

QUICK SETUP GUIDE



Luxul L2/L3 Managed Switches

XMS-2624P, XMS-5248P, XMS-7048P

AMS-1208P, AMS-2616P, AMS-2624P, AMS-4424P

AMS-2600

- ▶ Quick Installation
- ▶ Quick System Setup
- ▶ IP Configuration and Routing
- ▶ PoE
- ▶ VLANs
- ▶ Private VLANs
- ▶ Spanning Tree

LUXUL

CONTENTS

INTRODUCTION	1
QUICK INSTALLATION	2
Rack Installation	2
Ethernet and Power Connections	2
Network Cabling	2
IP Addressing	2
Getting Connected.....	3
Logging In	3
MANAGED SWITCH BASICS	4
QUICK SETUP: SYSTEM	5
System	5
Information.....	5
IP.....	6
NTP.....	8
Time	9
Log	11
UNDERSTANDING POE	13
QUICK SETUP: POE	14
UNDERSTANDING VLANS	16
QUICK SETUP: VLANS	17
Global VLAN Configuration	17
Port VLAN Configuration	18
Allowed VLANs	19
Forbidden VLANs	19
QUICK SETUP: PRIVATE VLANS	20
VLAN Membership	20
VLAN Port Isolation	21
UNDERSTANDING SPANNING TREE	22
QUICK SETUP: SPANNING TREE	23
Bridge Settings.....	23
MSTI Mapping	25
MSTI Priorities	26
CIST Ports	27
MSTI Ports.....	29

INTRODUCTION

This guide covers installation and basic setup of the following models of Luxul managed switches using the built-in web configuration interface:

- ▶ AMS-2600
- ▶ AMS-1208P, AMS-2616P, AMS-2624P, AMS-4424P
- ▶ XMS-2624P, XMS-5248P, XMS-7048P

✓ NOTE: *This guide covers several different Luxul L2/L3 managed switch models. Not all features covered in this guide will apply to every model of switch. Refer to the spec sheet and/or the switch web interface for features specific to the model.*

This guide assumes you have a reasonable working knowledge of basic networking concepts and that you're already familiar with managed switches and their capabilities. If you aren't familiar with managed switches, routing, and other advanced networking concepts, we recommend you familiarize yourself with these concepts before you attempt to configure a Luxul managed switch.

Visit luxul.com/educational-webinars to find informative webinars ranging from basic networking to relatively advanced topics like remote access, VPNs, routing and VLANs.

QUICK INSTALLATION

Before you can start configuring your switch, you'll need to install it in a safe, stable location, then connect it to a network and/or connect your computer to the switch to configure it. If your Luxul switch is already installed, and connected to the network, and you can access it from your computer, you can skip ahead to the next section titled QUICK SETUP: SYSTEM.

1 Physical Installation

Luxul AMS- and XMS- series switches should be rack-mounted. Install the switch in a stable/safe rack to avoid any possible damage. Make sure there is adequate space around the switch for proper ventilation and heat dissipation. Avoid placement in direct sunlight, do not place heavy articles on the switch and verify that the outlet's ground connection is functioning properly.

Rack Installation

Use the included brackets for convenient installation in a 19-inch server or audio rack. Use the included screws to attach the L-shaped brackets to each side of the switch, and horizontally insert the switch into a free space within the rack. Use your desired hardware to affix the switch supports to the rack.

2 Connecting Ethernet and Power

Ethernet and Power Connections

Use any RJ-45 cable to connect the switch to an Ethernet-enabled device, including servers, routers and other switches. No crossover cable is necessary.

The AMS- and XMS- series switches support 10/100/1000 Mbps Ethernet; 10/100 Mbps half/full-duplex mode and 1000 Mbps full-duplex mode. All RJ-45 ports support Auto MDI/MDIX and can be used as ordinary ports or as Uplink ports.

The rear panel features an AC input socket and power switch. Use the included power cable to connect the switch to a surge-protected outlet.

Network Cabling

For connecting to the RJ-45 ports, Luxul recommends Category-5, super Category-5 or Category-6 unshielded twisted pair (CAT5/CAT5e/CAT6 UTP). To ensure best performance and stable data transmission at 1000 Mbps, use Category-6 shielded twisted pair. For connecting to the SFP ports, optical fiber/cable should be selected based on the wavelength of the SFP optical module to be used.

⚠ CAUTION: Multiple Uplink channels can create loops, resulting in network failure. Ensure only one Uplink channel exists between switches or between the switch and a router.

✔ NOTE: When powering up, the port LEDs corresponding to the optical interface may take a moment to initialize. This is normal as the switch initialization and startup completes.

✔ NOTE: For optimal switch performance, do not exceed the combined consumption budget for all external PoE devices connected to a PoE switch: 130w for AMS-1208P, 250w for AMS-2616P and AMS-2624P, 370w for AMS-2624P and XMS-2624P, and 740w for the XMS-5248P and XMS-7048P.

3 Preparing for Access

IP Addressing

If the Luxul managed switch is connected to a network with a 192.168.0.X address scheme, and your computer shares a similar address on the same network, you can skip to the next step, **Access and Setup**.

✔ **NOTE:** *If another device on your network shares the same IP address as the switch's default IP address, you'll need to temporarily reassign or disconnect that device while you configure the switch.*

If your network uses an address scheme other than 192.168.0.X, you'll need to set a temporary static IP address on the computer you're using for configuration. To do so, set the IP address of your computer to an address in the 192.168.0.X range (but not one of the addresses in the table below), then set the Gateway/Router address to one of the addresses below that coincides with the switch you're configuring (refer to the table below).

Once you're finished configuring the switch, you can return your computer's IP address configuration to normal, typically "Obtain Automatically/DHCP."

✔ **NOTE:** Visit <http://luxul.com/ip-addressing> to learn more about changing your computer's IP address and getting connected.

4 Access and Setup

Getting Connected

Use an Ethernet cable to connect your computer to the switch, then power on the switch.

Logging In

To access the Luxul managed switch web configuration, open your web browser and enter the default IP address in the address field (refer to table below). Log in to the switch using the default user name and password:

Default IP: (Refer to table below)

Username: admin

Password: admin

Refer to the following table to find the default IP address of the switch you're configuring.

Switch Model(s)	Default IP Address
AMS-2600	192.168.0.2
AMS-1208P	192.168.0.3
AMS-2616P, AMS-2624P, AMS-4424P, XMS-2624P, XMS-5248P, XMS-7048P	192.168.0.4

Once you're logged in to the switch web configuration, continue with configuration as described in the next chapter, Quick Setup: System.

5 Hardware Operation

The front panel of the AMS-series switches include dual-color Link/Activity LEDs that can be switched from green to blue. In addition, the front panel has Link/Activity and PoE mode indicators as well as System and Power LEDs.

Indicator	State	Description
POWER	On	The switch is powered on.
	Off	The switch is powered off or not connected to AC power. Check power connections and power switch at the back of the unit.
Link/Act	On	There is a device connected to the port.
	Flashing	Port is receiving or transmitting data.
	Off	No device is connected to the port.
1000 Mbps	On	A 1000 Mbps-capable device is connected.
	Off	No device is connected and/or the device is not 1000 Mbps-capable.
PoE	On	A PoE-enabled device is connected and the switch is supplying power to the device.
	Off	No PoE-enabled device is connected or PoE is not enabled on this port
SYSTEM	On	The switch is booting.
	Flashing	The switch is running normally.
	Off	The switch is in startup and initialization process or is not on.

At startup, port LEDs will flash for 1 second as a self test.

MANAGED SWITCH BASICS

Before you get started setting up your new Luxul managed switch, it's helpful to have a basic understanding of a few advanced networking concepts. In this document, we assume you already understand basic networking. If you don't, just visit luxul.com/educational-webinars to view informative webinars on subjects ranging from IP networking basics, wired, and wireless networking, to advanced topics like remote access and using VLANs for guest network access.

What is a Network Switch?

Fundamentally, a network switch simply connects devices together on a computer network, receiving, processing and forwarding data from one device to another. Unlike simple network hubs, switches can forward data only to devices that need to receive it, rather than broadcasting the same data out of each of its ports.

What are “Layers”?

Without going into too much technical detail, “layers” in networking describe standards for different levels of functionality and operation.

- ▶ Layer 1 switches are the most basic, functioning in the “physical layer”, essentially connecting devices together.
- ▶ Layer 2 switches work with the “data link layer” and uses hardware to function like a multi-port bridge.
- ▶ Layer 3 switches function in the “network layer” and manage multi-node networks, including addressing, routing and traffic control. Layer 3 switches are the most capable of the three and offer functionality very similar to a router, but with more physical ports.

Switches may operate at one or more layers, including the data link and network layers. A device that operates simultaneously at more than one of these layers is known as a multilayer switch. The Luxul managed switches covered in this document are multilayer switches.

Managed Versus Unmanaged

There are two basic types of network switches: managed and unmanaged. Unmanaged switches have no configuration interface or options and are generally plug-and-play devices. Most unmanaged switches are Layer 1 switches since they require no configuration.

Managed switches include a full set of management features such as Spanning Tree Protocol or port mirroring, creating or modifying virtual LANs (VLANs), etc., so are typically Layer 2 or Layer 3 switches. The switches covered in this guide are Layer 3 managed switches.

Now that you have a basic understanding of what managed switches do, you can get started with configuration.

QUICK SETUP: SYSTEM

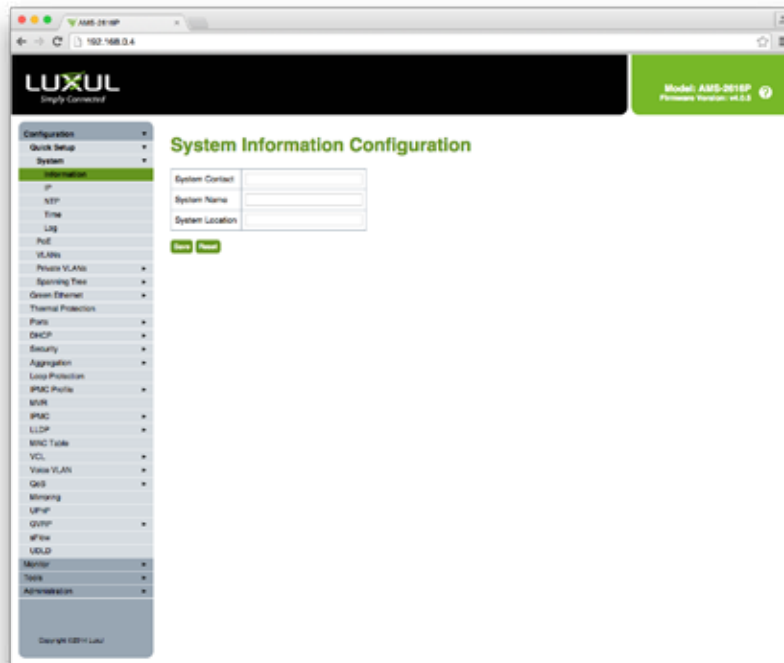
This chapter covers Configuration of functions found in the “System” section of the configuration interface, including Information, IP, NTP, Time and Log.

System

By configuring the System Information settings including System Contact, System Name and System Location, you can easily identify the Switch location and function. This is particularly helpful in installations with several switches in multiple locations.

Information

To access the System Information Configuration, click Configuration > Quick Setup > System > Information in the navigation menu.



System Information Configuration

System Contact: The Name and Contact Information of the Switch Administrator. The allowed string length is 0 to 128 characters but does not allow spaces.

System name: The Name assigned to the Switch to enable easy identification of the Switch. This entry will also be used as the switch's hostname on the local Network. The allowed string length is 0 to 128 characters and follows standard Hostname conventions. The permitted characters are numbers, uppercase letters, lowercase letters, and hyphens. Spaces and special characters (i.e. !@#%) are not permitted. The first character of the hostname must be an alpha character and last character may not be a hyphen.

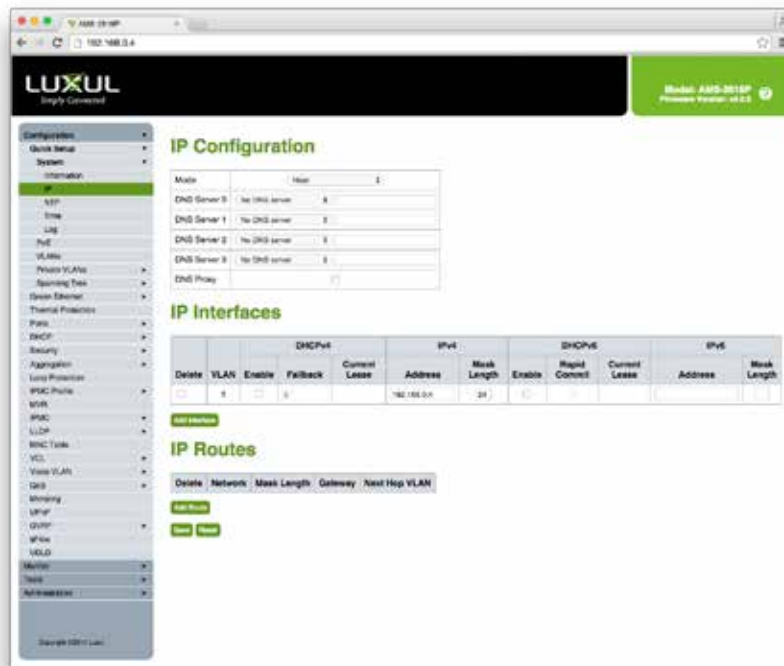
System Location: The physical location of the switch (i.e. Telephone Closet, 3rd floor). The allowed string length is 0 to 128 characters and all characters are permitted including spaces.

- **Save:** Click to save any unsaved changes.
- **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

IP

The IP address of the switch is set to 192.168.0.4 (or 192.168.0.3 for the AMS-1208P) by default. The IP address can also be obtained via the DHCP server for VLAN 1. To manually configure a custom IP address, you can change the switch default settings to values that are compatible with your network. We also recommend configuring DNS servers and a Default Gateway, allowing the switch to obtain time and date information.

To configure switch IP settings, select Configuration > Quick Setup > System > IP from the navigation menu.



IP Configuration

IP Configuration

Mode: Configure whether the IP stack should act as a Host or a Router. In Host Mode, IP traffic between interfaces will not be routed (including VLANs). In Router Mode traffic is routed between all interfaces (including VLANs).

DNS Server: This setting configures the DNS name resolution of the Switch. The following Modes are supported:

- **From any DHCPv4 interfaces:** The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.
- **No DNS server:** No DNS server will be used.
- **Configured IPv4:** Allows you to provide the IP Address of the DNS Server.
- **From this DHCPv4 interface:** Specify from which DHCP-enabled interface a provided DNS server should be configured.

- ▶ **From any DHCPv6 interfaces:** The first DNS server offered from a DHCP lease to a DHCP-enabled interface will be used.
- ▶ **Configured IPv6:** Allows you to provide the IP Address of the DNS Server.
- ▶ **From this DHCPv6 interface:** Specify from which DHCP-enabled interface a provided DNS server should be configured.
- ▶ **DNS Proxy:** When DNS proxy is enabled the Switch will relay DNS requests to the configured DNS server, and reply as a DNS resolver to the client devices connected through the Switch.

IP Interfaces

Delete: Select this option to delete an existing IP Interface.

VLAN: The VLAN associated with this IP interface. Only Ports in this VLAN will be able to access this IP Interface. This field is only available for input when creating a new Interface.

DHCPv4

- ▶ **DHCPv4 - Enable:** Enable the DHCP client by checking the Enable check-box. If this option is enabled the Switch will configure the IPv4 Address and mask of the interface using DHCP. The DHCP client will announce the configured System Name as hostname to provide local DNS lookup.
- ▶ **DHCPv4 - Fallback:** The number of seconds the Switch will try to obtain a DHCP lease. After this period expires the configured IPv4 Address will be used as the IPv4 interface Address. A value of zero disables the fallback mechanism, the Switch will keep retrying until a valid DHCP lease is obtained. The available range is from 0-4294967295 seconds.
- ▶ **DHCPv4 - Current Lease:** For DHCP interfaces with an active lease this column shows the current interface Address as provided by the DHCP server.

IPv4

- ▶ **IPv4 - IPv4 Address:** The static IPv4 Address of the interface (set to 192.168.0.4 by default). The field may also be left blank if IPv4 operation on the interface is not desired. If DHCP is enabled this field is not used.
- ▶ **IPv4 – Mask Length:** The IPv4 Network mask in number of bits (also called CIDR notation). Valid values are between 0 and 30 bits for an IPv4 Address. The field may also be left blank if IPv4 operation on the interface is not desired. If DHCP is enabled, this field is not used.

DHCPv6

- ▶ **DHCPv6 - Enable:** Enable the DHCP client by checking the Enable checkbox. If this option is enabled the Switch will configure the IPv6 Address and mask of the interface using DHCP. The DHCP client will announce the configured System Name as hostname to provide local DNS lookup.
- ▶ **DHCPv6 – Rapid Commit:** Allows the Switch to change the IPv6 Address as soon as a new lease is advertised to the interface.
- ▶ **DHCPv6 – Current Lease:** For DHCP interfaces with an active lease this column shows the current interface Address as provided by the DHCP server.

IPv6

- ▶ **IPv6 - Address:** The static IPv6 Address of the interface (IPv4 with an Address of 192.168.0.4 is configured by default). The field may be left blank if IPv6 operation on the interface is not desired.
- ▶ **IPv6 - Mask Length:** The IPv6 Network mask length in number of bits (also called CIDR notation). Valid values are between 1 and 128 bits for an IPv6 Address. The field may be left blank if IPv6 operation on the interface is not desired.

IP Routes

Delete: Select this option to delete an existing IP route.

Network: The destination IP Network or Host Address of this route. Valid format is standard IPv4 or IPv6 notation. A default route can use the value 0.0.0.0 or IPv6 :: notation.

Mask Length: The destination IP Network or Host Mask in number of bits (also called CIDR notation). Valid values are between 0-32 bits for IPv4 and 0-128 bits for IPv6 routes. Only a default route will have a mask length of 0.

Gateway: The IP Address of the routes Gateway. Valid format is standard IPv4 or IPv6 notation. The Gateway and Network must be in the same Subnet.

Next Hop VLAN (Only for IPv6): The VLAN ID (VID) of the specific IPv6 interface associated with the gateway.

The given VID ranges from 1 to 4094 and will be effective only when the corresponding IPv6 interface is valid. If an IPv6 gateway Address is a link-local Address, you must specify the next hop VLAN for the gateway. If the IPv6 gateway Address is not link-local Address, the Switch will ignore the next hop VLAN.

► **Add Interface:** Click to Add a new IP Interface. A maximum of 8 interfaces are supported.

► **Add Route:** Click to Add a new IP Route. A maximum of 32 routes are supported.

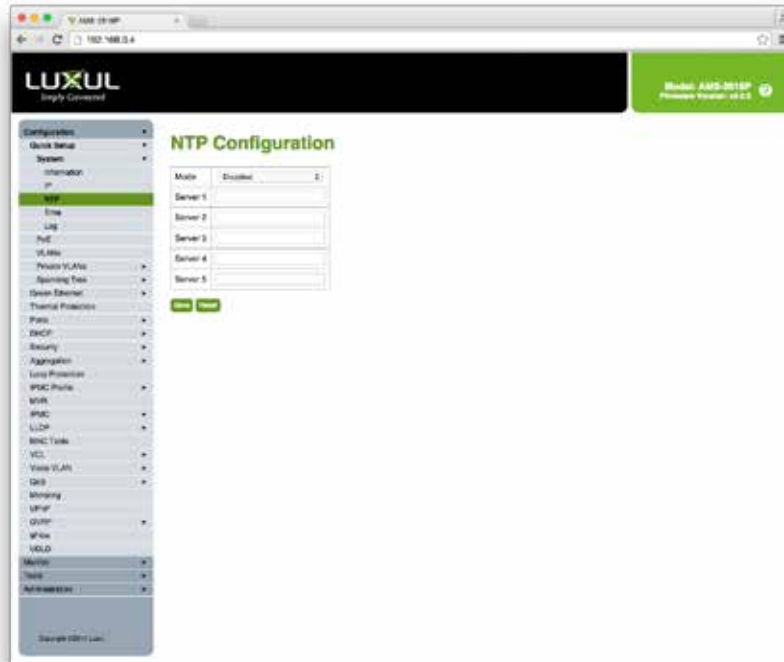
► **Save:** Click to save any unsaved changes.

► **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

NTP

NTP (Network Time Protocol) is used to sync the Network time based on Greenwich Mean Time (GMT). When using the NTP Mode you must manually specify an NTP server(s), the Switch will sync the time after saving the configuration.

To configure NTP settings, select Configuration > Quick Setup > System > NTP from the navigation menu.



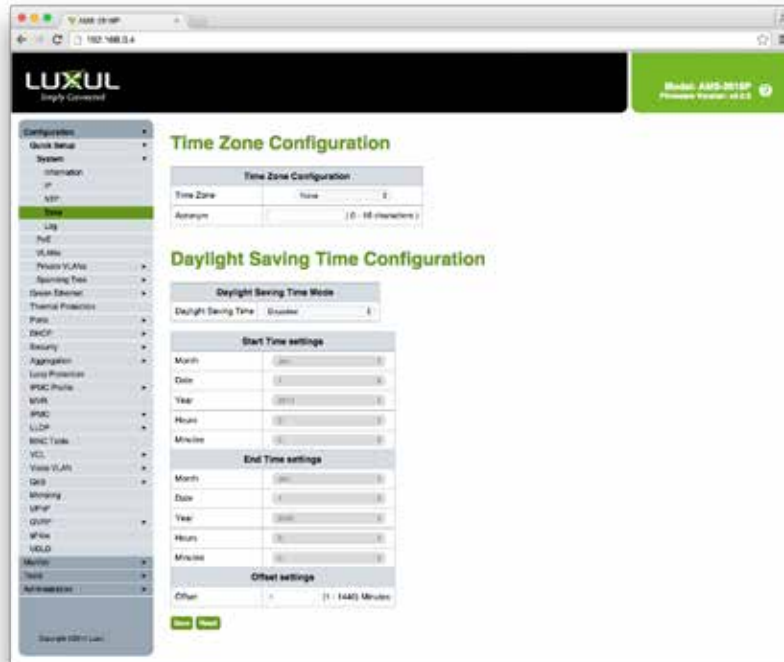
NTP Configuration

- ▶ **Mode Menu:** Indicates whether NTP is Enabled or Disabled.
- ▶ **Server 1 to 5:** Enter the NTP Server DNS, IPv4 or IPv6 Address. For a list of Addresses simply search NTP Servers on any online search engine.
- ▶ **Save:** Click to save any unsaved changes.
- ▶ **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

Time

The Switch provides Automatic options to set the System Time and apply Daylight Savings Time options.

To configure Time Zone and Daylight Savings Time settings, select Configuration > Quick Setup > System > Time from the navigation menu.



Time Configuration

Time Zone Configuration

- ▶ **Time Zone:** Lists various worldwide Time Zones, select the appropriate Time Zone from the drop down.
- ▶ **Acronym:** You can set the acronym of the time zone. This is a User configurable acronym to help identify the time zone selected. (Range: Up to 16 characters, no spaces or special characters)

Daylight Saving Time Configuration

- ▶ **Daylight Saving Time Mode:** Set DST to Recurring or Non-Recurring to use Daylight Savings in conjunction with your NTP Server Settings.

Start Time Settings

- ▶ **Month:** Select the starting Month for DST.
- ▶ **Date:** Select the starting Date for DST.
- ▶ **Year:** Select the starting Year for DST.
- ▶ **Hours:** Select the starting Hour for DST.
- ▶ **Minutes:** Select the starting Minute for DST.

End Time Settings

- ▶ **Month:** Select the ending Month for DST.
- ▶ **Date:** Select the ending Date for DST.

- ▶ **Year:** Select the ending Year for DST.
- ▶ **Hours:** Select the ending Hour for DST.
- ▶ **Minutes:** Select the ending Minute for DST.

Offset settings

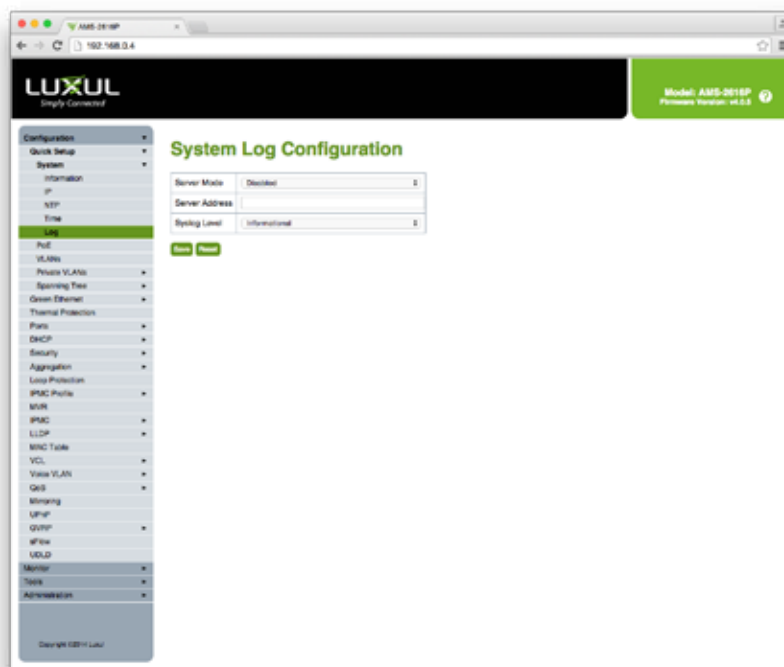
Offset: Enter the number of minutes to add during Daylight Saving Time. (Range: 1 to 1440)

- ▶ **Save:** Click to save any unsaved changes.
- ▶ **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

Log

The Log enables you to configure the Log Server to be used by the Switch for remote storage and management of log files.

To configure the System Log, select Configuration > Quick Setup > System > Log from the navigation menu.



System Log configuration

System Log Configuration

- ▶ **Server Mode:** Allows you to Enable or Disable the Syslog Server configuration.

► **Server Address:** Indicates the IPv4 Address of your Syslog Server. If the Switch has a local DNS Server configured the Server Address can be a Host Name.

Syslog Level: Indicates what level of messages will be sent to your Syslog Server. There are four message levels; information messages (Severity 6 or less), notice messages (Severity 5 or less), warnings (Severity 4 or less) and errors (Severity 6 or less). The possible Modes are:

► **Informational:** Switch will send information messages, notice messages, warnings and errors.

► **Notice:** Switch will send notice messages, warnings and errors only.

► **Warning:** Switch will send warnings and errors only.

► **Error:** Switch will send errors only.

► **Save:** *Click to save any unsaved changes.*

► **Reset:** *Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.*

UNDERSTANDING POE

Power over Ethernet (or PoE) is a system which passes electrical power along with data over Ethernet cabling. This allows a single cable to provide both data connection and electrical power to devices such as wireless access points or IP cameras. This feature can simplify network installation and maintenance by using the switch as a central power source for other network devices.

There are several common techniques for transmitting power over Ethernet cabling, and two have been standardized by IEEE 802.3. Power may be transmitted on the unused conductors of an Ethernet cable, or by applying a common-mode voltage to each pair. The latter is similar to phantom power commonly used for powering balanced microphones.

In addition to standardizing existing practice for spare-pair and common-mode data pair power transmission, the IEEE PoE standards provide for signaling between the power source equipment (PSE) and powered device (PD). This signaling allows the power source to sense and negotiate the amount of power required for a connected device.

Power Budget

One challenge during system design and installation is to consider and calculate the total device power consumption to ensure it is less than the total power budget of the switch. The power supply in the switch - not the number of ports - determines your total power budget.

For instance, the AMS-1208P AV Series Gigabit Managed Switch features a total PoE power budget of 130 Watts. If you were planning an 8-camera surveillance system, and each camera consumed 10W, your total power consumption would be 80W, which is well under the 130W total power budget. However, if each camera consumed 20W, total consumption would exceed the 130W total power budget.

Depending on the devices you intend to connect, you may need a larger switch, not because of the number of ports, but because of the total power budget.

Cable Length

Power over Ethernet (POE) will only power a connected device if there is enough voltage after the cable run. The maximum cable run for PoE devices is approximately 300ft (100m). Beyond this point, voltage will drop and become unstable. If you need to connect PoE devices more than 300ft from a switch, PoE extenders are available for that application.

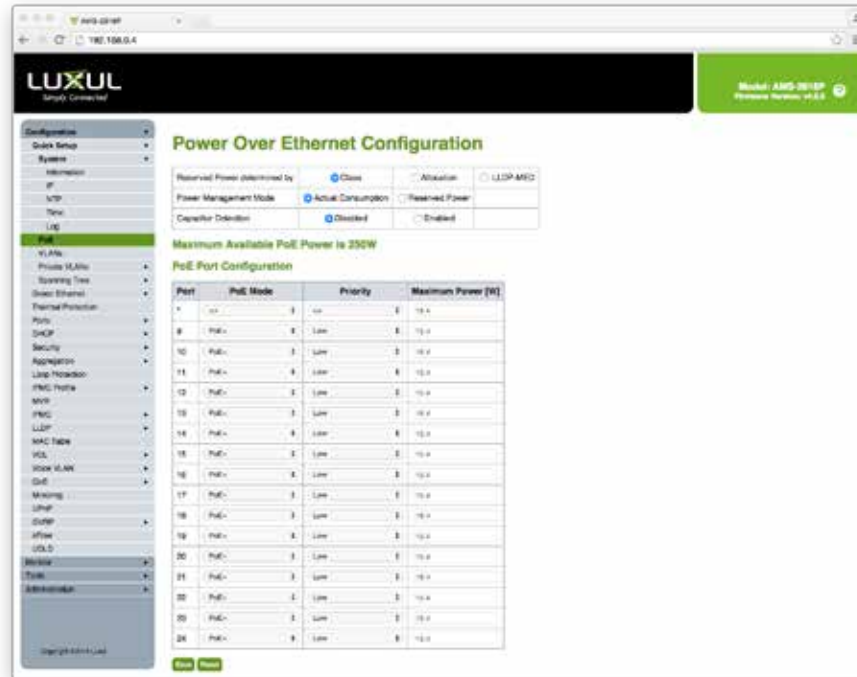
QUICK SETUP: POE

Power Over Ethernet (PoE) is used to transmit electrical power to remote devices over Ethernet. Some examples are IP telephones, wireless access points, IP cameras, or any device where it would be difficult/expensive to connect the equipment directly to AC line power.

Power Over Ethernet Configuration

Allows you to configure the PoE settings of the Switch including the PoE Port settings.

To configure PoE settings, select Configuration > Quick Setup > PoE from the navigation menu.



PoE Configuration

Reserved Power determined by: Allows you to set one of three Modes configuring how the Ports/PDs may reserve power.

- ▶ **Allocated:** You have to allocate the amount of Power that each Port may Reserve. The Allocated/Reserved power for each Port/PD is specified in the Maximum Power field of the PoE Port settings.
- ▶ **Class:** Each Port automatically determines how much Power to Reserve according to the Class of the connected PD. Four different Classes exist 1, 2, 3 and 4 with corresponding wattages of 4 watts, 7 watts, 15.4 watts and 30 watts. In this Mode the Maximum Power field is not used.
- ▶ **LLDP-MED:** This Mode operates similar to the Class Mode expect that each Port determines the amount power it reserves by exchanging PoE information using the LLDP Protocol. If no LLDP Information is available for a Port, the Port will Reserve Power using the Class Mode. In this Mode the Maximum Power field is not used.

✓ **NOTE:** If a Port attempts to use more Power than the Reserved Power of the Port Power to the Port is Shut Down.

Power Management Mode: Allows you to set one of two Modes for configuring when Ports Shut Down.

- ▶ **Actual Consumption:** In this Mode the Ports are Shut Down when the Actual Power Consumption for all Ports exceeds the amount of Power the Power Supply can deliver or if the Actual Power consumption for a given Port exceeds the Reserved Power for that Port. Ports are Shut Down according to the POE Port Priority. If two Ports have the same Priority the Port with the highest Port Number is Shut Down first.
- ▶ **Reserved Power:** In this Mode the Ports are Shut Down when the Total Reserved Power exceeds the amount of Power the Power Supply can deliver. In this Mode POE is not turned on if the PD requests more power than is available from the Power Supply.

Capacitor Detection: Allows you to Enable/Disable Capacitor Detection for use with Legacy POE Devices.

PoE Port Configuration

Port: Displays the Port Number that corresponds to the PoE Configuration Row. Ports that are not capable of PoE are not displayed.

PoE Mode: Allows you to set the PoE Mode of the Port.

- ▶ **Disabled:** PoE Disabled on this Port.
- ▶ **PoE:** Enables 802.3af PoE (Class 4 PDs limited to 15.4W)
- ▶ **PoE+:** Enables 802.3at PoE+ (Class 4 PDs limited to 30W)

Priority: Allows you to set the Priority of the Port.

- ▶ **Low:** Low Priority PDs should be set to Low. This is the default setting
- ▶ **High:** Middle Priority PDs that are more important than Low Priority devices but not Critical should be set to High.
- ▶ **Critical:** Critical Priority is used where the PD is Critical to the local Network.

NOTE: *The Port with the Lowest Priority will be turned off starting from the Port with the highest Port Number.*

Maximum Power: Allows you to specify the Maximum Power value of the Port used in conjunction with the Allocation Reserved Power setting. The maximum allowed 30 watts.

- ▶ **Save:** *Click to Save changes.*
- ▶ **Reset:** *Click to undo any changes made and revert to previously saved values (once Save is clicked this is no longer a valid option).*

UNDERSTANDING VLANS

A virtual local area network, virtual LAN or VLAN, is a group of hosts with a common set of requirements, which communicate as if they were attached to the same broadcast domain, regardless of their physical location.

In a VLAN, a single network is partitioned to create multiple distinct broadcast domains which are mutually isolated so that packets can only pass between them via one or more routers. A VLAN has the same attributes as a physical local area network (LAN), but allows for devices to be grouped together - even if they aren't on the same physical network switch.

In essence, VLANs build virtual fences between devices and data flows which may or may not have gates.

Uses

VLANs address issues such as scalability, security, and network management. Routers or switches in VLAN configurations provide broadcast filtering, security, address summarization, and traffic-flow management.

VLANs can also help create multiple layer 3 networks on a single physical infrastructure. For example, if a DHCP server is plugged into a switch, it will serve any host on that switch that is configured for DHCP. By using VLANs, the network can be easily split up so some hosts will not use that DHCP server and will obtain link-local addresses, or obtain an address from a different DHCP server.

Here are a few of the most common reasons you may want to consider using a VLAN in your installations:

Increased Security

Isolating certain devices on a VLAN can enhance security of the network and the devices on the network.

One of the most common applications of a VLAN are guest networks. In a guest network VLAN, clients can access the Internet and certain local devices, but have no access to other private LAN devices such as servers. In a VLAN-based guest network, specific access point SSIDs and any clients connected to them are isolated to a specific VLAN. That VLAN is then typically able to access the Internet, but nothing else on the LAN.

Security cameras or credit card processing equipment are examples of other devices that can be isolated on a VLAN for security or PCI compliance. VLANs can also be used to contain network attacks or other problems to a specific VLAN, thereby enhancing security for the overall network.

Reduced Network Congestion

Isolating devices on their own VLAN can also reduce congestion and increase network performance. A few examples of systems or devices that could be on a separate VLAN would be VoIP phone systems, streaming media, and security cameras.

Application Specific

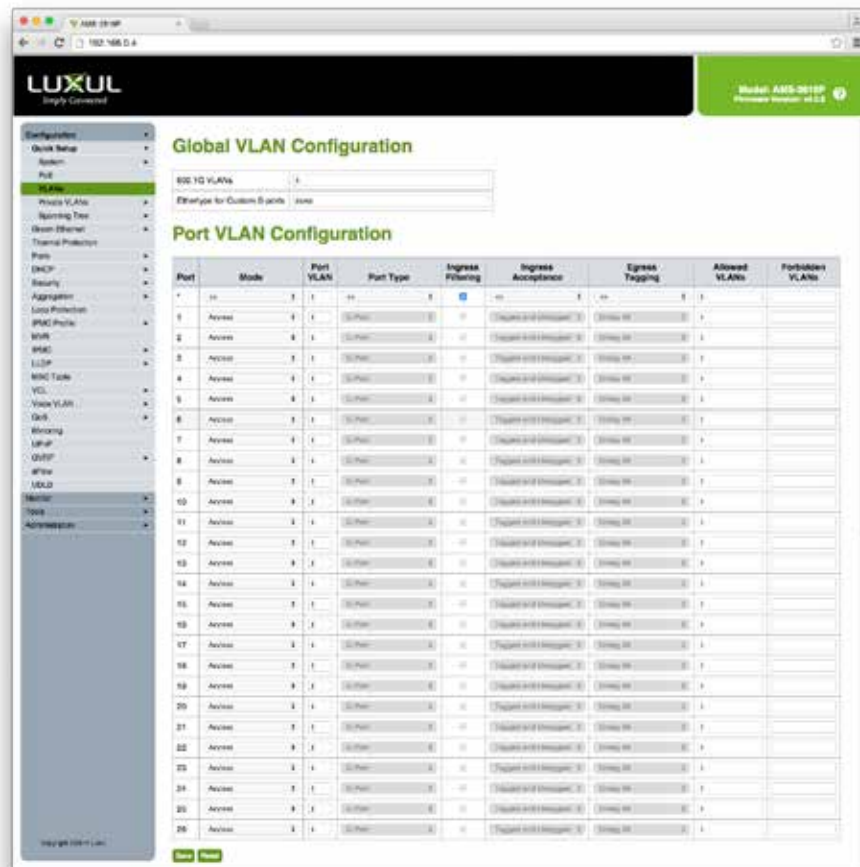
Another common application for VLANs is in HDMI over IP solutions such as that offered by Just Add Power. In the Just Add Power system, VLANs are used to route video signals from transmitters to receivers. In that scenario, VLANs also simultaneously reduces network congestion and enhance reliability and usability of control systems operating on the same physical network.

✔ **NOTE:** To learn about VLANs in depth and learn how to use them to create isolated virtual networks or guest networks, visit luxul.com/educational-webinars and click on the video titled *Course 5: VLANs & Guest Networks*.

QUICK SETUP: VLANS

Virtual Local Area Networks (VLANs) allow you to break a single Physical Switch into two or more Logical Switches. VLANs can be used to secure the local network, control broadcast packets on the local network, and resolve latency issues with latency-sensitive systems like VoIP.

To configure VLAN settings, select Configuration > Quick Setup > VLANs from the navigation menu.



VLAN Configuration

Global VLAN Configuration

802.1Q VLANs: Allows you to create your 802.1Q VLANs and define what VLANs Access Mode Ports have the ability to connect to. Trunk or Hybrid Port Modes will still require the VLAN to be Created using Allowed Access VLANs. By default only VLAN 1 exists. More VLANs may be created by Adding a list using syntax where the individual VLANs are separated by commas. Ranges can be specified with a dash. The following example would create VLANs 1, 10, 11, 12, 13, 200, and 300:

```
1, 10-13, 200, 300
```

Spaces are not allowed between the delimiters.

Ethertype for Custom S-Ports: Allows you to specify the EtherType/TPID used for Custom S-Ports. The setting is only used for Ports whose Port Type is set to S-Custom-Port. For a list of EtherTypes please visit: <http://standards.ieee.org/develop/regauth/ethertype/eth.txt>

Port VLAN Configuration

Port: Displays the Port Number that corresponds to the VLAN Configuration Row.

Mode Column Menu

Allows you to set the Port Mode which determines the behavior of the Port.

Access: Access Ports are typically used to connect to Client Devices (i.e. PC, Laptop, IP Phone, etc...).

- ▶ Can only be a Member of one VLAN, default is VLAN 1.
- ▶ Will Accept Untagged Packets and C-Tagged Packets,
- ▶ Discards all Packets that are not Tagged to the Access VLAN.
- ▶ On Egress all Packets are Transmitted Untagged.

Trunk: Trunk Ports can carry traffic from multiple VLANs simultaneously and are typically used to connect to other Switches or VLAN capable Routers.

- ▶ By default a Trunk Port is Member of all existing VLANs. This can be limited using the Allowed VLANs option.
- ▶ By default all Packets except Packets classified as the Port VLAN are Tagged on Egress. Packets classified as the Port VLAN will not be Tagged on Egress.
- ▶ Egress Tagging can be changed to Tag all Packets in this configuration only Tagged Packets are Accepted on Ingress.

Hybrid: Hybrid Ports are similar to Trunk Ports in many ways but Add Additional Port configuration features. In Addition to the characteristics described for Trunk Ports Hybrid Ports support these additional functions:

- ▶ Can be configured to be VLAN Tag Unaware or, C-Tag Aware, S-Tag Aware, or S-custom-Tag Aware
- ▶ Ingress filtering can be configured.

Ingress Acceptance of Packets and configuration of Egress Tagging can be configured independently.

Port VLAN

Allows you to set the Ports default VLAN ID (PVID). Allowed VLANs Range from 1-4095 with a default of VLAN 1. Ingress Packets are classified as the Port VLAN if the Port is configured as VLAN Unaware, the Frame is Untagged or VLAN Awareness is Enabled on the Port but the Frame is Priority Tagged (VLAN ID = 0). Egress Packets classified as the Port VLAN will not be Tagged if Egress Tagging is set to UnTag Port VLAN. Port VLAN is the Access VLAN for Ports in Access Mode and Native VLAN for Ports in Trunk or Hybrid Mode.

Port Type

Ports in Hybrid Mode allow you to change the Port Type which affects whether a Packets VLAN Tag is used to Classify the Frame on Ingress to a particular VLAN. On Egress the Port Type determines the TPID of the Tag if a Tagging is required.

- ▶ **Unaware:** On Ingress all Packets VLAN Tagged or not are set as the Port VLAN and Tags are not removed on Egress.
- ▶ **C-Port:** On Ingress Packets with a VLAN Tag with TPID = 0x8100 are set to the VLAN ID embedded in the Tag. If a Frame is Untagged or Priority Tagged the Frame will be Tagged to the Port VLAN. If Packets are Tagged on Egress they will be Tagged with a C-Tag.
- ▶ **S-Port:** On Ingress Packets with a VLAN Tag with TPID = 0x8100 or 0x88A8 are set to the VLAN ID embedded in the Tag. If a Frame is Untagged or Priority Tagged the Frame will be Tagged to the Port VLAN. If Packets are Tagged on Egress they will be Tagged with a S-Tag.

- ▶ **S-Custom-Port:** On Ingress Packets with a VLAN Tag with a TPID = 0x8100 or equal to the Ethertype configured for Custom-S Ports are set to the VLAN ID embedded in the Tag. If a Frame is Untagged or Priority Tagged the Frame will be Tagged to the Port VLAN. If Packets are Tagged on Egress they will be Tagged with a S-Tag.

Ingress Filtering

Hybrid Ports allow you to change Ingress Filtering. Access and Trunk Ports always have Ingress Filtering Enabled. If Ingress Filtering is Enabled Packets Tagged to a VLAN the Port is not a Member of are Discarded. If Ingress Filtering is Disabled Packets Tagged to a VLAN the Port is not a Member of are Accepted and Forwarded. However the Port will not Transmit Packets Tagged to a VLAN it is not a Member of.

Ingress Acceptance

Hybrid Ports allow you to change the type of Packets that are Accepted on Ingress.

- ▶ **Tagged and Untagged:** Both Tagged and Untagged Packets are Accepted.
- ▶ **Tagged Only:** Only Tagged Packets are Accepted on Ingress. Untagged Packets are Discarded.
- ▶ **Untagged Only:** Only Untagged Packets are Accepted on Ingress. Tagged Packets are Discarded.

Egress Tagging

Ports in Trunk and Hybrid Mode can control the Tagging of Packets on Egress.

- ▶ **UnTag Port VLAN:** Packets classified within the Port VLAN are Transmitted Untagged. Other Packets are Transmitted with the relevant Tag.
- ▶ **Tag All:** All Packets whether classified to the Port VLAN or not are Transmitted with a Tag.
- ▶ **UnTag All:** All Packets whether classified to the Port VLAN or not are Transmitted without a Tag (This option is only available for Ports in Hybrid Mode).

Allowed VLANs

With Ports in Trunk and Hybrid Mode you can control which VLANs they are allowed to become Members of. Access Ports can only be Member of one VLAN the Port VLAN. The fields syntax is identical to the syntax used in the Allowed Access VLANs field. By default a Port may be a Member of all possible VLANs and is set to 1-4095. Allowed VLANs may be left blank, the Port will not be Member of any of the Existing VLANs. However, if it is configured for VLAN Trunking it will be able to carry all unknown VLANs.

Forbidden VLANs

A Port may be configured to never be allowed to become a Member of one or more VLANs. This is useful when dynamic VLAN Protocols MVRP and/or GVRP must be prevented from dynamically Adding Ports into unintended VLANs. The syntax is identical to the syntax used in the Allowed Access VLANs field. By default this field is left blank allowing the Port may become a Member of all existing VLANs.

- ▶ **Save:** Click to save any unsaved changes.
- ▶ **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

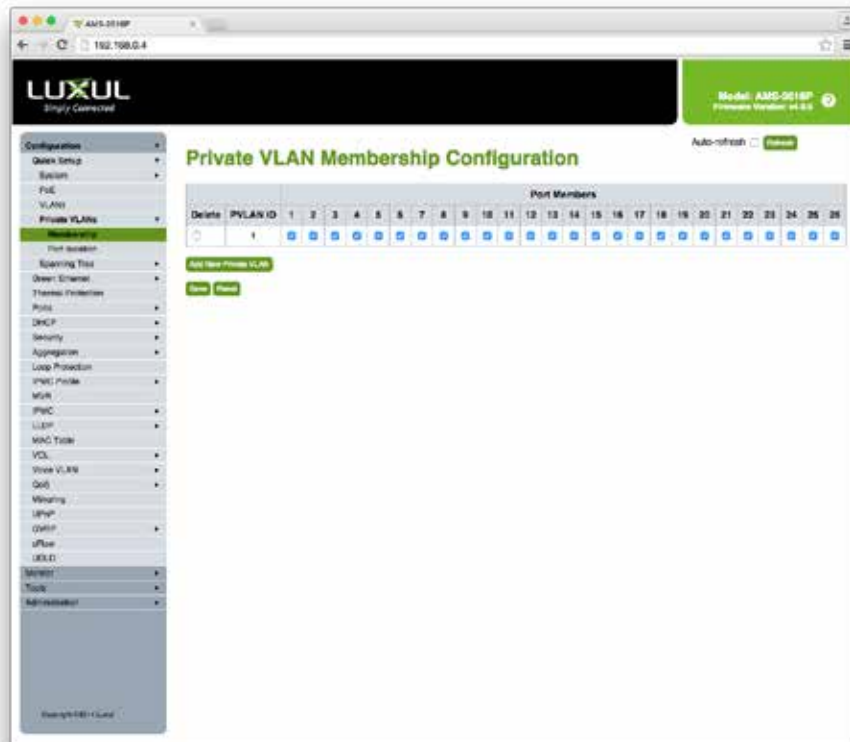
QUICK SETUP: PRIVATE VLANS

Communication between Ports in a Private VLAN is allowed, any Ports that are not a Member of a Private VLAN will not be allowed to pass data in that VLAN.

VLAN Membership

Allows you to define the Private VLAN Membership configuration up to 4095 VLANs are supported. This page also allows you to add and delete Port Members of each VLAN.

To configure VLAN Membership settings, select Configuration > Private VLANs > Membership from the navigation menu.



VLAN Membership Configuration

Delete: To delete a Private VLAN Membership entry, check this box. The entry will be deleted during the next Save.

PVLAN ID: Displays and allows you to set the ID of this Private VLAN. This ID corresponds to the Allowed Access VLANs configured under Configuration>VLANs

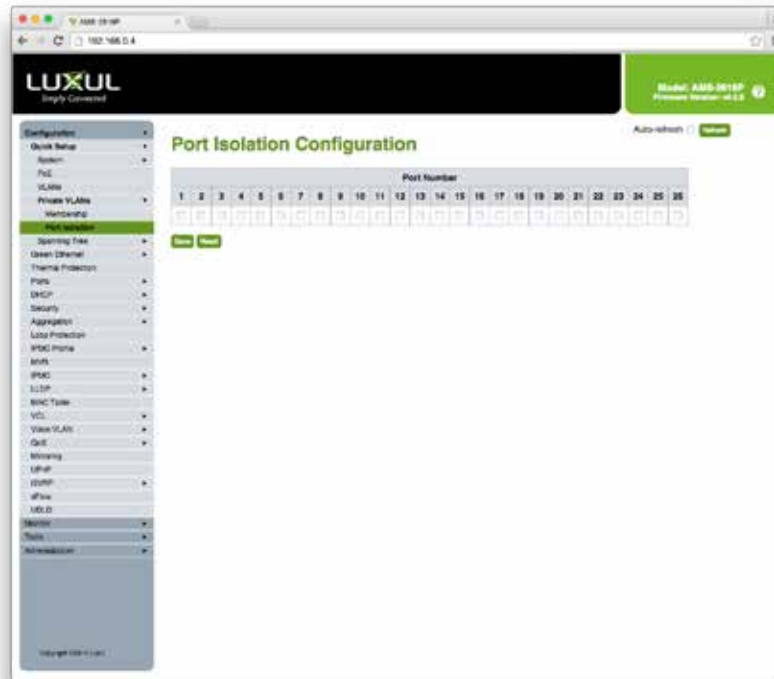
Port Members: Allows you to select the Ports to include in the Private VLAN. To Include a Port in the Private VLAN check the corresponding box. To Remove or Exclude the Port from the VLAN make sure the box is unchecked. By default PVLAN ID 1 is created with all Ports selected as Members.

- ▶ **Refresh:** Click to Refresh the Private VLAN Membership Configuration page.
- ▶ **Add New Private VLAN:** Click to Add New Private VLAN Entry.
- ▶ **Save:** Click to save any unsaved changes.
- ▶ **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

VLAN Port Isolation

This page is used for Enabling or Disabling Port isolation on Ports in a VLAN. A Port Member of a VLAN can be isolated to other isolated Ports on the same VLAN.

To configure VLAN Port Isolation, select Configuration > Private VLANs > Port Isolation from the navigation menu.



VLAN Port Isolation Configuration

Port Number: Allows you to place the Port in Isolation or remove the port from Isolation. When checked Port Isolation is Enabled on the Port, when unchecked Port Isolation is Disabled on that Port. By default Port Isolation is Disabled on all Ports.

- ▶ **Refresh:** Click to refresh the Port Isolation Configuration page.
- ▶ **Save:** Click to save any unsaved changes.
- ▶ **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

UNDERSTANDING SPANNING TREE

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the resulting broadcast radiation. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

As the name suggests, Spanning Tree creates a tree within a network of connected Ethernet switches, and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes.

Eliminating Loops

If your switches are connected in a loop without STP, each switch would infinitely duplicate the first broadcast packet it received because there's nothing to prevent a loop.

STP prevents loops by blocking one or more of the links. If one of the links in use goes down, then it would fail over to a previously-blocked link. How spanning tree chooses which link to use depends entirely on the topology that it can see.

The idea behind a spanning tree topology is that bridges can discover a subset of the topology that is loop-free: that's the tree. STP also makes certain there is enough connectivity to reach every portion of the network by spanning the entire LAN.

Spanning Tree Configuration

Bridges will perform the spanning tree algorithm when they are first connected to the network or whenever there is a topology change.

When a bridge hears a "configuration message," it will begin its disruptive spanning tree algorithm. This starts with the election of a "root bridge" through which all data will flow.

Next, each bridge determines the shortest path to the root bridge so that it knows how to get to the "center." A second election happens on each LAN, and it elects the designated bridge, or the bridge that's closest to the root bridge. The designated bridge will forward packets from the LAN toward the root bridge.

The final step for an individual bridge is to select a root port. This simply means "the port that I use to send data towards the root bridge."

✔ **NOTE:** *Every single port on a bridge (even those connected to endpoints) will participate in the spanning tree unless a port is configured as "ignore."*

A newly-connected bridge will send a reconfiguration message, and other connected devices will comply. All traffic is stopped for 30-50 seconds while the spanning tree is calculated.

Spanning Tree Drawbacks

One drawback of STP is that even though there may be many physical or equal-cost multiple paths through your network from one node to another, all your traffic will flow along a single path defined by a spanning tree. The benefit of this is that traffic loops are avoided, but the cost of restricting traffic to a unique path means blocking alternative, and sometimes more direct, paths. That means that your full potential network capacity can never be realized.

QUICK SETUP: SPANNING TREE

Spanning Tree Protocol (STP) is used to Detect and Disable Network loops but also provide Backup links between Switches. This allows the Switch to interact with other bridging devices (an STP-compliant Switch, bridge or router) in your Network to ensure that only one route exists between any two stations on the Network and provide Backup links which automatically take over when a primary link goes down.

Bridge Settings

Allows you to configure the Spanning Tree Bridge and STP System settings.

To configure STP Bridge settings, select Configuration > Spanning Tree > Bridge Settings from the navigation menu.



STP Bridge Configuration

Basic Settings

Protocol Version: Allows you to set the STP Protocol version used by the Switch.

- ▶ **STP:** Switch will run v1 Spanning Tree.
- ▶ **RSTP:** Switch will run Rapid Spanning Tree (backwards compatible with STP v1).
- ▶ **MSTP:** Switch will run Multiple Spanning Tree (backwards compatible with STP v1 and RSTP)

Bridge Priority: Allows you to set the Bridge Priority. Priority values are Descending (i.e. 100 has a higher priority than 1000). The Bridge Priority plus the MSTI Instance concatenated with the 6-byte MAC Address of the Switch forms the Bridge Identifier. In MSTP this is the priority of the CIST. We do not recommend changing this value without consulting a knowledgeable Network Administrator.

Forward Delay: Allows you to set the delay used when Transmitting Root and Designated Ports BPDU. The valid range is 4-30 seconds with a default of 15 seconds. We do not recommend changing this value without consulting a knowledgeable Network Administrator.

Max Age: Allows you to set the Maximum Age of the BPDU Transmitted by the Root Bridge. The valid Range is 6-40 seconds with the default of 20 seconds (MaxAge must be $\leq (\text{FwdDelay}-1)*2$). We do not recommend changing this value without consulting a knowledgeable Network Administrator.

Maximum Hop Count: Allows you to set the number of Remaining Hops for STP BPDUs generated at the boundary of an MSTP region. The valid range is 6-40 hops. We do not recommend changing this value without consulting a knowledgeable Network Administrator.

Transmit Hold Count: Allows you to set the number of BPDUs a Bridge Port can send per second. When per second limit is exceeded the transmission of the next BPDU will be delayed. The valid Range is 1-10 BPDUs per second. We do not recommend changing this value without consulting a knowledgeable Network Administrator.

Advanced Settings

Edge Port BPDU Filtering: Allows you to set whether a Port explicitly configured as an Edge Port will Transmit and receive BPDUs.

Edge Port BPDU Guard: Allows you to set whether a Port explicitly configured as an Edge Port will Disable itself upon reception of a BPDU. If Enabled he Port will enter the Error-Disabled State and will be removed from the active topology.

Port Error Recovery: Allows you to set whether a Port in the Error-Disabled State can automatically re-enabled itself. If Recovery is not enabled Ports have to be Disabled then Re-enabled for normal STP operation to resume. The condition is also cleared by a system Reboot.

Port Error Recovery Timeout: Allows you to set the Port Error Recovery Timeout. The valid Range is 30-86400 seconds.

► **Save:** Click to save any unsaved changes.

► **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

MSTI Mapping

When you implement Multiple Spanning Tree Protocol on the Switch the CIST is not available for explicit Mapping as it will receive BPDUs from VLANs not explicitly Mapped to the CIST. You must set the list of VLANs Mapped to the MSTI if there is more than one VLAN configured within the CIST. If entering multiple VLANs they can be separated by a comma or space. A VLAN can only be Mapped to one MSTI. Any unused MSTI should be left empty.

To configure MSTI Mapping, select Configuration > Spanning Tree > MSTI Mapping from the navigation menu.



MSTI Configuration

Configuration Identification

Configuration Name: Allows you to set the Name identifying the VLAN to MSTP Instance Mapping. Bridges must share the same Name, Revision and VLAN-to-MSTI Mapping configuration in order to share Spanning Trees within the MSTI Region. The Name must be configured and can have a maximum of 32 characters, the permitted characters are Numbers, Uppercase letters, Lowercase letters and Hyphens.

Configuration Revision: Allows you to set the Revision of the MSTP Instance Named above. The value must be an integer between 0-65535.

MSTI Mapping

MSTI: Displays the MSTI ID that corresponds to the MSTI Mapping row.

VLANs Mapped: Allows you to enter the list of VLANs mapped to the MSTI. VLANs can be given as a single integer between 1-4094 or a Range separated by a hyphen (i.e. 20-40) each of which must be separated with comma or space. A VLAN can only be Mapped to one MSTI. Any unused MSTI should be left empty.

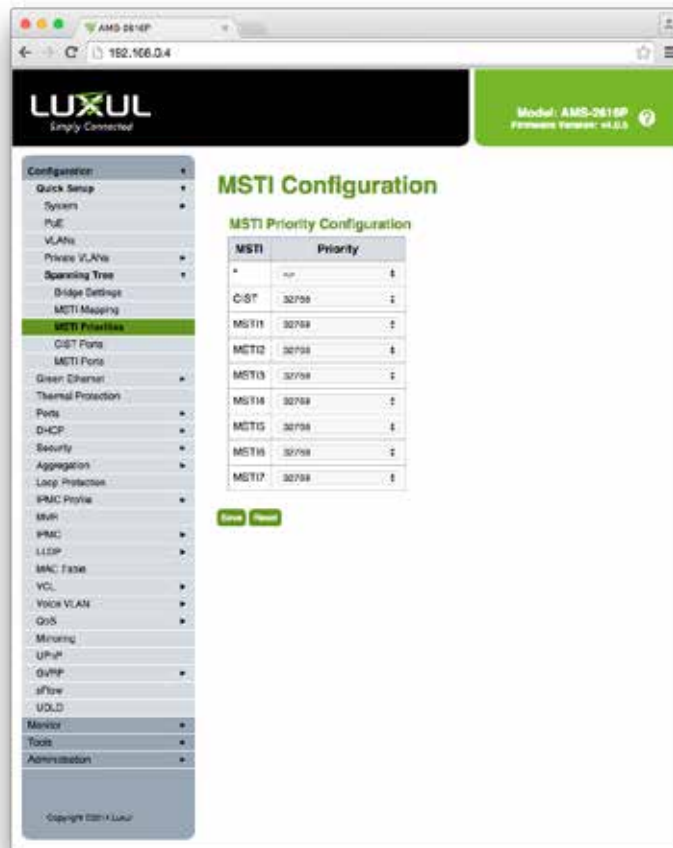
► **Save:** Click to save any unsaved changes.

► **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

MSTI Priorities

When you implement a Spanning Tree Instance on the Switch the CIST is the default Instance which is always active and controls the Bridge Priority. MSTI Priorities allows you to configure the Priority of the MSTI Instances of the Switch. The Priority value is Descending (i.e. 100 has a higher priority than 1000).

To configure MSTI Priorities, select Configuration > Spanning Tree > MSTI Priorities from the navigation menu.



MSTI Configuration

MSTI: Displays the bridge instance, CIST is the default instance and is always active.

Priority: Allows you to set the Bridge Priority per Instance Priority. Value is descending (i.e. 100 has a higher priority than 1000). It is typically recommended to keep the MSTI Instance Priority lower than the CIST Priority.

► **Save:** Click to save any unsaved changes.

► **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

CIST Ports

When you implement a Spanning Tree Instance on the Switch you will need to configure the CIST Port settings for Spanning Tree to be activated.

To configure STP CIST Port settings, select Configuration > Spanning Tree > CIST Ports from the navigation menu.

The screenshot shows the LUXUL network management interface. The main content area is titled "STP CIST Port Configuration". It contains two tables:

- CIST Aggregated Port Configuration:** A single row showing port 1 with STP Enabled (checked), Path Cost (0), Priority (100), Admin Edge (Non-Edge), Auto Edge (checked), Restricted Role (checked), STCN (checked), BPDU Guard (checked), and Port-to-port (checked).
- CIST Normal Port Configuration:** A table with 24 rows, one for each port (1-24). Each row has columns for Port, STP Enabled (checked), Path Cost (0), Priority (100), Admin Edge (Non-Edge), Auto Edge (checked), Restricted Role (checked), STCN (checked), BPDU Guard (checked), and Port-to-port (checked).

STP CIST Port Configuration

CIST Aggregated Port Configuration and CIST Normal Port Configuration

Port: Displays the Port Number that corresponds to the CIST Configuration Row. When using the Aggregated Port Configuration the settings will be applied to All valid Ports.

STP Enabled: Allows you to Enable/Disable STP on the specified Switch Port.


Path Cost: Allows you to set the path cost of the Port. The Auto setting will set the path cost using the Physical Link speed and the 802.1D recommended values. Using the Specific setting you can define a Value. Path Cost is used when establishing the Active Topology of the Network. Lower Path Cost Ports are chosen as forwarding Ports while Higher Path Cost Ports are used as backup links. Valid values range from 1-200000000.

Priority: Allows you to set the Port Priority. This is used to control the Priority of Ports with identical Port Costs. (See Path Cost).

AdminEdge: Allows you to set whether the Port is connected directly to an Edge Device. This allows Transition to the Forwarding State Faster for Edge Ports than non-Edge Ports. The value of this flag is based on the AdminEdge and AutoEdge settings. When set to Edge it is displayed as Edge in Monitor>Spanning Tree>Port Status.

- ▶ **Edge:** The Port has been set as an Edge Port and will Transition to Forwarding state faster.
- ▶ **Non-Edge:** The Port is not set as an Edge Port and will follow normal Transition timing. This is the default value.
- ▶ **AutoEdge:** Allows you to set whether the Switch should attempt Edge Port detection. This allows the AdminEdge state to be derived from whether BPDU's are received on the Port or not.

Restricted Role: Allows you to Restrict the Port so it will not to be selected as Root Port for the CIST or any MSTI, even if it has the best Spanning Tree Priority. The Port will be selected as a Backup after the Root Port has been selected. Restricted Role can be set by the Network Administrator to prevent bridges external to a core region of the Network from influencing the Spanning Tree Active Topology. This feature is also known as Root Guard.

 **Warning:** *This setting can cause lack of Spanning Tree connectivity.*


Restricted TCN: Allows you to Restrict the Port so it will not Propagate Received Topology Change Notifications and Topology Changes to other Ports. Restricted TCN can be set by the Network Administrator to prevent bridges external to a core region of the Network from causing Address flushing within that region. An example of use would be when the Physical Link State of an attached LAN(s) Transitions frequently.

 **NOTE:** *This setting can cause temporary loss of connectivity after changes to a Spanning Tree Active Topology as a result of incorrect learned station location information.*

BPDU Guard: Allows you to set the Port to Disable itself upon receiving valid BPDU's. Port Edge status will not affect this setting. A Port that has entered error-Disabled State due to this setting is subject to the bridge Port Error Recovery setting as well.

Point to Point: Allows you to set whether the Port connects to a Point-to-Point LAN rather than to a Shared Medium.

- ▶ **Auto:** Point-to-Point status is Automatically detected. This is the default setting.
- ▶ **Forced True:** Allows you to Force the Switch into the Point-to-Point configuration.
- ▶ **Forced False:** Allows you to Force the Switch to Disable the Point-to-Point configuration.

 **NOTE:** *Transition to the Forwarding State is faster for Point-to-Point LANs than for Shared Media.*

▶ **Save:** *Click to save any unsaved changes.*

▶ **Reset:** *Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.*

MSTI Ports

When you implement a Multiple Spanning Tree Instance on the Switch you will need to configure the MSTI Port settings for Spanning Tree to be activated.

To configure MSTI Ports, select Configuration > Spanning Tree > MSTI Ports from the navigation menu.

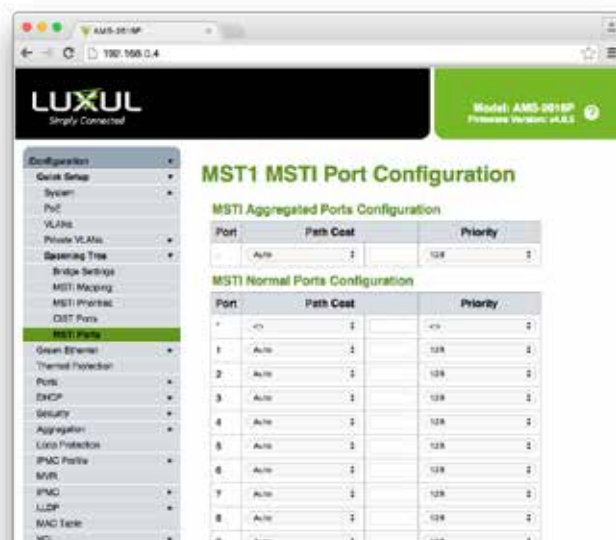


MSTI Port Configuration (Select MSTI)

MST# Drop-down: Allows you to select the MSTI you would like to configure.

MST#: Select the desired MSTI to configure.

► **Get:** Open the selected MSTI for configuration.



MSTI Port Configuration

Port: Displays the Port Number that corresponds to the MSTI Configuration Row.

Path Cost: Allows you to set the path cost of the Port. The Auto setting will set the path cost using the Physical Link speed and the 802.1D recommended values. Using the Specific setting you can define a Value. Path Cost is used when establishing the Active Topology of the Network. Lower Path Cost Ports are chosen as forwarding Ports while Higher Path Cost Ports are used as backup links. Valid values range from 1-200000000.

Priority: Allows you to set the Port Priority. This is used to control the Priority of Ports with identical Port Costs. (See Path Cost).

► **Save:** Click to save any unsaved changes.

► **Reset:** Click to cancel any unsaved changes and revert to previously-saved values. Not available once changes are saved.

