifier
- **Mode** – Enables or disables a port as a trusted source of DHCP messages (Default: Trusted).

Configuration Instructions To configure DHCP Snooping:

1. Click Advanced, Security, DHCP Snooping.
2. Set the status for the global DHCP snooping process, and set any ports within the local network to Trusted.
3. Click Apply.

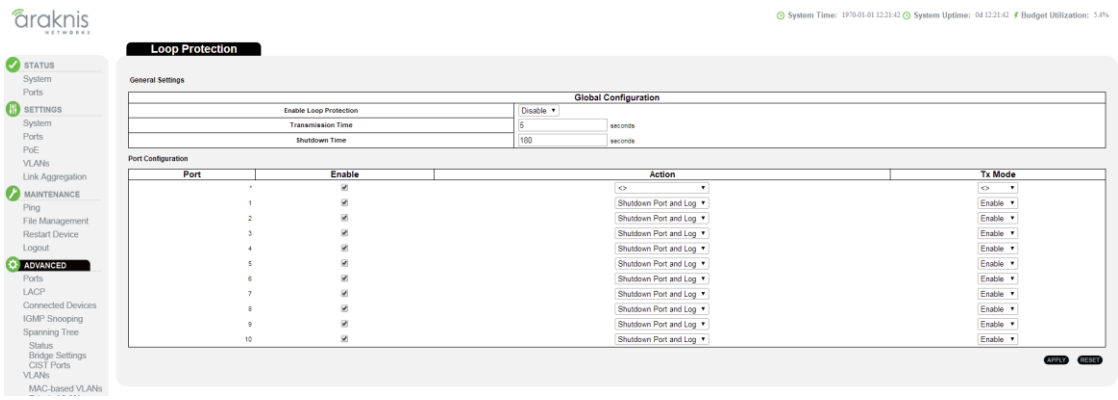
Pro Tip – DHCP Snooping Process

- DHCP snooping is used to filter DHCP messages received on a non-secure interface from outside the network or firewall. When DHCP snooping is enabled, DHCP messages received on an untrusted interface from a device not listed in the DHCP snooping table will be dropped.
- Table entries are only learned for trusted interfaces. An entry is added or removed automatically to the DHCP snooping table when a client receives, renews or releases an IP address from a DHCP server. Each entry includes a MAC address, IP address, lease time, VLAN identifier, and port identifier.

4.7.4— Configuring Loop Protection

Use the Loop Protection page to detect general loopback conditions caused by hardware problems or faulty protocol settings. When enabled, a control frame is transmitted on the participating ports, and the switch monitors inbound traffic to see if the frame is looped back.

Figure 77. Loop Protection Menu



4.7.4.1— Loop Protection-Global Configuration

Use the global settings table to configure loop protection for the entire switch.

Path Advanced Configuration, Loop Protection

Parameters

- **Enable Loop Protection –** Enables loopback detection globally on the switch. (Default: Disabled)

  Loopback must be enabled both globally and on a specific port for this function to take effect.
- **Transmission Time –** The transmission interval for loopback detection control frames. (Range: 1-10 seconds)
- **Shutdown Time –** The interval to wait before the switch automatically releases an interface from shutdown state. (Range: 1-604,800 seconds, or 0 to disable automatic recovery.) If the shutdown time is set to zero, any ports placed in shutdown state will remain in that state until the switch is reset. If the loop protection setting is changed, any ports placed in shutdown state by the loopback detection process will be immediately restored to operation regardless of the remaining shutdown time.

Configuration Instructions To configure global loop protection settings:

1. Click Advanced, Security, Loop Protection.
2. Enable loop protection globally, and adjust the control frame transmission interval and shutdown time as required.
3. Enable loop protection for the port to be monitored, set the behavior to take if a loop is detected, and select whether or not the port will actively transmit control frames.
4. Click Apply.

4.7.4.2— Loop Protection-Port Configuration

Figure 78. Port Loop Protection Menu

Path Advanced Configuration, Loop Protection

Parameters

- **Port –** Port Identifier.
- **Enable –** Enables loopback detection on a port. (Default: Enabled)
- **Action –** Select the action to take when a loop is detected on a port. (Options: Shutdown Port, Shutdown Port and Log, Log Only)
- **Tx Mode –** Controls whether the port is actively generating loop protection PDUs, or whether it is just passively looking for looped PDUs. (Default: Enabled)

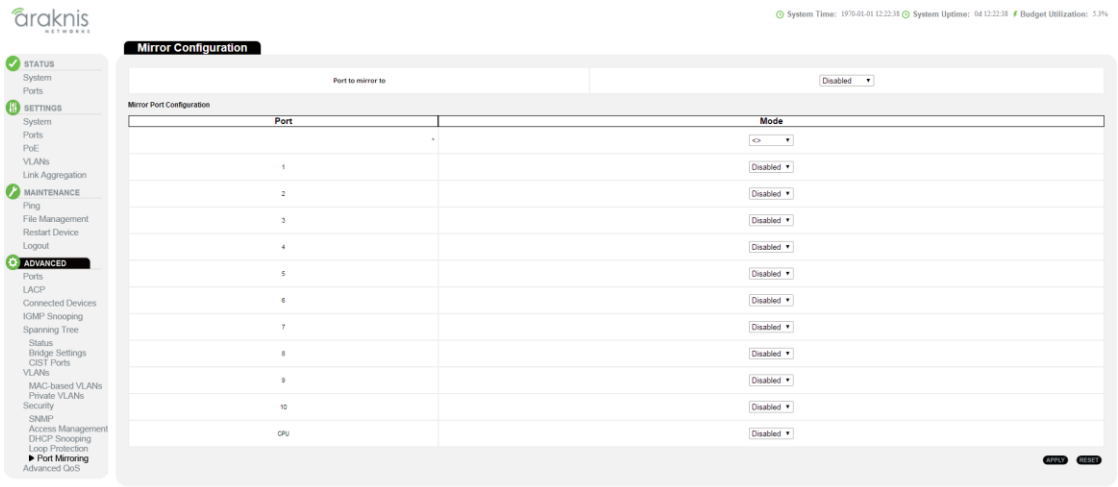
Configuration Instructions To configure port loop protection:

1. Click Advanced Configuration, Loop Protection.
2. Enable loop protection globally, and adjust the control frame transmission interval and shutdown time as required.
3. Enable loop protection for the port to be monitored, set the action to take if a loop is detected, and select whether or not the port will actively transmit control frames.
4. Click Apply.

4.7.5— Port Mirroring

Port mirroring is used on a switch 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 79. Port Configuration Settings



Path Advanced, Security, Port Mirroring

Parameters These parameters are displayed:

- **Port to mirror to —** The destination port that will mirror the traffic from the source port. All mirror sessions must share the same destination port. (Default: Disabled)
- **Port —** The port whose traffic will be monitored.
- **Mode —** Specifies which traffic to mirror to the target port.
  (Options: Disabled, Enabled (receive and transmit), Rx only (receive), Tx only (transmit); Default: Disabled)

Configuration Instructions To configure port mirroring:

1. Click Advanced, Security, Port Mirroring.
2. Select the destination port to which all mirrored traffic will be sent.
3. Set the mirror mode on any of the source ports to be monitored.
4. Click Apply.

4.8— Advanced QoS

Quality of service (QoS) is the overall performance of a network, particularly the performance seen by the users of the network. This is usually measured by several related aspects of the network service, such as error rates, bandwidth, throughput, transmission delay, availability, jitter, etc. All switches rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end devices, or switches or routers along the path. Priority can then be assigned to those classes.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The behavior in which an individual network device handles traffic is called per-hop behavior. All devices along a path (from a source to a destination) should be configured to perform a consistent manner in order to achieve end-to-end Quality of Service (QoS) solution.

This section describes how to specify which data packets have higher priority when traffic is buffered in the switch due to congestion. This switch provides eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each port, the queuing mode, and queue weights.

The switch also allows you to configure QoS classification criteria and service policies. Each packet is classified upon entry into the network based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or its VLAN priority tag.

4.8.1— Port Classification

Use the QoS Ingress Port Classification page to set the basic QoS parameters for a port, including the default traffic class, DP level (IEEE 802.1p), user priority, drop eligible indicator, classification mode for tagged frames, and DSCP-based QoS classification.

Figure 80. Port Classification Settings

Figure 81. QoS Ingress Port Tag Classification (Port 1, same for all)

Path Advanced, Advanced QoS, Port Classification

Parameters

- **Port —** Port identifier.
- **QoS class —** Controls the default QoS class, i.e., the QoS class for frames not classified in any other way. There is a one-to-one mapping between QoS class, queue and priority. A QoS class of 0 (zero) has the lowest priority. (Range: 0-7; Default: 0)
- **DP level —** Controls the default drop priority for frames not classified in any other way. (Range: 0-1; Default: 0)
- **PCP —** Controls the default Priority Code Point (or User Priority) for untagged frames. (Range: 0-7; Default: 0)
- **DEI —** Controls the default Drop Eligible Indicator for untagged frames. (Range: 0-1; Default: 0)
- **Tag Class**. **—** Shows classification mode for tagged frames on this port:
  - **Disabled —** Uses the default QoS class and DP level for tagged frames.
  - **Enabled —** Uses the mapped versions of PCP and DEI for tagged frames. Click on the mode in order to configure the mode and/or mapping.
- **DSCP Based —** Click to Enable DSCP Based QoS Ingress Port Classification (see section 4.8.3.3—Port DSCP on page 99).

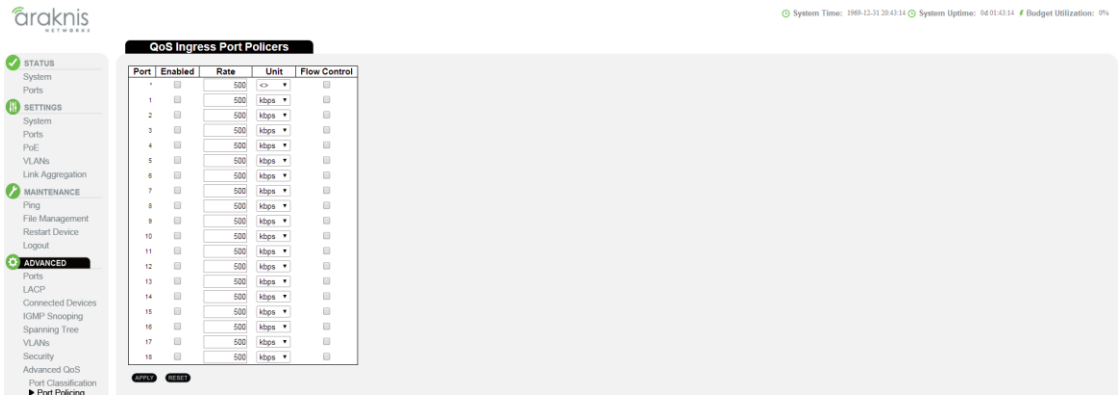
Configuration Instructions To set the basic QoS parameters for a port:

1. Click Configuration, QoS, Port Classification.
2. Set any of the ingress port QoS classification parameters. To change tag class parameters, click “Disabled” to enter the QoS Ingress Port Tag Classification submenu.
3. Click Apply.

4.8.2— Port Policing

This page allows you to configure the Policer settings for all switch ports.

Figure 82. QoS Ingress Port Policers page



Path Advanced, Advanced QoS, Port Policing

Parameters

- **Port —** The port number for which the configuration below applies.
- **Enabled —** Controls whether the policer is enabled on this switch port.
- **Rate —** Controls the rate for the policer. The default value is 500. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps".
- **Unit —** Controls the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps".

Configuration Instructions To set up port policing for one or more ports:

1. Click on Advanced, Advanced QoS, Port Policing
2. Configure Port Policing for each desired port.
3. Click Apply.

4.8.3— Port Scheduler

Use the QoS Egress Port Schedulers page to show an overview of the QoS Egress Port Schedulers, including the queue mode and weight. Click on any of the entries in the Port field to configure egress queue mode, queue shaper (rate and access to excess bandwidth), and port shaper.

Figure 83. QoS Egress Port Schedulers page

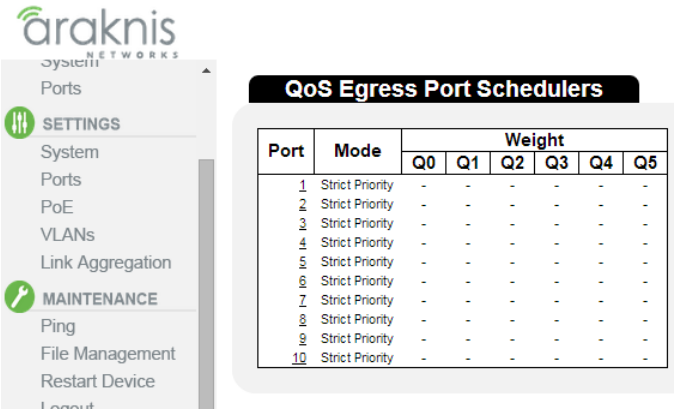


Figure 84. QoS Egress Port Scheduler and Shapers — Strict Mode

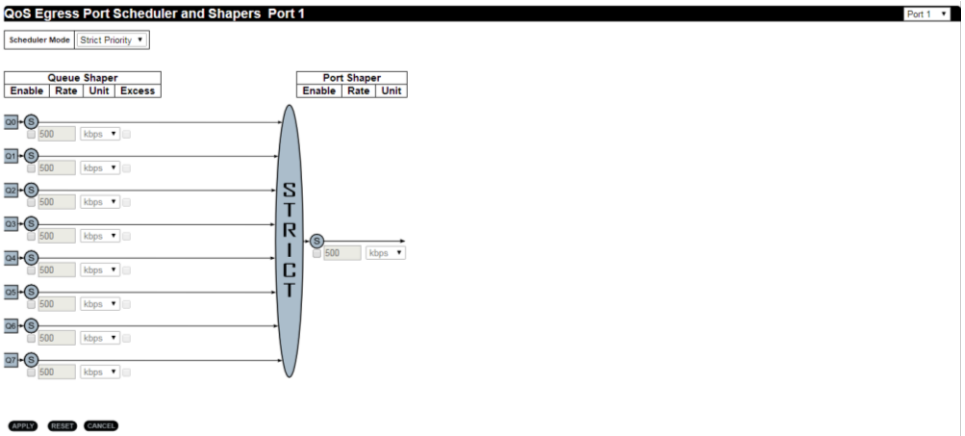
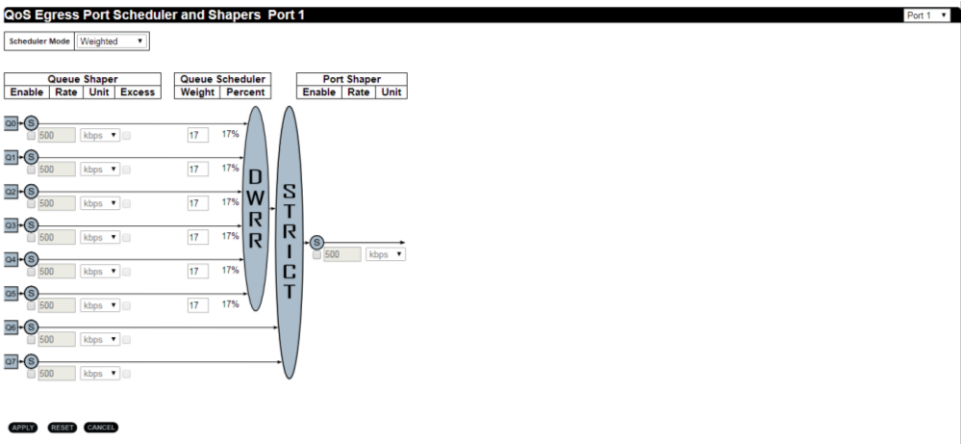


Figure 85. QoS Egress Port Scheduler and Shapers — Weighted Mode



Path Advanced, Advanced QoS, Port Scheduler

Parameters

- **Port** – Port identifier. Click the port number to access advanced scheduling and shaping for the port. (see below)

- **Mode** – Shows the scheduling mode for this port.
- **Weight** – Shows the weight of each egress queue used by the port.
- **On the QoS Egress Port Scheduler and Shapers page for each port (____below):**
  - **Scheduler Mode** – The switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before the lower priority queues are serviced, or Deficit Weighted Round-Robin (DWRR) queuing which specifies a scheduling weight for each queue. (Options: Strict, Weighted; Default: Strict)

    DWRR services the queues in a manner similar to WRR, but the next queue is serviced only when the queue's Deficit Counter becomes smaller than the packet size to be transmitted.

    Note — Weighted scheduling uses a combination of weighted service for queues 0 - 6, and strict service for the high priority queues 7 and 8.

  - **Queue Shaper —** Controls whether queue shaping is enabled for this queue on this port.
    - **Enable —** Enables or disables queue shaping. (Default: Disabled)
    - **Rate —** Controls the rate for the queue shaper. The default value is500. This value is restricted to 100-1000000 kbps, or 1-3300 Mbps.
    - **Unit —** Controls the unit of measure for the queue shaper rate as "kbps" or "Mbps." (Default: kbps)
    - **Excess —** Controls whether the queue is allowed to use excess bandwidth. (Default: Disabled)
  - **Queue Scheduler —** When the Scheduler Mode is set to Weighted, you need to specify a relative weight for each queue. DWRR uses a predefined relative weight for each queue that determines the percentage of service time the switch services each queue before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing.
    - **Weight —** A weight assigned to each of the queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue is polled for service, and subsequently affects the response time for software applications assigned a specific priority value. (Range: 1-100; Default: 17)
    - **Percent —** The weight as a percentage for this queue.
  - **Port Shaper —** Sets the rate at which traffic can egress this queue.
    - **Enable —** Enables or disables port shaping. (Default: Disabled)
    - **Rate —** Controls the rate for the port shaper. The default value is 500. This value is restricted to 100-1000000 kbps, or 1-3300 Mbps
    - **Unit** – Controls the unit of measure for the port shaper rate as "kbps" or "Mbps." (Default: kbps)

Configuration Instructions

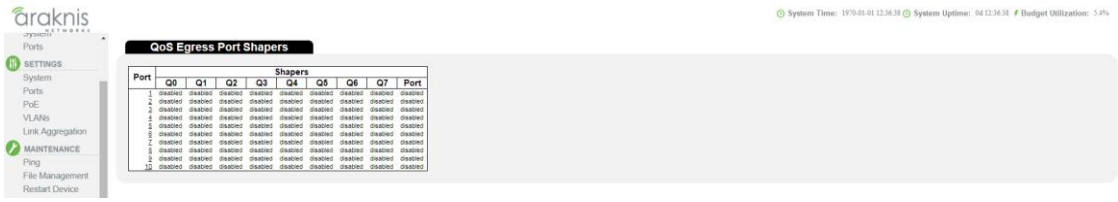
To configure the scheduler mode, the egress queue mode, queue shaper, and port shaper used by egress ports:

1. Click Advanced, Advanced QoS, Port Scheduler.
2. Click on any of the entries in the Port field.
3. Set the scheduler mode, the queue shaper, queue scheduler (when the scheduler mode is set to Weighted), and the port shaper.
4. Click Apply.

4.8.3.1— Port Shaping

Use the QoS Egress Port Shapers page to show an overview of the QoS Egress Port Shapers, including the rate for each queue and port. Click on any of the entries in the Port field to configure egress queue mode, queue shaper (rate and access to excess bandwidth), and port shaper.

Figure 86. QoS Egress Port Shapers Menu



Path Advanced, Advanced QoS, Port Shaper

Parameters

- **Port** – Port identifier.
- **Shapers** – Shows the queue shaper rate and port shaper rate. Configuring QoS Egress Port Scheduler, Queue Scheduler and Port Shapers This configuration page can be access from the Port Scheduler or Port Shaper page. Refer to the description of these parameters under "Port Scheduler".

Configuration Instructions To show an overview of the rate for each queue and port:

1. Click Advanced, Advanced QoS, Port Shaper.
2. Click on any entry under the Port field to configure the Port Scheduler and Shaper. See section 4.8.3—Port Scheduler on page 94.

4.8.3.2— Port Tag Remarking

Use the QoS Egress Port Tag Remarking page to show an overview of QoS Egress Port Tag Remarking mode. Click on any of the entries in the Port field to configure the remarking mode using classified PCP/DEI values, default PCP/DEI values, or mapped versions of QoS class and drop priority.

Figure 87. QoS Egress Port Tag Remarking

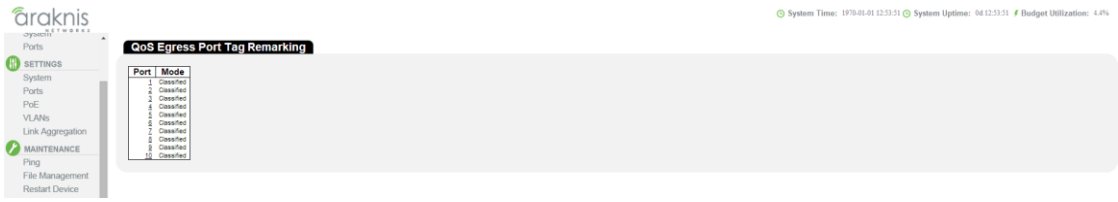


Figure 88. QoS Port tag Remarking — Classified Mode

Figure 89. QoS Port tag Remarking — Default Mode

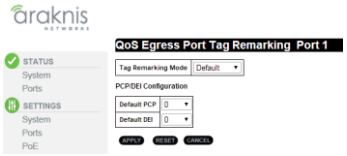
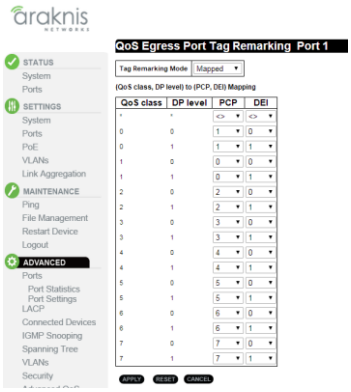


Figure 90. QoS Port tag Remarking — Mapped Mode



Path Advanced, Advanced QoS, Port Tag Remarking

Parameters

- **Main Menu Page:**
  - **Port —** Port identifier.
  - **Mode —** Shows the tag remarking mode used by this port:
    - **Classified —** Uses classified PCP (Priority Code Point or User Priority) and DEI (Drop Eligible Indicator) values.
    - **Default —** Uses default PCP/DEI values.
    - **Mapped —** Uses mapped versions of QoS class and drop precedence level.
- **Configuring Port Remarking Mode:**
  - **Tag Remarking Mode —** Configures the tag remarking mode used by this port:
    - **Classified —** Uses classified PCP/DEI values.
    - **Default —** Uses default PCP/DEI values.(Range: PCP – 0-7, Default: 0; DEI – 0-1, Default: 0)
    - **Mapped —** Controls the mapping of the classified QoS class values and DP levels (drop precedence) to (PCP/DEI) values.
      - **QoS class/DP level —** Shows the mapping options for QoS class values and DP levels (drop precedence).

- **PCP —** Remarks matching egress frames with the specified Priority Code Point (or User Priority) value. (Range: 0-7; Default: 0)
- **DEI —** Remarks matching egress frames with the specified Drop Eligible Indicator. (Range: 0-1; Default: 0)

Configuration Instructions

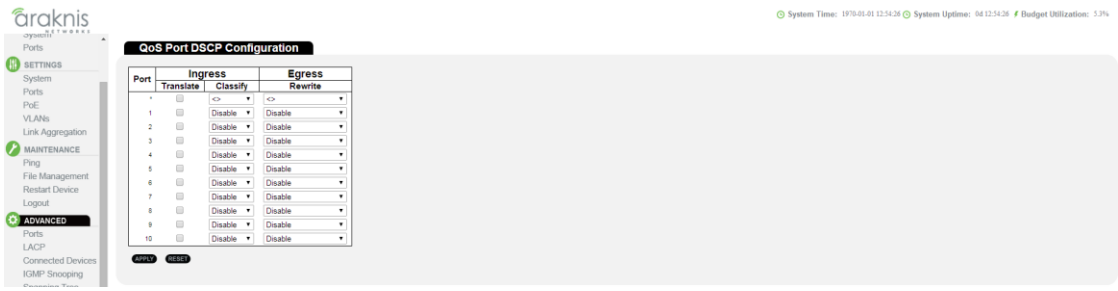
To show the QoS Egress Port Tag Remarking mode used for each port:

1. Click Advanced, Advanced QoS, Port Tag Remarking.
2. Click on any entry under the Port field to configure the Port Tag Remarking mode.
3. Set the tag remarking mode and any parameters associated with the selected mode.
4. Click Apply.

4.8.3.3— Port DSCP

Use the QoS Port DSCP Configuration page to configure ingress translation and classification settings and egress rewriting of DSCP values.

Figure 91. QoS Port DSCP Configuration



Path Advanced, Advanced QoS, Port DSCP

Parameters

- **Port** – Port identifier.
- **Ingress Translate** – Enables ingress translation of DSCP values based on the specified classification method.
- **Ingress Classify** – Specifies the classification method:
  - **Disable** – No Ingress DSCP Classification is performed.
  - **DSCP=0** – Classify if incoming DSCP is 0.
  - **Selected** – Classify only selected DSCP for which classification is enabled in DSCP Translation table (see 4.8.3.5—DSCP Translation on page 101).
  - **All** – Classify all DSCP.
- **Egress Rewrite** – Configures port egress rewriting of DSCP values:
  - **Disable** – Egress rewriting is not performed.
  - **Enable** – Egress rewriting is performed without remapping.
  - **Remap DP Aware** – Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. Depending on the frame's DP level, the remapped DSCP value is either taken from the DSCP Translation table, Egress Remap DP0 or DP1 field (see 4.8.3.5—DSCP Translation on page 101).
  - **Remap DP Unaware** – Frame with DSCP from analyzer is remapped and remarked with the remapped DSCP value. The remapped DSCP value is always taken from the DSCP Translation table, Egress Remap DP0 field (see 4.8.3.5—DSCP Translation on page 101).

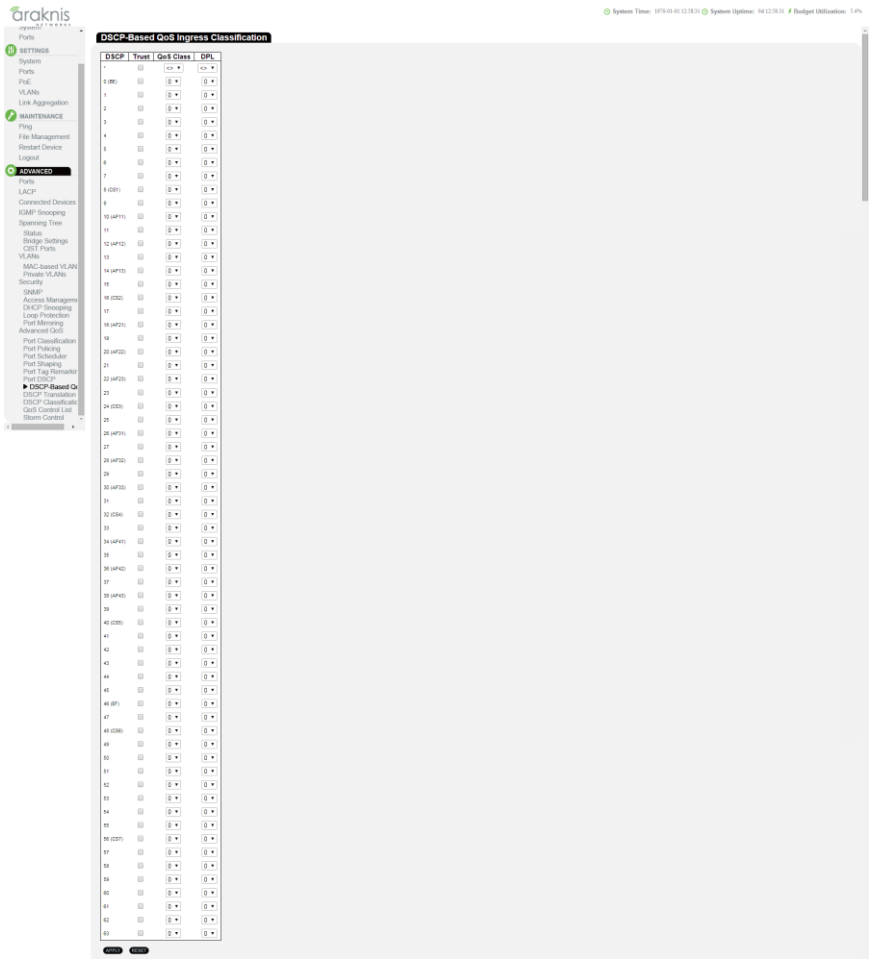
Configuration Instructions To configure ingress translation and classification settings and egress re- writing of DSCP values:

1. Click Advanced, Advance QoS, Port DSCP.
2. Set the required ingress translation and egress re-writing parameters.
3. Click Apply.

4.8.3.4— DSCP-based QoS

Use the DSCP-Based QoS Ingress Classification page to configure DSCP-based QoS ingress classification settings.

Figure 92. DSCP-Based QoS Ingress Classification



Path Advanced, Advance QoS, DSCP-Based QoS

Parameters

- **DSCP —** DSCP value in ingress packets. (Range: 0-63)
- **Trust —** Controls whether a specific DSCP value is trusted. Only frames with trusted DSCP values are mapped to a specific QoS class and drop level (DPL). Frames with untrusted DSCP values are treated as non-IP frames.
- **QoS Class —** QoS value to which the corresponding DSCP value is classified for ingress processing. (Range: 0-7; Default: 0)
- **DPL —** Drop Precedence Level to which the corresponding DSCP value is classified for ingress processing. (Range: 0-1, where 1 is the higher drop priority; Default: 0)

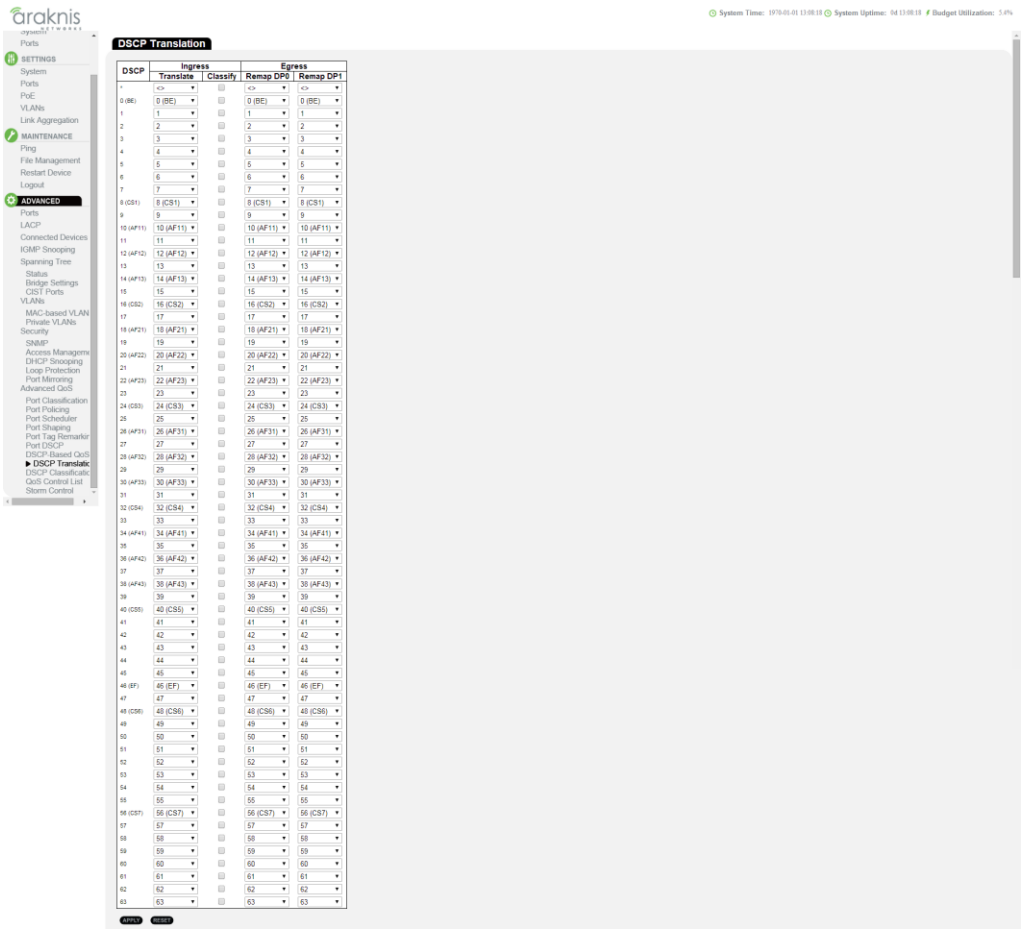
Configuration Instructions To configure DSCP-based QoS ingress classification settings:

1. Click Advanced, Advance QoS, DSCP-Based QoS.
2. Specify whether the DSCP value is trusted, and set the corresponding QoS value and DP level used for ingress processing.
3. Click Apply.

4.8.3.5— DSCP Translation

Use the DSCP Translation page to configure DSCP translation for ingress traffic or DSCP re-mapping for egress traffic.

Figure 93. DSCP Translation Table



Path Advanced, Advanced QoS, DSCP Translation

Parameters

- **DSCP** – DSCP value. (Range: 0-63)
- **Ingress Translate** – Enables ingress translation of DSCP values based on the specified classification method.
- **Ingress Classify** – Enable Classification at ingress side as defined in the QoS Port DSCP Configuration table (see section 4.8.3.3—Port DSCP on page 99).
- **Egress Remap DP0** – Re-maps DP0 field to selected DSCP value. DP0 indicates a drop precedence with a low priority.
- **Egress Remap DP1** – Re-maps DP1 field to selected DSCP value. DP1 indicates a drop precedence with a high priority.

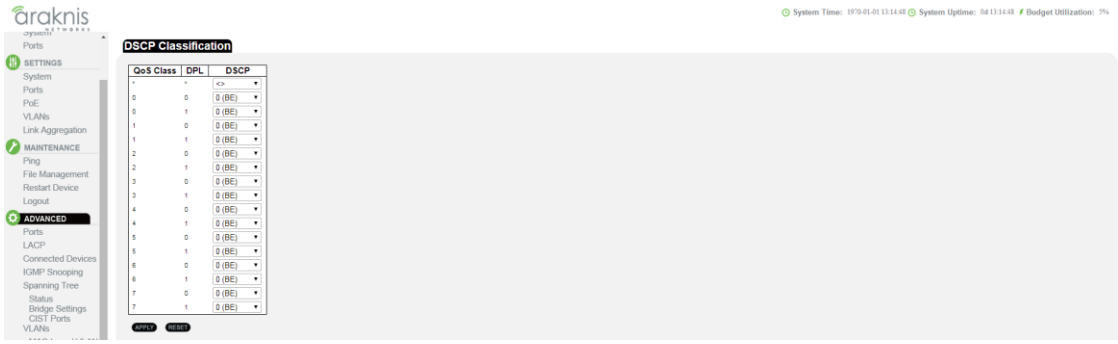
Configuration Instructions To configure DSCP translation or re-mapping:

1. Click Advanced, Advanced QoS, DSCP Translation.
2. Set the required ingress translation and egress re-mapping parameters.
3. Click Apply.

4.8.3.6— DSCP Classification

Use the DSCP Classification page to map DSCP values to a QoS class and drop precedence level.

Figure 94. DSCP Classification



Path Advanced, Advanced QoS, DSCP Classification

Parameters

- **QoS class/DPL** – Shows the mapping options for QoS class values and DP (drop precedence) levels.
- **DSCP** – DSCP value. (Range: 0-63)

Configuration Instructions To map DSCP values to a QoS class and drop precedence level.

1. Click Advanced, Advanced QoS, DSCP Classification.
2. Map key DSCP values to a corresponding QoS class and drop precedence level.
3. Click Apply.

4.8.3.7— QoS Control List

Use the QoS Control List Configuration menu to configure Quality of Service policies for handling ingress packets based on Ethernet type, VLAN ID, TCP/UDP port, DSCP, ToS, or VLAN priority tag.

Once a QCE is mapped to a port, traffic matching the first entry in the QoS Control List is assigned to the QoS class, drop precedence level, and DSCP value defined by that entry. Traffic not matching any of the QCEs are classified to the default QoS Class for the port.

Figure 95. QoS Control List

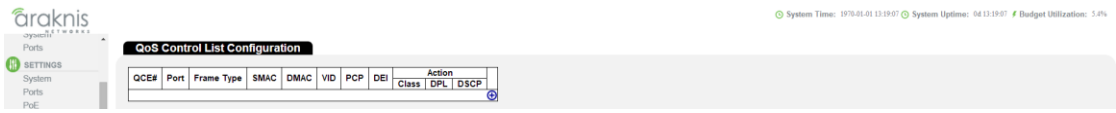
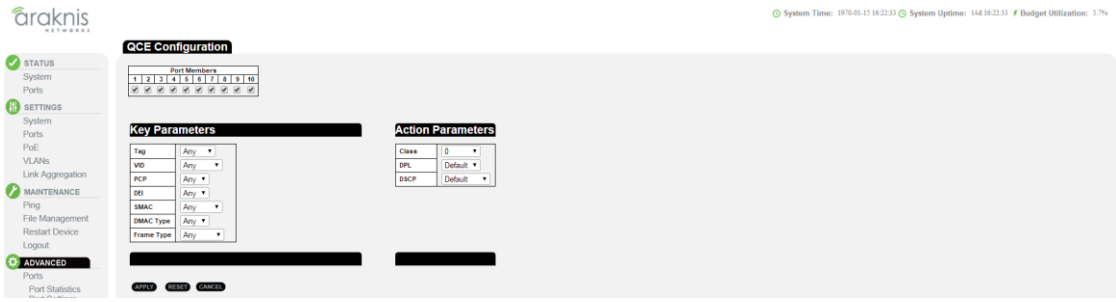


Figure 96. QCE Configuration



Path Configuration, QoS, QoS Control List

Parameters

QoS Control List

- **QCE** – Quality Control Entry index.
- **Port** - Port identifier.
- **Frame Type** – Indicates the type of frame to look for in incoming frames. Possible frame types are: Any, Ethernet, LLC, SNAP, IPv4, IPv6.
- **SMAC** - The OUI field of the source MAC address, i.e. the first three octets (bytes) of the MAC address.
- **DMAC** - The type of destination MAC address. Possible values are: Any, Broadcast, Multicast, Unicast.
- **VID** – VLAN identifier. (Range: 1-4095)
- **Action** – Indicates the classification action taken on ingress frame if the configured parameters are matched in the frame's content. If a frame matches the QCE, the following actions will be taken:
  - **Class** (Classified QoS Class) – If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class.
  - **DPL** – The drop precedence level will be set to the specified value.
  - **DSCP** – The DSCP value will be set the specified value. The following buttons are used to edit or move the QCEs:

QCE Configuration

- **Port Members** – The ports assigned to this entry.

Key Parameters

- **Tag** – VLAN tag type. (Options: Any, Tag, Untag; Default: Any)
- **VID** – VLAN identifier. (Options: Any, Specific (1-4095), Range; Default: Any)
- **PCP** – Priority Code Point (User Priority). (Options: a specific value of 0, 1, 2, 3, 4, 5, 6, 7, a range of 0-1, 2-3, 4-5, 6-7, 0-3, 4-7, or Any; Default: 0)

- **DEI** – Drop Eligible Indicator. (Options: 0, 1 or Any)
- **SMAC** – The OUI field of the source MAC address. Enter the first three octets (bytes) of the MAC address, or Any.
- **DMAC Type** – The type of destination MAC address. (Options: Any, BC (Broadcast), MC (Multicast), UC (Unicast)
- **Frame Type** – The supported types are listed below:
  - **Any** – Allow all types of frames.
  - **Ethernet** – This option can only be used to filter Ethernet II formatted packets. (Options: Any, Specific – 600-ffff hex; Default: ffff)
    - Note that 800 (IPv4) and 86DD (IPv6) are excluded.
    - A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
  - **LLC** – Link Logical Control includes the following settings:
  - **SSAP Address** – Source Service Access Point address. (Options: Any, Specific (0x00-0xff); Default: 0xff)
  - **DSAP Address** – Destination Service Access Point address. (Options: Any, Specific (0x00-0xff); Default: 0xff)
  - **Control** – Control field may contain command, response, or sequence information depending on whether the LLC frame type is Unnumbered, Supervisory, or Information. (Options: Any, Specific (0x00-0xff); Default: 0xff)
  - **SNAP** – SubNetwork Access Protocol can be distinguished by an OUI and a Protocol ID. (Options for PID: Any, Specific (0x00-0xffff); Default: Any)
    - If the OUI is hexadecimal 000000, the protocol ID is the Ethernet type (EtherType) field value for the protocol running on top of SNAP. If the OUI is that of a particular organization, the protocol ID is a value assigned by that organization to the protocol running on top of SNAP.
    - In other words, if value of the OUI field is 00-00-00, then value of the PID will be etherType (0x0600-0xffff), and if value of the OUI is other than 00-00-00, then valid value of the PID will be any value from 0x0000 to 0xffff.
  - **IPv4** – IPv4 frame type includes the following settings:
  - **Protocol** – IP protocol number. (Options: Any, UDP, TCP, or Other (0-255))
  - **Source IP** – Source IP address. (Options: Any, Specific)
    - To configure a specific source IP address, enter both the address and mask format. The address and mask must be in the format x.y.z.w where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero
  - **IP Fragment** – Indicates whether or not fragmented packets are accepted. (Options: Any, Yes, No; Default: Any)
    - Datagrams may be fragmented to ensure they can pass through a network device which uses a maximum transfer unit smaller than the original packet's size.
  - **DSCP** – Diffserv Code Point value. (Options: Any, specific value of 0-63, BE, CS1-CS7, EF or AF11-AF43, or Range; Default: Any)
  - **IPv6** – IPv6 frame type includes the same settings as those used for IPv4, except for the Source IP. When configuring a specific IPv6 source address, enter the least significant 32 bits (a.b.c.d) using the same type of mask as that used for an IPv4 address.
  - **Sport** – Source TCP/UDP port. (Any, Specific/Range: 0-65535)
  - **Dport** – Destination TCP/UDP port. (Any, Specific/Range: 0-65535)

Action Parameters

- **Action** – Indicates the classification action taken on ingress frame if the configured parameters are matched in the frame's content. If a frame matches the QCE, the following

actions will be taken:

- **Class** (Classified QoS Class) – If a frame matches the QCE, it will be put in the queue corresponding to the specified QoS class, or placed in a queue based on basic classification rules. (Options: 0-7, Default (use basic classification); Default setting: 0)
- **DPL** – The drop precedence level will be set to the specified value or left unchanged. (Options: 0-1, Default; Default setting: Default)
- **DSCP** – The DSCP value will be set to the specified value or left unchanged. (Options: 0-63, BE, CS1-CS7, Default (not changed); Default setting: Default)

Configuration Instructions

To configure QoS Control Lists:

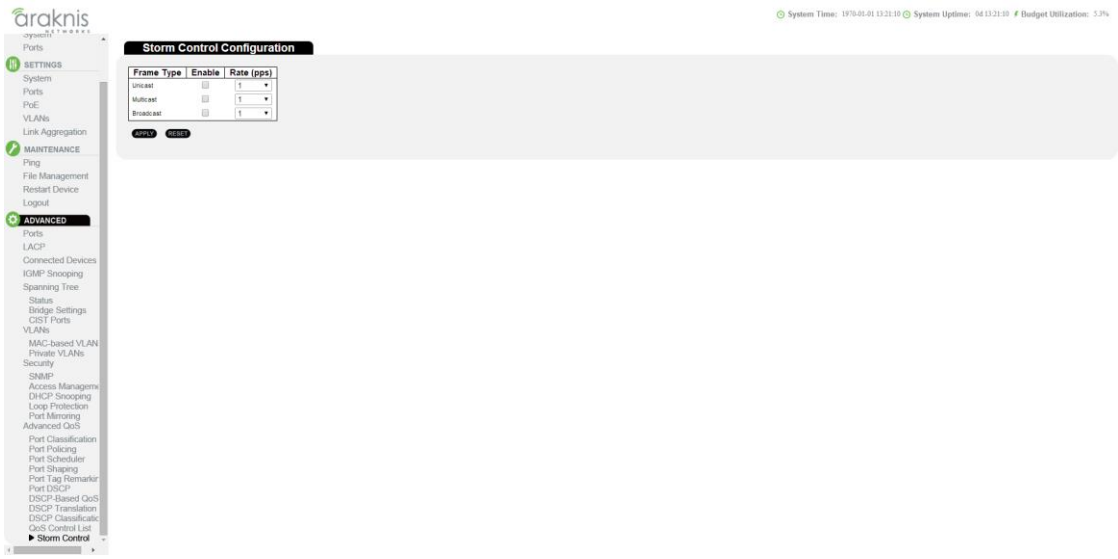
1. Click Configuration, QoS, QoS Control List.
2. Click the button to add a new QCE, or use the other QCE modification buttons to specify the editing action (i.e., edit, delete, or moving the relative position of entry in the list).
3. When editing an entry on the QCE Configuration page, specify the relevant criteria to be matched, and the response to a match.
4. Click Save.

4.8.3.8— Storm Control

Use the Storm Control Configuration page to set limits on broadcast, multicast and unknown unicast traffic to control traffic storms which may occur when a network device is malfunctioning, the network is not properly configured, or application programs are not well designed or properly configured. Traffic storms caused by any of these problems can severely degrade performance or bring your network to a complete halt.

You can protect your network from traffic storms by setting a threshold for broadcast, multicast, or unknown unicast traffic. Any packets exceeding the specified threshold will then be dropped. Note that the limit specified on this page applies to each port.

Figure 97. Storm Control Configuration



Path Advanced, Advanced QoS, Storm Control

Parameters

- **Frame Type** - Specifies broadcast, multicast or unknown unicast traffic.
- **Status** - Enables or disables storm control. (Default: Disabled)
- **Rate (pps)** - The threshold above which packets are dropped. This limit can be set by specifying a value of 2n packets per second (pps), or by selecting one of the options in Kpps (i.e., marked with the suffix “K”). (Options: 2n pps where n = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512; or 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024 Kpps; Default: 2 pps)\

  Due to an ASIC limitation, the enforced rate limits are slightly less than the listed options. For example: 1 Kpps translates into an enforced threshold of 1002.1 pps.

Configuration Instructions To configure Storm Control:

1. Click Advanced, Advanced QoS, Storm Control.
2. Enable storm control for unknown unicast, broadcast, or multicast traffic by marking the Status box next to the required frame type.
3. Select the control rate as a function of 2n pps (i.e., a value with no suffix for the unit of measure) or a rate in Kpps (i.e., a value marked with the suffix “K”).
4. Click Apply.

300 Series Non-PoE Managed Switch Specifications				
Model —		**AN-300-SW-F/R-8**	**AN-300-SW-F/R-16**	**AN-300-SW-F/R-24**
Interface				
Ports	**10/100/1000Base RJ-45 Ports**	8	16	24
	1000Base SFP	2	2	2
	PoE Ports	---	---	---
Physical Configuration				
Flash Memory		16MB SPI		
SDRAM		128MB		
Packet Buffer		512KB		
Performance				
MAC Address Table		8K		
Switching Capacity		20Gbps	36Gbps	52Gbps
Forwarding Rate		14.8Mpps	26.7Mpps	38.7Mpps
L2 Features				
Flow Control	**802.3x, Back Pressure**	Yes		
Spanning Tree	**802.1D (STP)/802.1w (RSTP)**	Yes		
	802.1s (MSTP)	Yes		
VLAN	**802.1Q**	Yes		
	VLAN Group	4K		
	Port-based VLANs	Yes		
	MAC-based VLANs	Yes		
	Private VLANs/QinQ/MVR	Yes		
	Protocol-based VLAN/Voice VLAN	Yes		
Link Aggregation	**Static, 802.3ad LACP**	Yes		
	Maximum Candidate Ports	10	18	26
	Maximum Ports per Group	10	16	16
	Max Group	13		
Multicast	**IGMP Snooping v1/v2/v3**	Yes		
	MLD Snooping v1/v2	Yes		
	Maximum Multicast Group Address	8K		
	Querier, Immediate Leave	Yes		
Storm Control	**Broadcast/Multicast/Unknown Unicast**	Yes		
Jumbo Frame Support		9K		
QoS Features				
Number of priority queues		8 queues/port		
Rate Limiting	**Ingress**	Yes, 1Kbps/1pps		
	Egress	Yes, 1Kbps/1pps		
DiffServ (RFC2474)		Yes		
Scheduling	**WRR, Strict, Hybrid**	Yes		
CoS	**802.1p**	Yes		
	IP ToS Precedence, IP DSCP	Yes		

(continued)

Model —		AN-300-SW-F/R-8	AN-300-SW-F/R-16	AN-300-SW-F/R-24
Security				
Port Security (MAC-based)		Yes		
802.1x		Yes		
ACL	L2/L3/L4	Yes		
IP Source Guard		Yes		
RADIUS		Yes		
TACACS+		Yes		
HTTPS and SSL		Yes		
SSH v2.0		Yes		
MAC Filter		Yes		
IP Filter		Yes		
Management				
Management	CLI, Web, Telnet	Yes		
Dual FW Images		Yes		
Management Access Filtering	SNMP/Web/Telnet	Yes		
SNMP	v1,2c,3	Yes		
RMON (1,2,3 and 9 groups)		Yes		
DHCP	Client, Relay/Option82, Snooping	Yes		
Event log	Local flash, Remote server	Yes		
sFlow		Yes		
Port Mirroring	One to One, Many to One	Yes		
Remote Ping		Yes		
NTP		Yes		
LLDP/UPnP		Yes		
Cable Diagnostics		Yes		
Environmental				
Dimensions	Inches (WxHxD)	1.7 x 12.9 x 8.2	1.7 x 12.9 x 8.2	1.7 x 17.2 x 8.6
Power Supply		100-240V AC, 50/60 Hz		
Maximum Power Consumption for System (W)		7W	12W	16W
Operating Temperature (°F)		32 - 104°F		
Humidity (non-condensing)		10 - 90%		
Weight (lbs.)		4.4	4.7	6.2
Certification				
FCC Class A		Yes		
CE		Yes		
UL		Yes		

300 Series PoE Managed Switch Specifications

Model		AN-300-SW-F/R-8-POE	AN-300-SW-F/R-16-POE	AN-300-SW-F/R-24-POE
Interface				
Ports	10/100/1000Base RJ-45 Ports	8	16	24
	1000Base SFP	2	2	2
	PoE Ports	8	16	24
Physical Configuration				
Flash Memory		16MB SPI		
SDRAM		128MB		
Packet Buffer		512KB		
Performance				
MAC Address Table		8K		
Switching Capacity		20Gbps	36Gbps	52Gbps
Forwarding Rate		14.8Mpps	26.7Mpps	38.7Mpps
PoE Features				
802.3af/at Compliant		Yes		
Max Power Output per Port		30W		
PoE Power Budget		120W	240W	360W
PD Classification		Yes		
Rate	Enable/Disable per port	Yes		
	Priority Setting per port	Yes		
	Overloading Protection per port	Yes		
	Power level setting per port	Yes		
L2 Features				
Flow Control	802.3x, Back Pressure	Yes		
Spanning Tree	802.1D (STP)/802.1w (RSTP)	Yes		
	802.1s (MSTP)	Yes		
VLAN	802.1Q	Yes		
	VLAN Group	4K		
	Port-based VLANs	Yes		
	MAC-based VLANs	Yes		
	Private VLANs/QinQ/MVR	Yes		
	Protocol-based VLAN/Voice VLAN	Yes		
Link Aggregation	Static, 802.3ad LACP	Yes		
	Maximum Candidate Ports	10	18	26
	Maximum Ports per Group	10	16	16
	Max Group	13		
Multicast	IGMP Snooping v1/v2/v3	Yes		
	MLD Snooping v1/v2	Yes		
	Maximum Multicast Group Address	8K		
	Querier, Immediate Leave	Yes		
Storm Control	Broadcast/Multicast/Unknown Unicast	Yes		
Jumbo Frame Support		9K		

(continued)

Model		AN-300-SW- F/R-8-POE	AN-300-SW- F/R-16-POE	AN-300-SW- F/R-24-POE
QoS Features				
Number of priority queues		8 queues/port		
Rate Limiting	Ingress	Yes, 1Kbps/1pps		
	Egress	Yes, 1Kbps/1pps		
DiffServ (RFC2474)		Yes		
Scheduling	WRR, Strict, Hybrid	Yes		
CoS	802.1p	Yes		
	IP ToS Precedence, IP DSCP	Yes		
Security				
Port Security (MAC-based)		Yes		
802.1x		Yes		
ACL	L2/L3/L4	Yes		
IP Source Guard		Yes		
RADIUS		Yes		
TACACS+		Yes		
HTTPS and SSL		Yes		
SSH v2.0		Yes		
MAC Filter		Yes		
IP Filter		Yes		
Management				
Management	CLI, Web, Telnet	Yes		
Dual FW Images		Yes		
Management Access Filtering	SNMP/Web/Telnet	Yes		
SNMP	v1,2c,3	Yes		
RMON (1,2,3 and 9 groups)		Yes		
DHCP	Client, Relay/Option82, Snooping	Yes		
Event log	Local flash, Remote server	Yes		
sFlow		Yes		
Port Mirroring	One to One, Many to One	Yes		
Remote Ping		Yes		
NTP		Yes		
LLDP/UPnP		Yes		
Cable Diagnostics		Yes		
Environmental				
Dimensions	Inches (WxHxD)	1.7 x 12.9 x 8.2	1.7 x 12.9 x 8.2	1.7 x 17.2 x 8.6
Power Supply		100-240V AC, 50/60 Hz		
Maximum Power Consumption for System (W)		7W	12W	16W
Operating Temperature (°F)		32 - 104°F		
Humidity (non-condensing)		10 - 90%		
Weight (lbs.)		4.4	4.7	6.2
Certifications				
FCC Class A		Yes		
CE		Yes		
UL		Yes		

5.1— Contacting Technical Support

Table 7. Tech Support

Phone:	(866) 838-5052
Email:	support@snapav.com

5.2— 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 SnapAV or a designated service center with prior notification and an assigned return authorization number (RA).