MANAGED SWITCH BASIC FEATURES

CHAPTER 3

In this Chapter...

Managed Switch Features 3-2

Switch Management Settings 3-3

Port Configuration.. 3-4

Change Password 3-5

Redundancy Settings 3-6

Spanning Tree Protocols 3-7

Recovery Time, Hops and Convergence 3-9

RSTP/STP Configuration 3-10

Port Priority 3-15

RSTP Examples 3-16

Multicast Filtering (IGMP).. 3-20

IGMP Protocol Settings 3-21

Static FDB Multicast 3-21

The Benefits of Enabling IGMP 3-22

Port Monitoring 3-23

Browser Access Protocol (HTTPS) 3-24

Virtual LANs (VLANs)... 3-25

PVLAN – Private VLANs 3-27

VLAN with RSTP 3-30

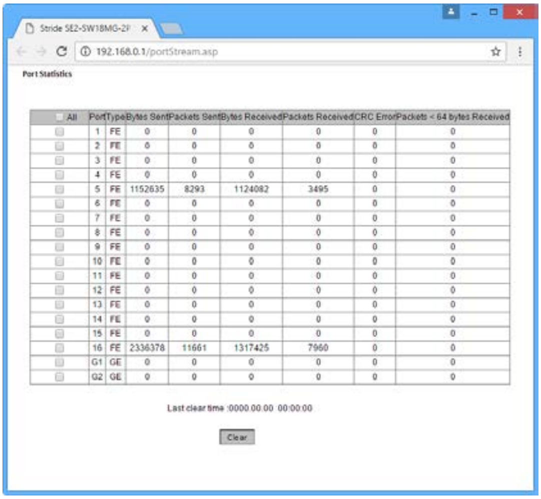
VLAN Examples 3-32

Alarms 3-42

Managed Switch Features

Besides the network settings and the device information described in Chapter 2, the switch has a variety of features that will be valuable for many networks.

NOTE: *All configuration changes except IP address and password must be committed to the switch by performing SAVE. If not committed by SAVE, changes will be lost on power cycle. Likewise, changes made by performing RESET DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.*



Port Statistics

□ All	Port	Type	Bytes Sent	Packets Sent	Bytes Received	Packets Received	CRC Error	Packets < 64 bytes Received
□	1	FE	0	0	0	0	0	0
□	2	FE	0	0	0	0	0	0
□	3	FE	0	0	0	0	0	0
□	4	FE	0	0	0	0	0	0
□	5	FE	1152635	8293	1124082	3495	0	0
□	6	FE	0	0	0	0	0	0
□	7	FE	0	0	0	0	0	0
□	8	FE	0	0	0	0	0	0
□	9	FE	0	0	0	0	0	0
□	10	FE	0	0	0	0	0	0
□	11	FE	0	0	0	0	0	0
□	12	FE	0	0	0	0	0	0
□	13	FE	0	0	0	0	0	0
□	14	FE	0	0	0	0	0	0
□	15	FE	0	0	0	0	0	0
□	16	FE	2336378	11661	1317425	7960	0	0
□	G1	GE	0	0	0	0	0	0
□	G2	GE	0	0	0	0	0	0

Last clear time :0000.00.00 00:00:00

The port statistics page provides information that may be useful to troubleshoot or tune your network.

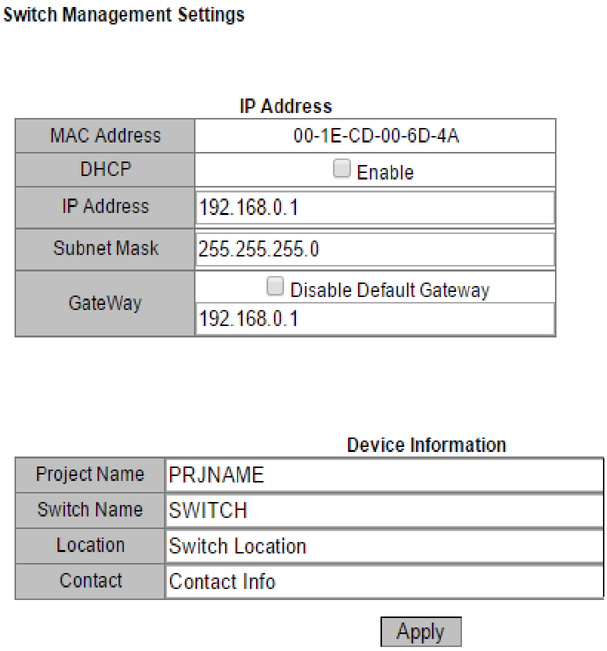
The Port Statistics table identifies each port and port type:

- FE – Fast Ethernet – RJ45 connection
- FX – 100Base Fx Fiber connection – ST or SC connection depending on model
- GE – Gigabit Ethernet – RJ45 connection available on some models
- GX – SFP - Optional SFP transceivers may be purchased separately and installed in some models.

Bytes and packets sent or received show how busy and efficient your network is.

CRC errors and packets smaller than 64 bytes are symptoms of a problem on a port; start troubleshooting by checking the integrity of the physical connections on that port. Also check for a malfunctioning network card or software issues. The port may have been unintentionally configured for half duplex rather than full duplex and these errors may point to traffic collisions.

Switch Management Settings



Switch Management Settings

IP Address

MAC Address	00-1E-CD-00-6D-4A
DHCP	☐ Enable
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
GateWay	☐ Disable Default Gateway 192.168.0.1

Device Information

Project Name	PRJNAME
Switch Name	SWITCH
Location	Switch Location
Contact	Contact Info

To control and monitor the switch via the network, it must be configured with basic network settings, including an IP address and subnet mask. Refer to Chapter 2 to learn how to initially access your switch.

DHCP Enabled/Disabled: The switch can automatically obtain an IP address from a DHCP server using the Dynamic Host Configuration Protocol (DHCP). This can speed up initial set up, as the network administrator does not have to find an open IP address.

***NOTE:** If DHCP has been enabled, it will be necessary to connect to the console port to ascertain which IP address has been assigned so that you may be able to access the switch using the web browser.*

Gateway: The Gateway address is the address of a router that connects two different networks.If you prefer to have no address configured for the Gateway, check “Disable Default Gateway”. A Gateway is required to access switch management from a device that is not on the same subnet as the switch management IP address.

Port Configuration

The switch default port settings allow you to connect to the Ethernet Ports without any configuration. Should there be a need to change the negotiation settings or flow control settings, you can do this on the Port Configuration page.

Jumbo Frames – Jumbo Frames (1632 bytes) are always enabled on SE2-SW16M and SE2-SW18MG-2P and these switches do not have a Jumbo Frame enable option. On SE2-SW8M(-x) models, the user can enable or disable Jumbo Frames on this page. Enabling Jumbo Frames allows the switch to support 1632 byte frames. When Jumbo Frames are disabled, the switch supports up to 1522 byte frames.

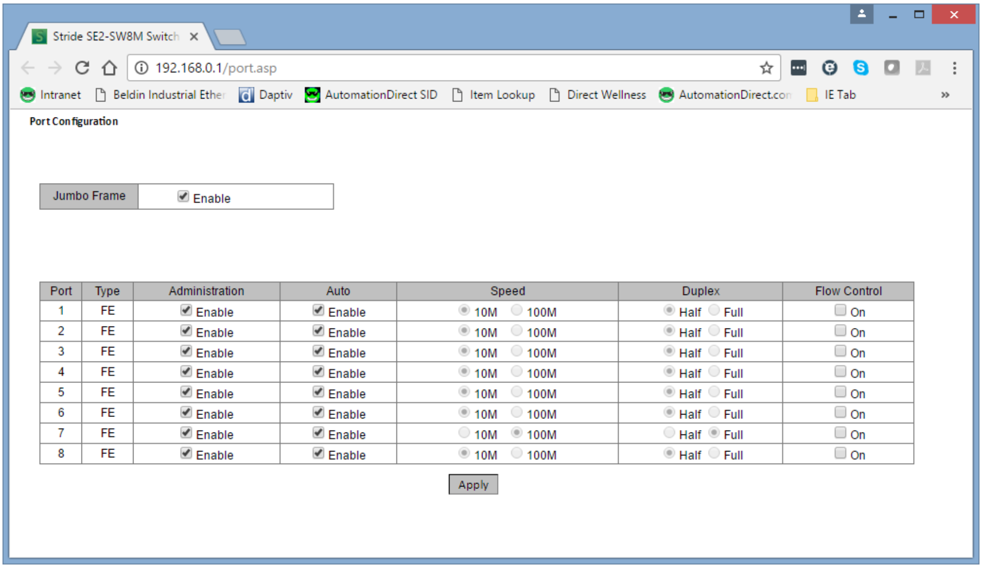
Administration – Also, to provide a level of network security, you may choose to restrict access to the switch by administratively disabling unused ports. Ports that are disabled are virtually non-existent (not visible for switch operation or spanning tree algorithm).

Auto – Auto Negotiation: All copper ports (FE and GE) are capable of auto-negotiation such that the fastest bandwidth is selected. Choose to enable auto negotiation or use fixed settings. Network performance can be optimized by disabling auto-negotiation and configuring Speed and Duplex if network traffic is known.

100Mbps fiber ports are fixed speed only.

NOTE: *The SFP settings are NOT automatically sensed or negotiated. If a 100 Mbps SFP is installed in the switch, that port must be manually set on the port configuration page to 100 Mbps.*

Flow Control: Flow control can also be enabled or disabled. Flow control ensures that the receiving devices takes in all the data without error. If the transmitting device sends at a faster rate than the receiving device can manage, then the receiving device will eventually fill its buffer. No further information can be taken when the buffer is full, so a flow control signal is sent to the transmitting device to temporarily stop the flow of incoming data.



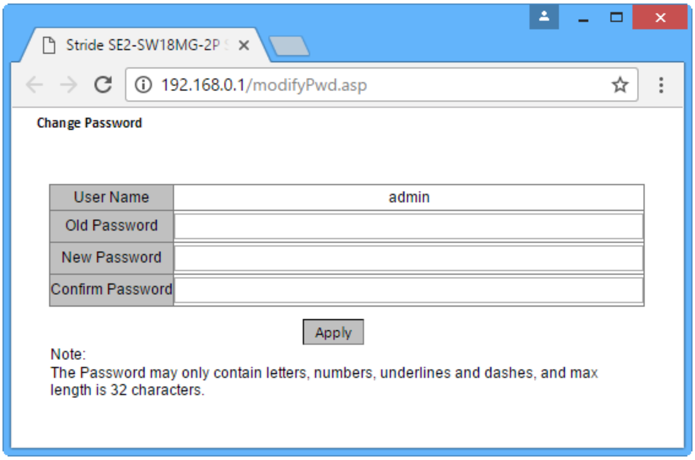
Port Configuration

Jumbo Frame	☑ Enable

Port	Type	Administration	Auto	Speed	Duplex	Flow Control
1	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On
2	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On
3	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On
4	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On
5	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On
6	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On
7	FE	☑ Enable	☑ Enable	○ 10M ● 100M	○ Half ● Full	□ On
8	FE	☑ Enable	☑ Enable	● 10M ○ 100M	● Half ○ Full	□ On

Change Password

The SE2 series switches allow browser management access for user name admin. The default password is admin. To provide an additional level of security, the password may be changed.



Change Password

User Name	admin
Old Password	
New Password	
Confirm Password	

Note:
The Password may only contain letters, numbers, underlines and dashes, and max length is 32 characters.

Redundancy Settings

Another benefit of using managed switches over unmanaged switches is their redundancy capabilities. This allows you to have an Ethernet network with extra connections, so if one path between two points on the network fails, another path can be used to deliver messages. If one link or switch fails, another link or switch can take over transparently to prevent unnecessary down time. So why not just physically connect each of the switches in your network in various loop configurations such that there are always at least two paths going to and from each switch? That would create a broadcast loop that will bring a network to its knees very quickly.

In an unmanaged Ethernet network there can be only one path between any two ports on the network. If there is more than one path from one switch to another, broadcast messages (and in some cases other messages) sent by the network will be forwarded until traffic completes a loop by returning on the second path. Since the switches forward all broadcasts and do not keep track of the messages they have sent, the returning message will be sent around the loop again and again. A single message circulating forever around a loop at high speed is clearly not a good thing, so no loops are allowed.

The limitations of having only one path are even simpler to see. If the one and only path fails for any reason, such as a broken cable or power failure at one of the switches, there are no paths left and no network traffic can get through. We need a way to add alternate paths without creating loops. A redundancy protocol such as RSTP, a loop prevention protocol, is used such that switches can communicate with each other to discover and prevent loops.

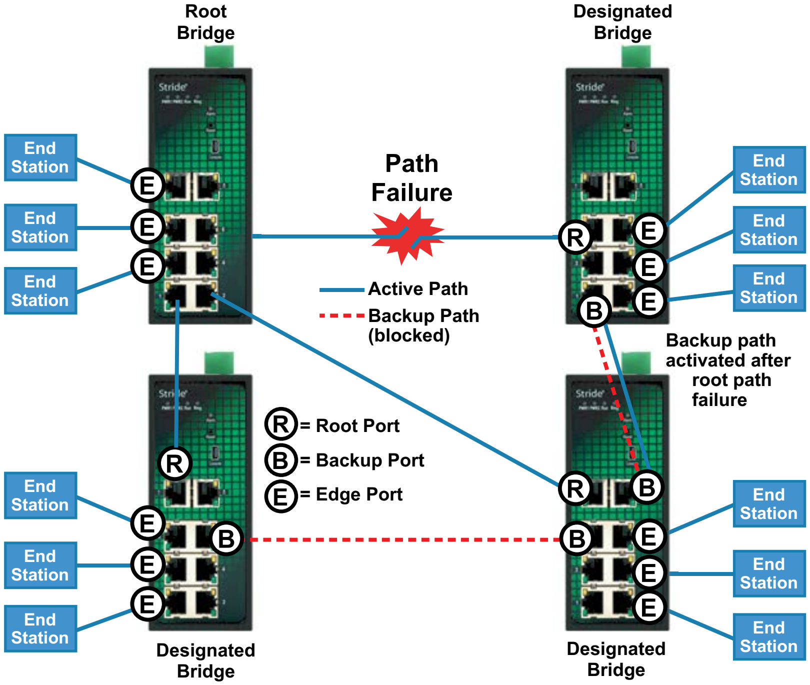
There are four methods of accomplishing redundancy in the **Stride** SE2 series managed switches:

1. Spanning Tree Protocol (STP)
2. Rapid Spanning Tree Protocol (RSTP)
3. AD-Ring
4. AD-RP

The Spanning Tree Protocols (STP and RSTP) are industry standards and are thus compatible with other manufacturer's managed switches for situations where switches from multiple manufacturers need to coexist and communicate. The recovery time, however, is slower with the Spanning Tree Protocols than with the proprietary AD-Ring and AD-RP protocols. Unless network conditions require you to use older STP, or application requirements require you to have a very fast recovery, you will probably use RSTP. Its merits are discussed more on the following pages.

Spanning Tree Protocols

In the diagram below all the links are the same speed, 100 Mbps. The root ports are those connected directly to the root bridge because they have the lowest path cost (only one hop). The paths that must go through another bridge (switch) have a higher path cost (two hops) and are designated as backup ports (decisions made internal to the switch by the Spanning Tree Protocol). For the most efficient network, the ports connected directly to end stations do not have RSTP Enabled so that RSTP doesn't waste time considering them.



The Rapid Spanning Tree Protocol provides a standardized means for intelligent switches (also called bridges) to enable or disable network paths so there are no loops, but there is an alternative path if it is needed. Why is it called Rapid Spanning Tree Protocol?

- **Rapid:** it is faster than the previous (and completely compatible) version called Spanning Tree Protocol (STP).
- **Spanning:** it spans (connects) all of the stations and switches of the network.
- **Tree:** its branches provide only one connection between two points.

In a Spanning Tree network, only one bridge (managed switch) is responsible for forwarding packets between two adjacent LAN segments to ensure that no loops exist in a LAN. To ensure that only one bridge is responsible, all other bridges on the network must cooperate with each other to form a logical spanning tree that defines the pathways that packets should take from bridge to bridge.

The logical spanning tree has exactly one bridge that is assigned the role of root. All of the other bridges need to have exactly one active path to the root. The job of the root bridge is to notify all bridges connected in the tree that there has been a topology change and restructuring of the tree is in progress (due to a communications link failure somewhere in the network or a new switch added in the network). The root bridge is determined by the bridge priority assigned to it and the MAC address.

By default, it is the bridge with the lowest MAC address that gets assigned the role as "root", but a specific bridge can be forced to be the root bridge by changing its bridge priority setting (a lower number with respect to other bridges means higher priority, set on the Spanning Tree Settings page).

Every communication path between each bridge (managed switch) on the network has an associated cost. This "path cost" may be determined by the speed of each segment, because it costs more time to move data at a slower speed, or the path cost can be manually configured to encourage or discourage the use of a particular network. For example, you may not want to use a particular high-speed link except when absolutely necessary because you pay a fee to a service provider for data using that path, while another path is free (no monetary cost).

The path cost is the cumulative cost of all the hops from the root bridge to a particular port on the network. A Spanning Tree network always uses the lower cost path available between a port and the root bridge. When the available network connections change, the network reconfigures itself as necessary.

See the RSTP examples topic in this section for an example of how the path cost can be utilized to establish the primary and backup connections.

During the start-up of a Spanning Tree Network, all bridges (managed switches) are transmitting configuration messages (BPDUs) claiming to be the root. If a switch receives a BPDU that is "better" than the one it is sending, it will immediately stop claiming itself as the root and send the "better" root information instead. Assuming the working network segments actually connect all of the switches, after a certain period of time there will be only one switch that is sending its own root information and this switch is the root. All other switches transmit the root bridge's information at the rate of the root bridge's "hello time" or when the root bridge's BPDU is received on one of their ports.

The factor for determining which switch is the root (has the "best" root information) is the bridge priority and its tie-breaker, the switch MAC address. If a switch has more than one path to get messages from the root, other information in the configuration message determines which path is the best.

Once the root bridge is determined, all other switches see the root bridge's information and path information to the root. If more than one port provides a path to the root the non-root switches must decide which port to use. They check all of their ports to select the port that is receiving messages indicating the best path to the root.

The selected port for each bridge is called the root port. It provides the best path to communicate with the root. The best path is determined first by the lowest total path cost to the root (root path cost). Each port is assigned a cost (usually based on the speed) for messages received on that port. The root path cost for a given path is the sum of the individual port costs for that path. The lowest path cost indicates the shortest, fastest path to the root. If more than one path has the same cost then the port priority assigned to each port and its tie-breaker, the port number, pick the best path.

Recovery Time, Hops and Convergence

The typical RSTP recovery time (time to start forwarding messages on the backup port) on a link-loss failure is <50ms per "hop". A hop is defined as a link between two switches. A link to an end station is not considered a hop.

The Max Age setting controls how long RSTP messages may circulate in the network. Since the largest value allowed for Max Age is 40, the largest RSTP network hop-diameter is also 40.

See the RSTP Examples topic in this section for a more detailed explanation about hops and recovery time.

The time it takes for all of the switches to have a stable configuration and send network traffic is called the convergence time. STP was developed when it was acceptable to have a convergence time of maybe a minute or more, but that is not the case anymore. Due to the increased demand for better convergence times, Rapid Spanning Tree Protocol was developed, bringing the normal convergence time for a properly configured network down to a few seconds. The RSTP takes advantage of the fact that most modern Ethernet links between switches are point-to-point connections. With a point-to-point link, the switches can quickly decide if the link should be active or not.

AD-Ring limits the redundant path to a simple ring. For this reason, the recovery time is much faster than even RSTP.

AD-RP allows one AD-Ring ring to provide redundancy for a second ring.

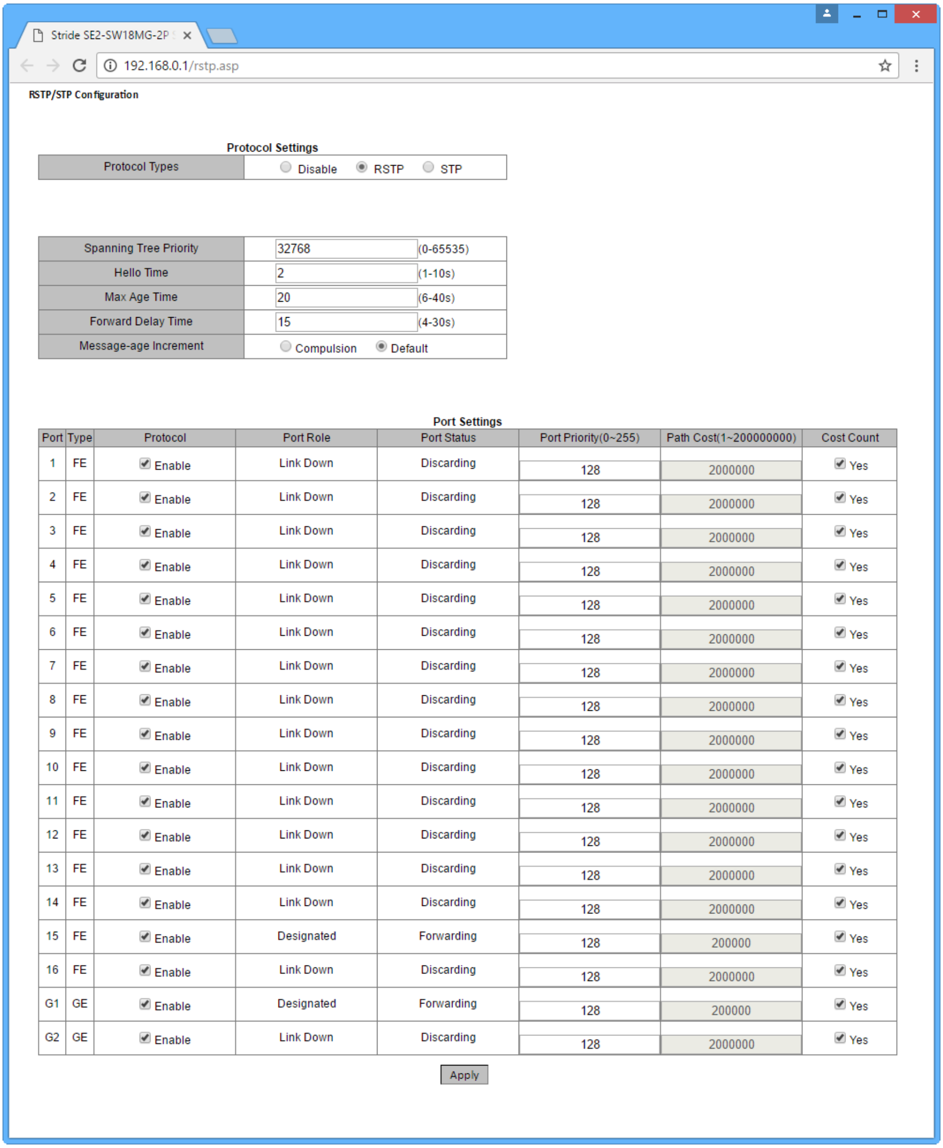
Pairs of ports that are configured for AD-Ring or AD-RP must be Disabled from participating in Spanning Tree.

NOTE: *AD-Ring and AD-RP are proprietary redundancy protocols and will only function properly in a network of all* ***Stride*** *SE2 series switches.*

RSTP/STP Configuration

By default, RSTP is Enabled on all ports.

The Spanning Tree Settings enable you to choose the redundancy protocol and set parameters related to that protocol.



RSTP/STP Configuration

Protocol Settings

Protocol Types	○ Disable ● RSTP ○ STP

Spanning Tree Priority	32768 (0-65535)
Hello Time	2 (1-10s)
Max Age Time	20 (6-40s)
Forward Delay Time	15 (4-30s)
Message-age Increment	○ Compulsion ● Default

Port Settings

Port	Type	Protocol	Port Role	Port Status	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
1	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
2	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
3	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
4	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
5	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
6	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
7	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
8	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
9	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
10	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
11	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
12	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
13	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
14	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
15	FE	☑ Enable	Designated	Forwarding	128	200000	☑ Yes
16	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
G1	GE	☑ Enable	Designated	Forwarding	128	200000	☑ Yes
G2	GE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes

Apply

Protocol Types Choose the protocol by selecting RSTP (Rapid Spanning Tree Protocol) or STP (Spanning Tree Protocol). Selecting “Disable” in the Protocol Settings box will globally disable this advanced feature on this switch. Choosing RSTP or STP will allow the wiring of redundant networks (such as rings) for automatic failover. RSTP is compatible with STP so in most cases you should choose RSTP. RSTP/STP use BPDUs (Bridge Protocol Data Units) to keep bridges informed of the network status.

CAUTION: If VLANS and redundancy (RSTP) are both enabled, situations can arise where the physical network is intact but one or more VLANs are being blocked by the redundancy algorithm and communication over those VLANS fails. The best practice is to make all switch-to-switch connections members of all VLANs to ensure connectivity at all times. Should you intend to use RSTP and VLANs at the same time, please see the “VLAN with RSTP” section in this chapter for important information concerning the setup of your network. Otherwise, communication failures may occur.

Select Disable if you do not require the switch to manage redundant network connections. All ports will forward network traffic just as an unmanaged switch would. Otherwise RSTP should usually be selected. RSTP is compatible with switches that only implement STP, an older version of the protocol. If STP is selected only the original STP format messages will be generated. Selecting STP reduces the chances of network packets being duplicated or delivered out of order, but at the expense of much longer reconfiguration time.

Spanning Tree Priority (0 to 65535; Default = 32768): The spanning tree priority (bridge priority) is used to determine the root bridge in the spanning tree. Lower numbers indicate a better priority.

By default, the bridge with the lowest bridge priority is selected as the root. In the event of a tie, the bridge with the lowest priority and lower MAC address is selected.

There are two ways to select a root bridge (switch).

The first is to leave all the spanning tree priority settings at the default setting of 32768. When all the switches are set at the default priority, the managed switch with the lowest MAC address is selected as the root. This may be adequate for networks with light or evenly distributed traffic.

The second way to select a root bridge is to customize priority settings of each bridge. Customizing the spanning tree priority settings allows the network to select a root bridge that gives the best network performance. The goal is generally to have the network traffic pass through the network as directly as possible, so the root should be central in the network. If most messages are between one central server and several clients, the root should probably be a switch near the server so messages do not take a long path to the root and another long path back to the server.

Once you decide which switch should be the root, it should be given the best (numerically lowest) spanning tree priority number in the network.

Hello Time (1 to 10 seconds; Default = 2): Configuration messages (BPDUs) are sent periodically to other bridges based on a time period labeled hello time. Decreasing the hello time gives faster recovery times; increasing the hello time interval decreases the overhead involved.

The hello time must satisfy the following constraints:

2 x (hello time + 1.0 seconds) < max age < 2 x (forward delay - 1.0 seconds)

Max Age Time (6 to 40 seconds; Default = 20): For STP, the max age indicates the maximum time (in seconds) that the switch will wait for configuration messages (BPDUs) from other managed switches. If that time expires, the switch assumes that it is no longer connected to the root of the network. If a link goes down in a way that the switch can detect the loss of link, it does not wait before reconfiguring the network.

For RSTP, the Maximum Age is not measured in seconds, rather these units are "hops". RSTP waits 3 times the Hello Time instead of Max Age before assuming that it is no longer connected to the root of the network. However, Max Age is used to limit the number of hops Spanning Tree information may travel from the root bridge before being discarded as invalid.

The maximum age must satisfy the following constraints:

2 x (hello time + 1.0 seconds) < max age < 2 x (forward delay - 1.0 seconds)

Forward Delay Time (4 to 30 seconds; Default = 15): The forward delay is a time (in seconds) used by all switches in the network. This value is controlled by the root bridge and is used as a timeout value to allow ports to begin forwarding traffic after network topology changes. If RSTP cannot negotiate the link status, a port must wait twice the forward delay before forwarding network traffic. In a properly configured network using RSTP (not STP) this setting has very little effect. For STP networks, setting the time too short may allow temporary loops when the network structure changes (switches turn on or off or links are added or broken). A longer time will prevent temporary loops, but network traffic will be disrupted for a longer time.

The default value for the forward delay is 15 seconds. If you change this setting, the switch will not allow a value unless it satisfies the following formula:

2 × (hello time + 1.0 seconds) < max age < 2 x (forward delay - 1.0 seconds)

Message Age Increment: How to modify the Message Age when a BPDU passes through the switch.

Default = Increments by the greater of (Max Age Time / 16) or one

Compulsory = Increments by one

Spanning Tree may be Enabled on individual ports. By default, RSTP is Enabled on all ports.

Commonly, Edge ports (ports connected directly to an end device and not connected to any other managed switch) should have RSTP Disabled to minimize the convergence time when the spanning tree must be renegotiated.

A port that has spanning tree participation Disabled will not be used as part of the managed network. For example, a single uplink from a managed network of factory devices to a business network would be configured to be excluded from RSTP use.

A pair of ports configured for AD-Ring or AD-RP must be excluded from Spanning Tree.

A port that is configured as a Monitor Port or a Monitoring Port ***must be*** excluded from in Spanning Tree.

A port configured as a Trunk Port ***must be*** excluded from Spanning Tree.

Port Status

The Port Status is the STP/RSTP State of the Port: The terms used are slightly different between STP and RSTP.

STP:

- Blocking = A port in this state does not participate in frame relay. That is, it doesn't transmit ordinary network traffic. Once a port is in this state, it prevents frame duplication caused by multiple paths in an active topology.
- Listening = A port in this state is preparing to participate in frame relay (ordinary network traffic) by building a description of the network by listening to BPDUs (Bridge Protocol Data Units, that is, network configuration messages) but not forwarding frames (ordinary network traffic). The reason for not entering frame relay immediately is to ensure that there are no temporary loops introduced when the network topology is changing.
- Learning = A port in this state is adding network information to the filtering database.
- Forwarding = A port in the forwarding state is currently participating in frame relay (ordinary network traffic). BPDUs will include the forwarding port in the computation of the active topology. BPDUs received are processed according to the Spanning Tree algorithm and transmitted based on the hello time or BPDU information received.

RSTP:

- Discarding = A port in this state does not participate in frame relay. That is, it doesn't transmit ordinary network traffic. Once a port is in this state, it prevents frame duplication caused by multiple paths in an active topology
- Learning = A port in this state is preparing to participate in frame relay (ordinary network traffic) by building a description of the network by listening to BPDUs (Bridge Protocol Data Units, that is, network configuration messages) but not forwarding frames (ordinary network traffic). The reason for not entering frame relay immediately is to ensure that there are no temporary loops introduced when the network topology is changing.
- Forwarding = A port in the forwarding state is currently participating in frame relay (ordinary network traffic). BPDUs will include the forwarding port in the computation of the active topology. BPDUs received are processed according to the Spanning Tree algorithm and transmitted based on the hello time or BPDU information received.

Port Priority

Port Priority 0 to 255; Default = 128): Selection of the port to be assigned “root” if two ports are connected in a loop is based on the port with the lowest port priority. If the root bridge fails, the bridge with the next lowest priority then becomes the root.

If the switch has more than one port that provides a path to the root bridge and the ports have the same root path cost, the selection of which port to use is based on the port priority. The port with the best (numerically lowest) priority will be used. If the port priority is the same, the switch will use the lowest numbered port.

Path Cost (1 to 200,000,000; Default = 20,000 for 10 / 100 / 1000 ports and 200,000 for 10 / 100 ports): As with any network, there is an associated cost to go from a source location to a destination location. For RSTP, the root path cost is calculated based on the bandwidth available for that particular connection to the root bridge. The port with the lowest cost for delivering messages to the root is used to pass traffic toward the root.

The path cost can be assigned automatically based on the port speed, using the IEEE standard values of 200,000 for 100Mbps links and 2,000,000 for 10Mbps links, or the value can be specified in the range 1 to 200,000,000 by UNCHECKING Path Cost Yes.

When Path Cost Yes is CHECKED, the default Path Cost values may not be changed.

See RSTP Examples for an illustration of how the path cost can be utilized to establish the primary and backup connections.

RSTP Examples

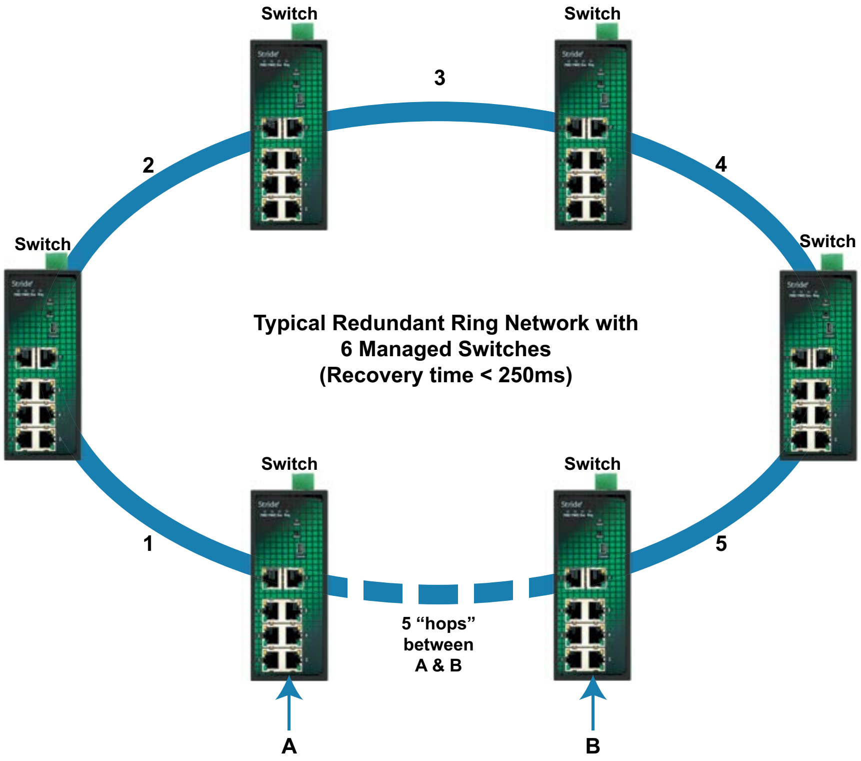
Example 1: Maximum "Hops" and Switches in a Redundant Ring:

The Max Age setting controls how long RSTP messages may circulate in the network. When a switch receives a message, it compares the age of the message with the Max Age (also carried in the message) and if the age has reached the Max Age, the message is discarded. Otherwise, the age is incremented before the message is forwarded. Therefore, the maximum diameter of a RSTP network is controlled by Max Age. Since the largest value allowed for Max Age is 40 (hops), the largest RSTP network hop diameter is also 40.

Number of Hops vs. Recovery Time:

The diagram below shows a typical redundant ring network with 6 managed switches and 5 hops between stations.

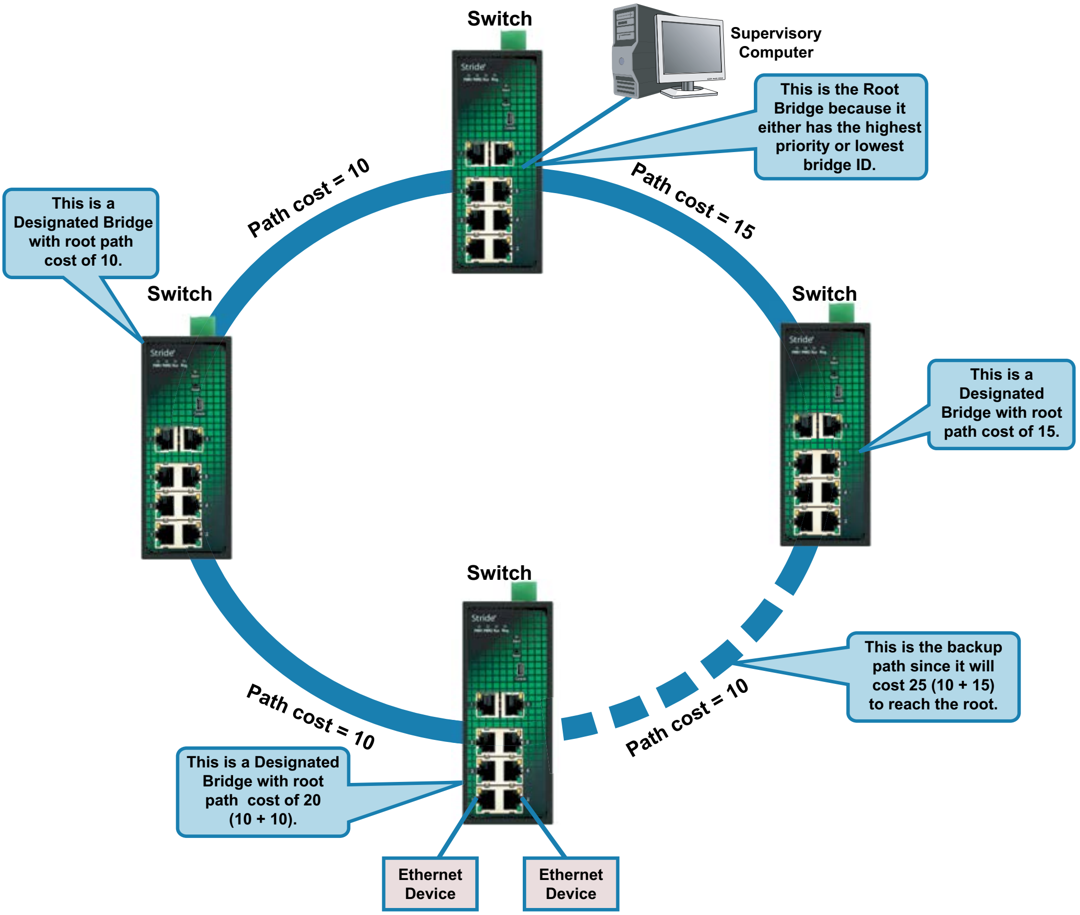
The overall recovery time when there is a network segment failure is dependent on the number of hops. The recovery time is typically less than 50ms per hop. Therefore, in the diagram below of a typical ring with 6 managed switches the overall recovery time would be less than 250ms (5 hops x <50ms).



Example 2: Using Path Costs to Establish Primary & Backup Connections:

The path cost can be used to determine the best connections to use. You can assign a higher cost to pathways that are more expensive, slower or less desirable in any way. The managed switches will then add up the path costs to determine the best route back to the root switch. See the example below.

NOTE: *In most networks you may leave the path costs set to the default settings and allow the Switches to automatically determine the best paths.*


Switch
Supervisory Computer
This is the Root Bridge because it either has the highest priority or lowest bridge ID.
Path cost = 10
Path cost = 15
This is a Designated Bridge with root path cost of 10.
Switch
Switch
This is a Designated Bridge with root path cost of 15.
Switch
This is the backup path since it will cost 25 (10 + 15) to reach the root.
Path cost = 10
Path cost = 10
This is a Designated Bridge with root path cost of 20 (10 + 10).
Ethernet Device
Ethernet Device

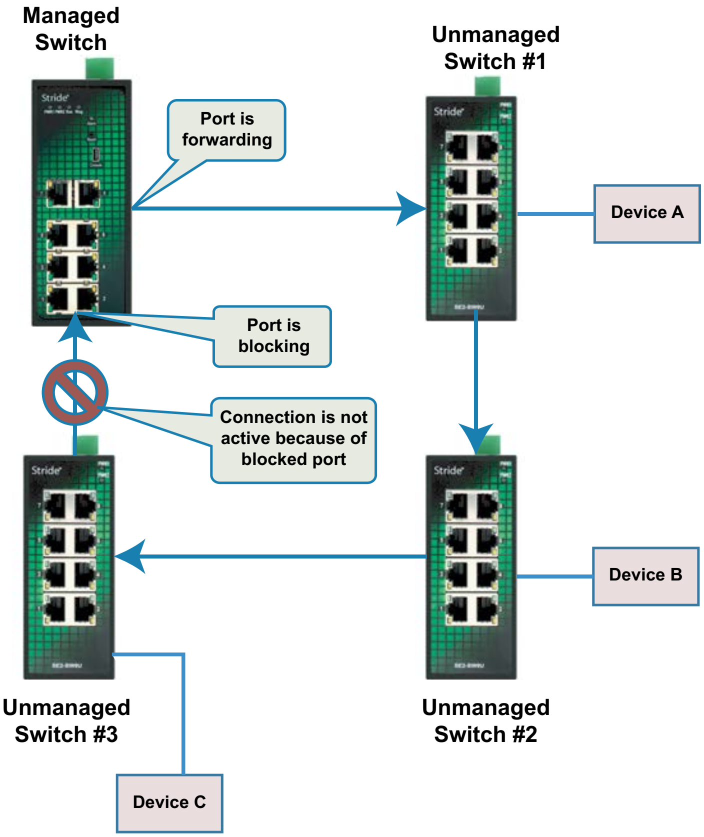
Example 3: Ring Topology with only 1 Managed Switch (Bad idea!)

Implementing a ring topology with a single managed switch and several unmanaged switches is occasionally considered to try to save money. The topology is legal only if that single managed switch is a member of each ring. Although it is legal, it is not recommended, as the hypothetical scenario indicated below will explain.

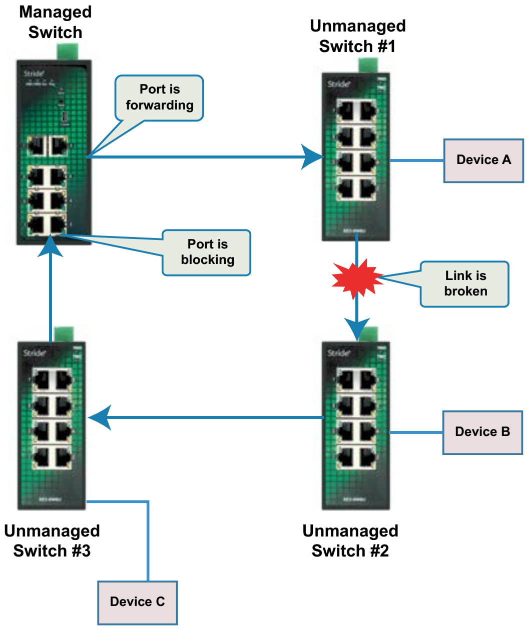
Hypothetical Scenario:

An integrator wishes to implement a single Ethernet ring topology for the proposed network. Only one managed switch is used to connect to three or more unmanaged switches in the loop (Figure below).

Initially, everything is working fine in the network. The managed switch detects the loop by seeing its own configuration messages and based on STP parameters, chooses one port to be in the forwarding state, and the other port to be in the blocking state. No loop is formed and device A can talk to device B.



Somewhere in the plant, a construction vehicle accidentally cuts the connection between unmanaged switch #1 and unmanaged switch #2. The managed switch in the network notices (typically around 6 seconds when connected to an unmanaged switch) that the port in blocking mode is not receiving configuration messages and transitions through the listening, learning, and forwarding states (Figure below).



This would seem to have solved the problem as both ports in the managed switch are in forwarding mode, but it is not the case. Due to the fact that the other three switches are unmanaged, they do not have the intelligence to know that there has been a change in the network topology. Switch #1 still points to switch #2 when device A is trying to talk to device B (across the broken Ethernet link). The bottleneck has been discovered, as we have to wait until the MAC table in switch #1 ages out its entries of device A and device B. The same applies for devices connected to switch #2 (B talking to A) and switch #3 (C talking to A).

As a result of this “money saving” configuration, the network redundancy performance is traded off and left at the mercy of the time it takes to age out MAC table entries in switches 1, 2, and 3. Depending on the model of unmanaged Ethernet switch, entries in the MAC table are usually aged out in a time period of 5 minutes or more.

This introduces at least 5 minutes of downtime for the plant, which could have a very detrimental cost with respect to the operation of the plant. By replacing switches 1, 2, and 3 with managed switches, the network convergence time is reduced to less than a second. An additional benefit is that the network is not limited to only one redundant loop and can have a “mesh” of connections for a truly redundant network scheme at all points in the network.

Multicast Filtering (IGMP)

IGMP (Internet Group Management Protocol) allows hosts and routers to work together to optimize forwarding of multicast traffic on a network. Without IGMP, all multicast packets must be forwarded to all network segments. With IGMP, multicast traffic is only forwarded to those network segments which connect interested hosts.

An IGMP snooping switch performs many of the functions of an IGMP router.

When a switch is configured to Enable Auto Query, it will send its own queries to speed network convergence. When Auto Query is not Enabled on a switch, it processes IGMP protocol messages sent by hosts and routers to configure efficient forwarding of multicast traffic.

Periodically, routers and IGMP snooping switches with Auto Query enabled send an IGMP Query on each attached network. (The query interval is generally around 1-2 minutes.) A host that wishes to be a member of a group sets a timer for a short, random delay when it sees the Query. If it sees a Report from another host before its timer expires, it cancels the timer and takes no further action until another Query is seen. If no other Report is seen, a Report is sent when the timer expires. The router or switch uses the Report to configure multicast forwarding.

The router or switch keeps track of how long it has been since the last Report on each port for each group. When the group expires, the router or switch stops forwarding multicast data to that port. Since the query interval is less than the expiration time, data for active groups continues to be forwarded without interruption.

IGMP Protocol Settings

The default settings will allow the switch to recognize members of a multicast group and forward the multicast message to only members of that group.

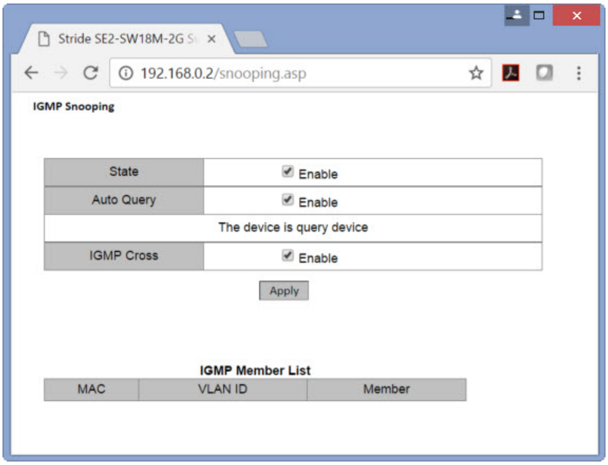
IGMP Snooping State – IGMP Snooping is Enabled by default. The switch will participate in IGMP handling.

When IGMP Snooping State is Disabled, the switch will ignore IGMP messages. All multicast traffic will be sent to all ports.

Auto Query – Also referred to as Active IGMP handling: Enabled by default. Causes the switch to act as an IGMP router, sending queries when needed and configuring multicast forwarding according to IGMP membership reports. At least one switch must have Auto Query Enabled.

When Auto Query is Disabled, the switch will listen to IGMP messages and configure forwarding of multicast traffic accordingly.

IGMP Cross – When Enabled allow multicast traffic to cross between VLANS



IGMP Snooping

State	☑ Enable
Auto Query	☑ Enable
The device is query device	
IGMP Cross	☑ Enable

IGMP Member List

MAC	VLAN ID	Member

Static FDB Multicast

Static FDB Multicast will allow a switch to function in a network with multicast groups. Although when IGMP is Enabled, the switch will dynamically learn which ports have IGMP routers attached to them by listening for IGMP Query messages, a Multicast group can be more permanently configured to force the switch to forward IGMP messages to a configured group of ports.

The Multicast MAC address must be in the range of **01**-00-5E-00-00-00 to **01**-00-5E-7F-FF-FF

GMRP

GMRP predates the ubiquity of IP protocols. Unless there are conditions specific to your network that warrant use of GMRP, IGMP Snooping is the preferred method of Multicast traffic management.

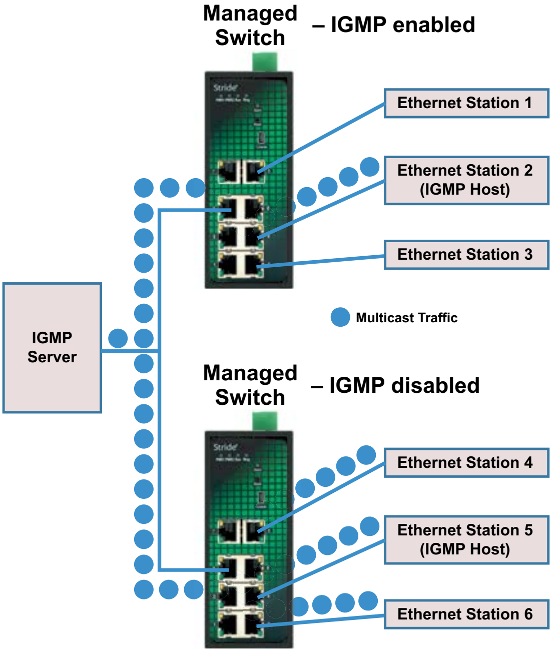
The Benefits of Enabling IGMP

Consider an already established control network that has an Ethernet device sending multicast data to several other Ethernet devices. Between the source of the multicast data, and the destination Ethernet devices that are interested in the multicast data, multicast packets might pass through a number of switches or routers.

To make this control network more efficient, the switches or routers should know how to handle the flow of multicast data by means of IGMP (Internet Group Management Protocol). Switches or routers that are not capable of supporting IGMP will not know what to do with the multicast data and forward multicast data out all ports. This will slow down the network.

Take a look at the following diagram, where the IGMP server is the source of the multicast data, and the IGMP hosts are the devices interested in receiving multicast data. On the network are two switches, where one has IGMP enabled and the other has IGMP disabled.

We see that the switch with IGMP enabled only forwards multicast data to the interested host (Ethernet Station 2). The switch with IGMP disabled will not know where to send the multicast data; thus Ethernet Stations 4 and 6 unnecessarily receive multicast data even though only Station 5 is the interested host.


Managed Switch – IGMP enabled
Ethernet Station 1
Ethernet Station 2 (IGMP Host)
Ethernet Station 3
● Multicast Traffic
IGMP Server
Managed Switch – IGMP disabled
Ethernet Station 4
Ethernet Station 5 (IGMP Host)
Ethernet Station 6

Port Monitoring

In an unmanaged switch, each port is filtered to only send and receive Ethernet packets to devices physically connected to that port. This makes it impossible to view the messages occurring between two other devices from a third device (such as a PC running a tool like "Wireshark").

The monitoring option is ideal for performing diagnostics by allowing traffic that is being sent to and received from one or more source ports to be replicated out the monitor port.

Choose a monitor port.

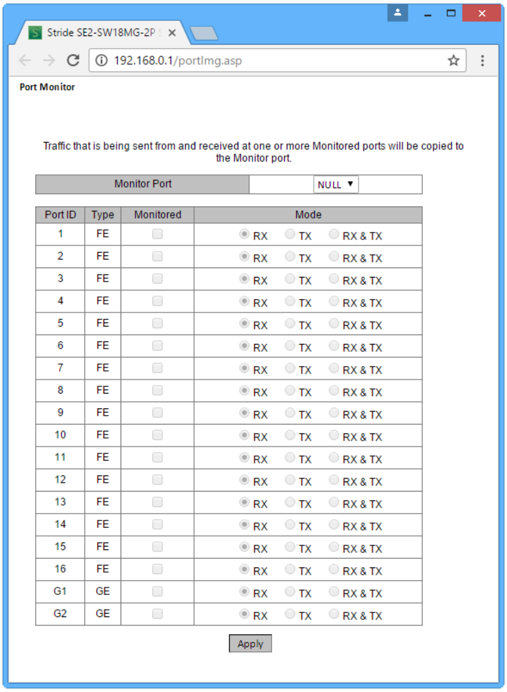
Choose the source ports to be monitored (mirrored).

For each source port choose the data to monitor: choose to monitor messages being received (Rx), sent (Tx), or messages being received and sent (Rx& Tx)

To view the traffic, connect a PC running network monitoring software (such as Wireshark) to the Monitor port.

Port monitoring and the following features are mutually exclusive. That is, to configure a port as a Monitor Port or as a Monitored Port, Disable the following features on those ports:

- Port Trunk
- RSTP/STP
- AD-Ring and AD-RP
- DHCP Snooping Trust port



Port Monitor

Traffic that is being sent from and received at one or more Monitored ports will be copied to the Monitor port.

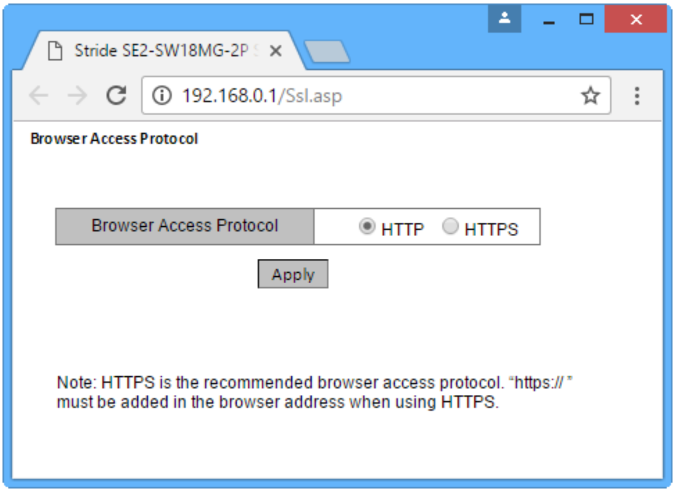
Monitor Port	NULL ▾

Port ID	Type	Monitored	Mode
1	FE	☐	● RX ○ TX ○ RX & TX
2	FE	☐	● RX ○ TX ○ RX & TX
3	FE	☐	● RX ○ TX ○ RX & TX
4	FE	☐	● RX ○ TX ○ RX & TX
5	FE	☐	● RX ○ TX ○ RX & TX
6	FE	☐	● RX ○ TX ○ RX & TX
7	FE	☐	● RX ○ TX ○ RX & TX
8	FE	☐	● RX ○ TX ○ RX & TX
9	FE	☐	● RX ○ TX ○ RX & TX
10	FE	☐	● RX ○ TX ○ RX & TX
11	FE	☐	● RX ○ TX ○ RX & TX
12	FE	☐	● RX ○ TX ○ RX & TX
13	FE	☐	● RX ○ TX ○ RX & TX
14	FE	☐	● RX ○ TX ○ RX & TX
15	FE	☐	● RX ○ TX ○ RX & TX
16	FE	☐	● RX ○ TX ○ RX & TX
G1	GE	☐	● RX ○ TX ○ RX & TX
G2	GE	☐	● RX ○ TX ○ RX & TX

Browser Access Protocol (HTTPS)

By default, access to the Switch Management Interface is configured for HTTP (port 80)

A level of security may be gained by configuring access using HTTPS (SSL 3.0, port 443.) SSL will encrypt data passing to and from the switch management interface, including the password.



Browser Access Protocol

Browser Access Protocol	● HTTP ○ HTTPS

Note: HTTPS is the recommended browser access protocol. "https:// " must be added in the browser address when using HTTPS.

Virtual LANs (VLANs)

VLANs can segregate traffic flowing through a switch to improve bandwidth utilization or security. Segregation is done based on membership in a group of ports (Untagged) or on IEEE 802.1Q tags which include a VLAN ID (Tagged).

An Untagged VLAN limits forwarding traffic coming in a port to the group of ports to which that port belongs. For example, on a 10-port switch if ports 1, 3, 5, 7, and 9 were placed in an Untagged VLAN, broadcast frames coming in port 3 would be sent to ports 1, 5, 7, and 9 (which are members of port 3's VLAN) but not to ports 2, 4, 6, 8 and 10 (which are not members).

A port may be a member of only one Untagged VLAN.

A tag-based VLAN is more common. A tag-based VLAN limits traffic based on the VLAN ID in a 'tag' associated with the frame. VLAN tags may be explicitly placed in frames by applications or switching equipment, or implicitly assigned to frames based on the switch port where they arrive.

VLAN IDs are 12-bits long providing 4096 possible IDs but several IDs are reserved:

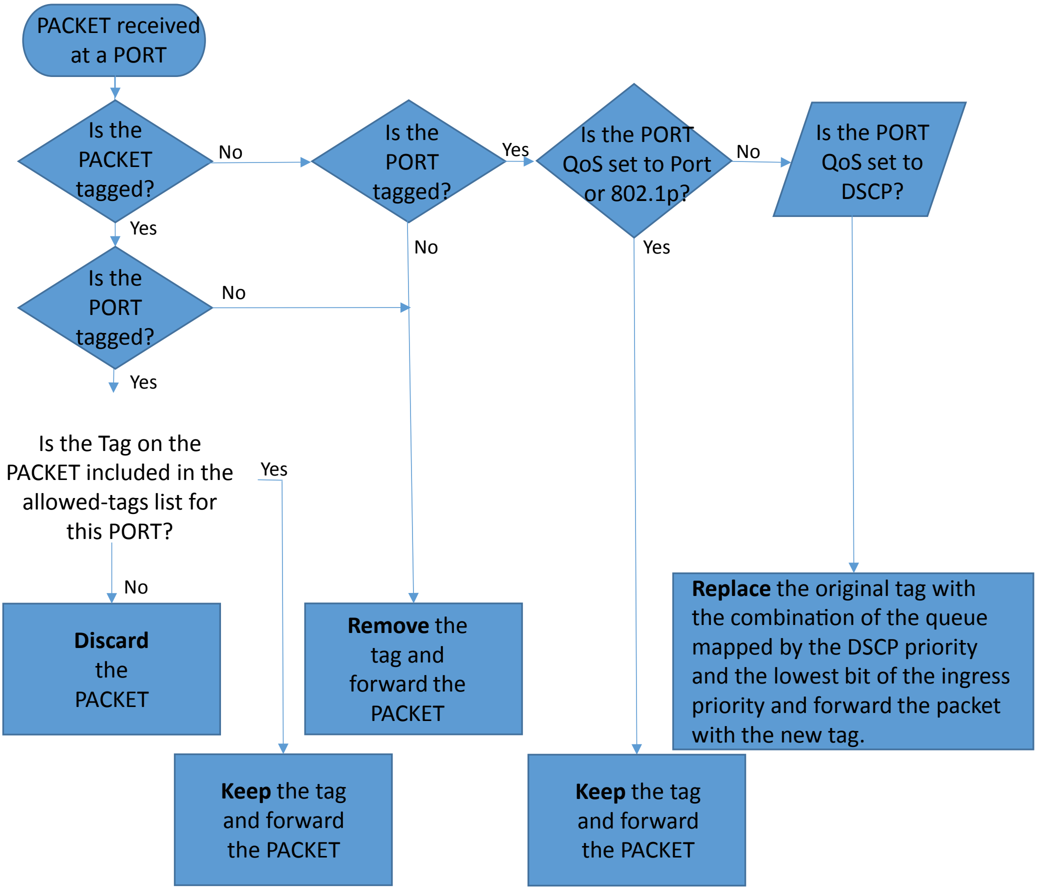
- 0 = Indicates that the tag is not being used for VLAN routing but only to carry priority information. (See QoS topic).
- 1 = Used for switch configuration and management.
- 4095 = Not allowed by the 802.1Q standard.

The default VID for all ports is VLAN 1.

The 802.1Q VID for a Port based VLAN is the VLAN ID for Untagged VLANs.

Max 256 VLANs are supported.

After setting port type and VID, there are several ways to process port-received and port-transmitted messages:


PACKET received at a PORT
Is the PACKET tagged?
No
Yes
Is the PORT tagged?
No
Yes
Is the PORT tagged?
Yes
No
Is the PORT QoS set to Port or 802.1p?
No
Yes
Is the PORT QoS set to DSCP?
Is the Tag on the PACKET included in the allowed-tags list for this PORT?
Yes
No
Discard the PACKET
Remove the tag and forward the PACKET
Replace the original tag with the combination of the queue mapped by the DSCP priority and the lowest bit of the ingress priority and forward the packet with the new tag.
Keep the tag and forward the PACKET
Keep the tag and forward the PACKET

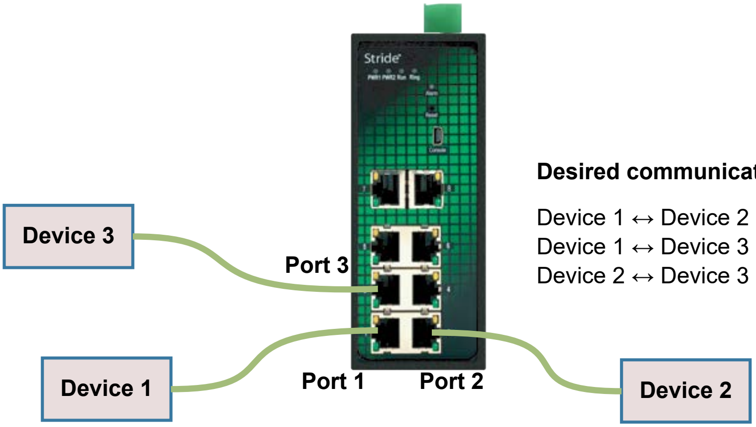
PVLAN – Private VLANs

An additional layer of traffic isolation and network security may be added by utilizing the Private VLAN (PVLAN) feature.

Within any configured VLAN, ports selected as PVLAN may not share traffic with any other port configured as Private. This feature is typically used where one port in a VLAN is NOT selected as Private and functions as an Uplink port. All other ports in that VLAN would typically be marked Private. Traffic may not be shared among the ports in the VLAN, but all traffic from all ports in that VLAN will be transmitted through the Uplink port to, typically, a router port.

NOTE 1: *When a PVLAN Tagged port forwards a message with a VLAN tag, the VLAN tag will be removed.*
NOTE 2: *Take care when setting the management VLAN ID. If the device you are configuring from cannot work with VLANs and the port it is connected to does not have the proper PVID and port type setting the management VLAN may make the Switch inaccessible and require a local serial connection to reconnect.*
NOTE 3: *Switch management and configuration is only possible through the port if the PVID is set to 1 (the default). Setting the PVID to another value prevents the Switch from being managed/configured via that port (unless the system you are using to configure the Switch can explicitly tag frames for VLAN 1, the management VLAN).*

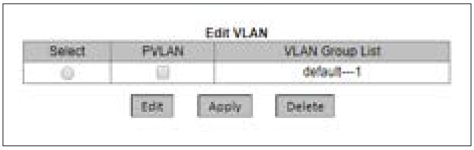
Example PVLAN configuration settings



Desired communication:

Device 1 ↔ Device 2 = Yes
Device 1 ↔ Device 3 = Yes
Device 2 ↔ Device 3 = NO

On the VLAN Configuration page, Select VLAN 1 in the Edit VLAN section in the middle of the page, then click the Edit button.

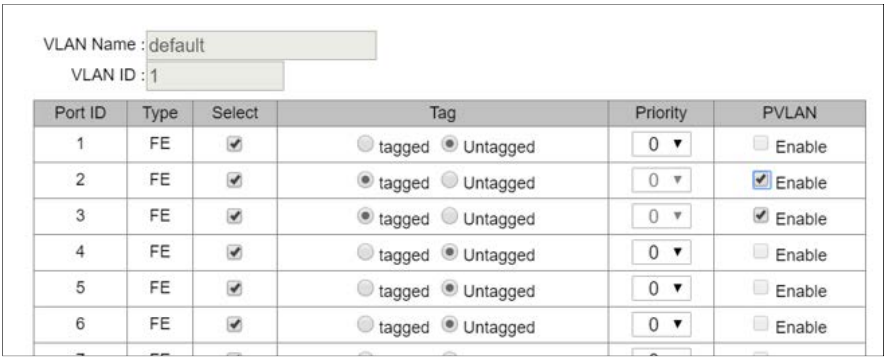

Edit VLAN

Select	PVLAN	VLAN Group List
○	□	default---1

Change ports 2 and 3 to "tagged" in the Tag column.

Enable PVLAN on ports 2 and 3 in the PVLAN column.

Click Apply to save these changes and return to the VLAN Configuration page.

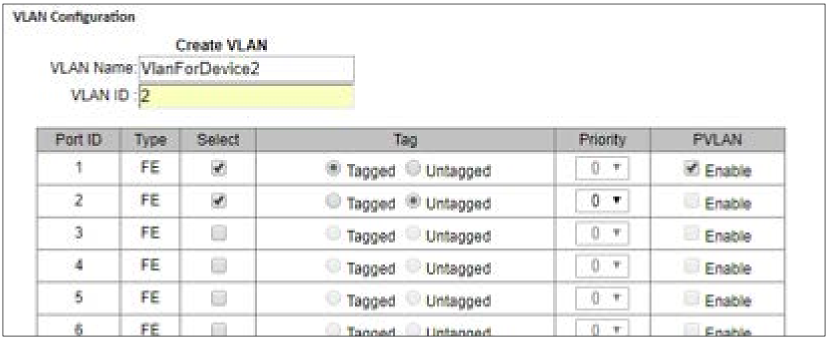


VLAN Name : default

VLAN ID : 1

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☑	○ tagged ● Untagged	0 ▼	□ Enable
2	FE	☑	● tagged ○ Untagged	0 ▼	☑ Enable
3	FE	☑	● tagged ○ Untagged	0 ▼	☑ Enable
4	FE	☑	○ tagged ● Untagged	0 ▼	□ Enable
5	FE	☑	○ tagged ● Untagged	0 ▼	□ Enable
6	FE	☑	○ tagged ● Untagged	0 ▼	□ Enable

In the Create VLAN section at the top of the page, configure and Add two new VLANs as shown below:



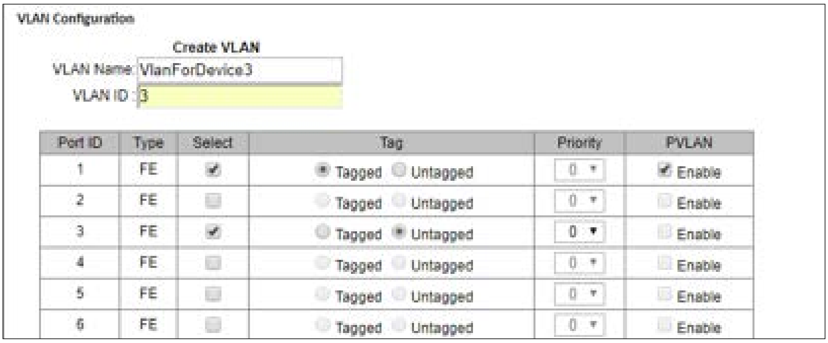
VLAN Configuration

Create VLAN

VLAN Name: VlanForDevice2

VLAN ID : 2

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☑	● Tagged ○ Untagged	0 ▼	☑ Enable
2	FE	☑	○ Tagged ● Untagged	0 ▼	□ Enable
3	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
4	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
5	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
6	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable



VLAN Configuration

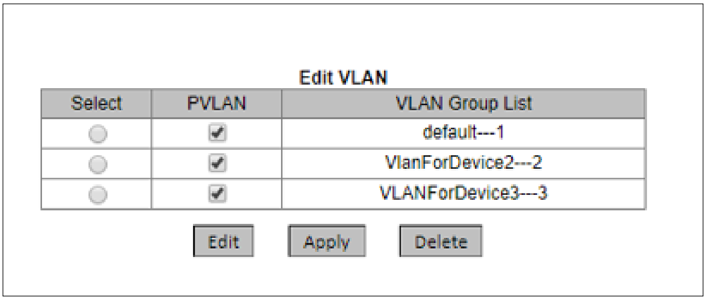
Create VLAN

VLAN Name: VlanForDevice3

VLAN ID : 3

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☑	● Tagged ○ Untagged	0 ▼	☑ Enable
2	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
3	FE	☑	○ Tagged ● Untagged	0 ▼	□ Enable
4	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
5	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
6	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable

In the Edit VLAN section in the middle of the page, Select the PVLAN option for all three of the VLANs:

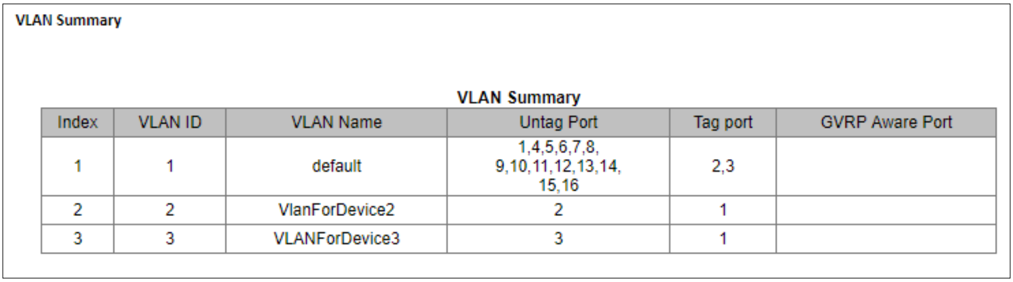


Edit VLAN

Select	PVLAN	VLAN Group List
○	☑	default---1
○	☑	VlanForDevice2---2
○	☑	VLANForDevice3---3

Click Apply to save these changes.

Navigate to the VLAN Summary page to verify the settings as shown below:



VLAN Summary

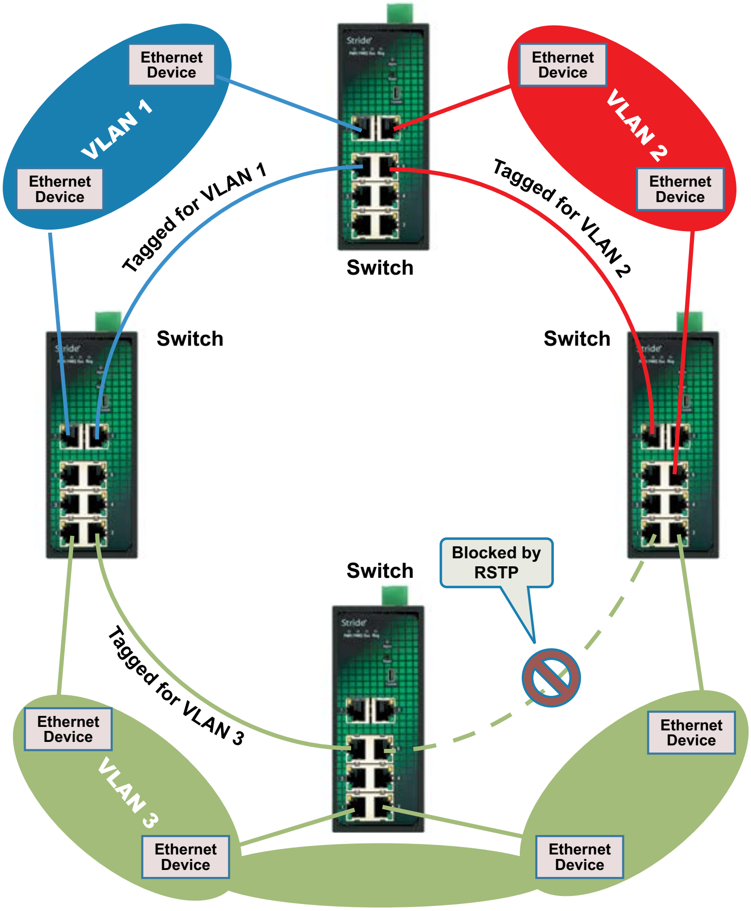
VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag port	GVRP Aware Port
1	1	default	1,4,5,6,7,8, 9,10,11,12,13,14, 15,16	2,3	
2	2	VlanForDevice2	2	1	
3	3	VLANForDevice3	3	1	

VLAN with RSTP

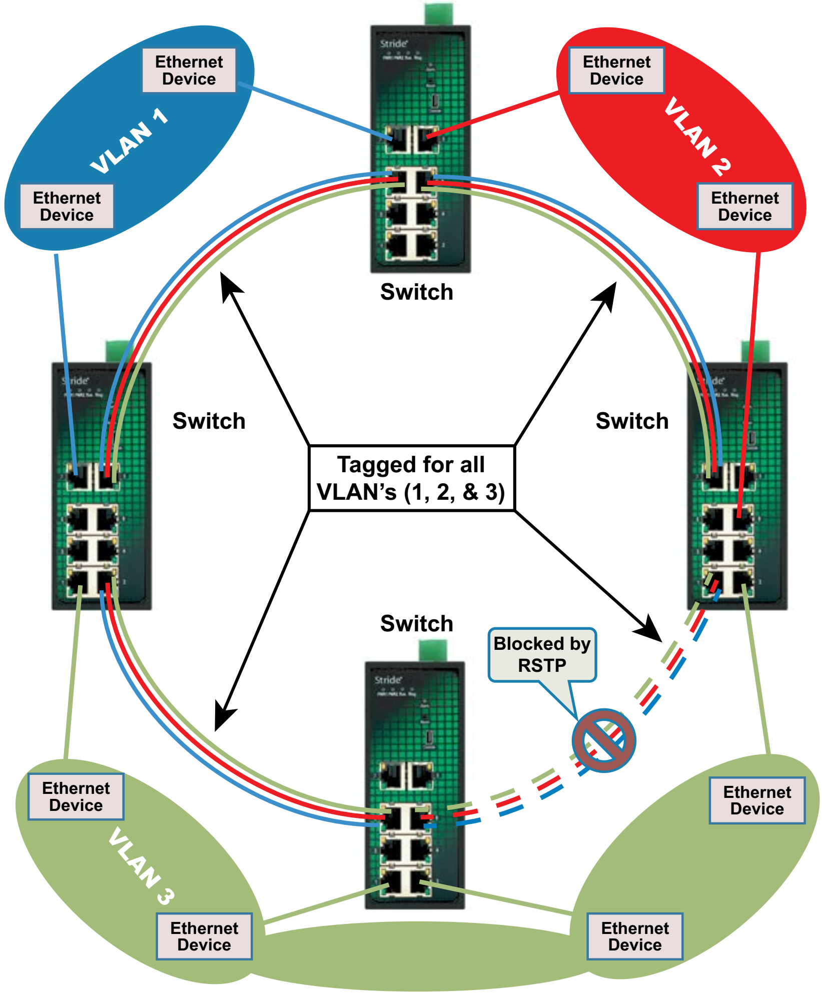
Extra care must be taken when enabling both VLANs and redundancy, or communications failures may occur.

The example shown in the following diagram depicts the problem with running the Rapid Spanning Tree Protocol (RSTP) and VLANs at the same time. The IEEE 802.1D based RSTP is not aware of the VLAN configuration. Therefore, in the example, one of the ports for VLAN 3 is being blocked. This prevents VLAN 3 from being able to forward data to all its members.



The solution to the problem above is to configure all ports connected between SWITCHES to carry all VLANs in the network.

As seen from the example shown in the following diagram, VLAN 3 can forward to all its members across another switch and is not affected by the blocked RSTP connection.



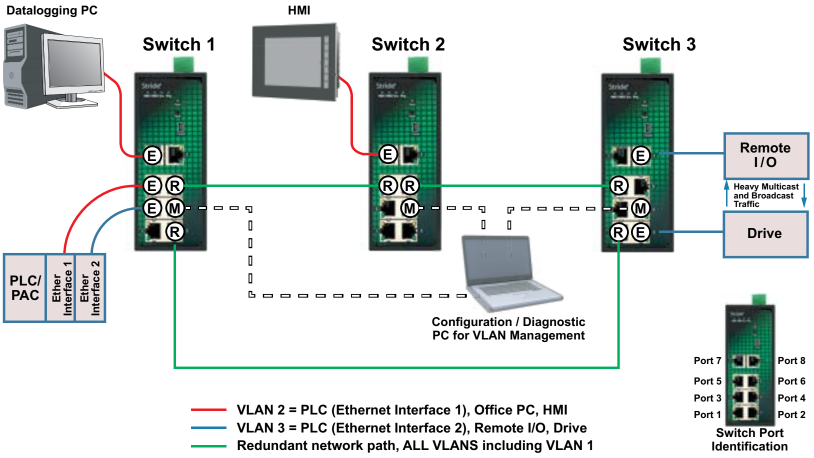
VLAN Examples

Shown below are two examples of using VLANs and how they can solve common network problems found in factory automation. Note that the end devices used in these examples do not recognize nor originate VLAN tags.

Problem #1: The process requires a PLC, Remote I/O, Variable Frequency Drive control, HMI access as well as a PC for Data Logging and a PC for configuration management. The Remote I/O device and drive communicate via Multicast and Broadcast messaging which an unmanaged switch cannot filter out. The PLC and the Remote I/O and Drive are remotely located from each other. Running multiple Ethernet connections would be costly and logistically complex so the customer wants to utilize existing wiring connections.

- Configuration and/or diagnostics of all switches can be accomplished by plugging into a port that participates in the management VLAN1. In our example, we designate these ports “M”.
- The ports designated “E” in our example are connected to edge devices. These devices neither recognize nor originate VLAN tags.
- To provide redundancy in our example network, we created a ring at the ports designated “R”. These ports must participate in RTSP or an AD-Ring. The ports must also participate in all VLANS used in our example network, VLAN1, VLAN2, and VLAN3.

Tag-based VLAN example


Datalogging PC
HMI
Switch 1
Switch 2
Switch 3
E
R
M
Remote I/O
Heavy Multicast and Broadcast Traffic
Drive
PLC/ PAC
Ether Interface 1
Ether Interface 2
Configuration / Diagnostic PC for VLAN Management
Port 7
Port 8
Port 5
Port 6
Port 3
Port 4
Port 1
Port 2
Switch Port Identification
VLAN 2 = PLC (Ethernet Interface 1), Office PC, HMI
VLAN 3 = PLC (Ethernet Interface 2), Remote I/O, Drive
Redundant network path, ALL VLANS including VLAN 1

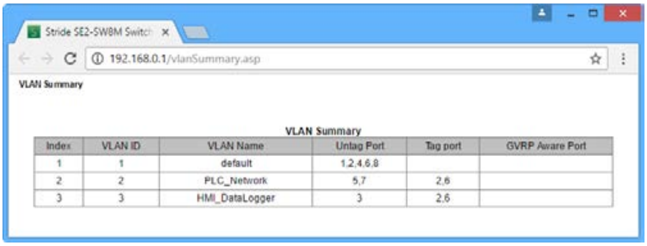
Solution: Use **Stride** managed switches, utilizing the VLAN feature to separate the broadcast and multicast traffic from all the devices except for the PLC. We will also wire the three switches into a Ring configuration so that we can take advantage of the redundancy feature of the switch. In this situation, we need to use Tag-based VLANs since the Ethernet packets will be traversing across multiple switches.

How to configure this setup

We created 3 VLANs:

- VLAN 1 is the default VLAN and we leave it there and enable it on what we will call a 'management port' for each switch. In this way, we can plug our laptop into the management port of any switch and be able to access the other switches across this VLAN to tweak the configuration or view the diagnostics.
- VLAN 2 will contain one of the Ethernet interfaces of the PLC, the HMI and the Office PC/ Data Logging PC.
- VLAN 3 will contain the other Ethernet interface of the PLC, the Remote I/O drop and the Drive.

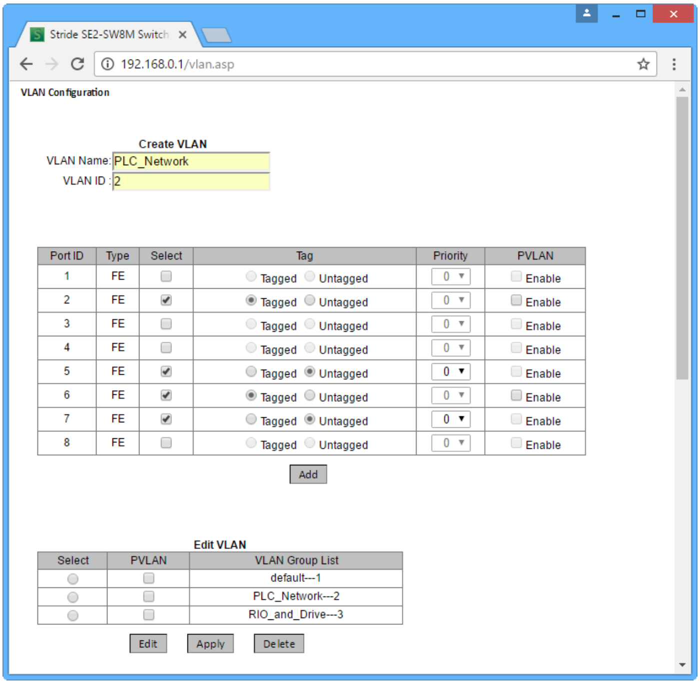
Switch 1 VLAN Configuration:



VLAN Summary

VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag port	GVRP Aware Port
1	1	default	1,2,4,6,8		
2	2	PLC_Network	5,7	2,6	
3	3	HMI_DataLogger	3	2,6	



VLAN Configuration

Create VLAN

VLAN Name: PLC_Network

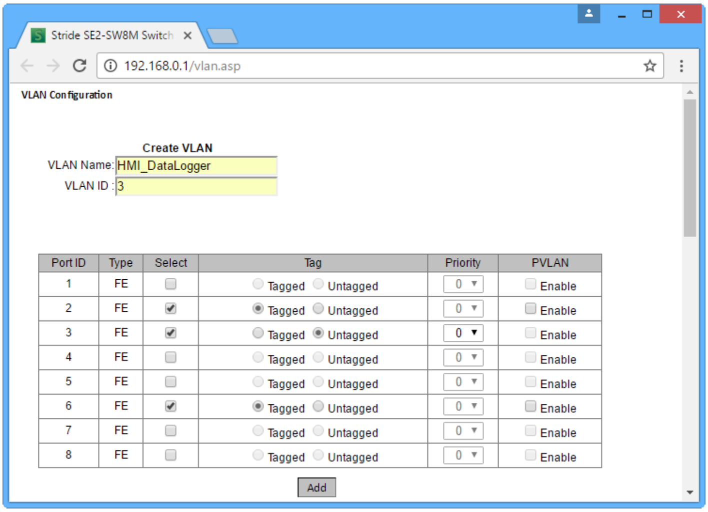
VLAN ID : 2

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	□	○ Tagged ○ Untagged	0	□ Enable
2	FE	☑	● Tagged ○ Untagged	0	□ Enable
3	FE	□	○ Tagged ○ Untagged	0	□ Enable
4	FE	□	○ Tagged ○ Untagged	0	□ Enable
5	FE	☑	○ Tagged ● Untagged	0	□ Enable
6	FE	☑	● Tagged ○ Untagged	0	□ Enable
7	FE	☑	○ Tagged ● Untagged	0	□ Enable
8	FE	□	○ Tagged ○ Untagged	0	□ Enable

Edit VLAN

Select	PVLAN	VLAN Group List
○	□	default---1
○	□	PLC_Network---2
○	□	RIO_and_Drive---3

Switch 1 VLAN Configuration (cont'd):



VLAN Configuration

Create VLAN

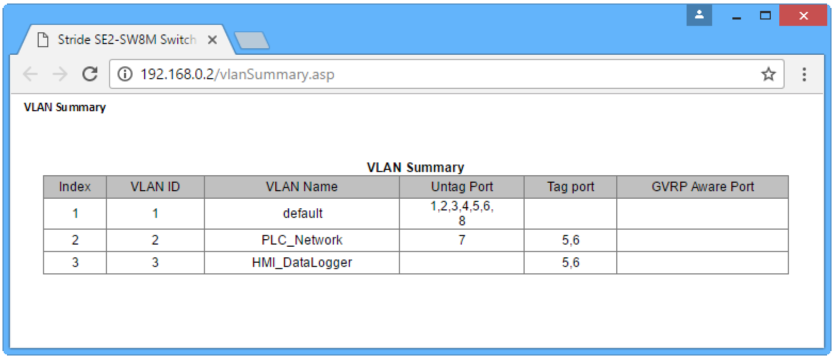
VLAN Name: HMI_DataLogger

VLAN ID : 3

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	□	○ Tagged ○ Untagged	0	□ Enable
2	FE	☑	● Tagged ○ Untagged	0	□ Enable
3	FE	☑	○ Tagged ● Untagged	0	□ Enable
4	FE	□	○ Tagged ○ Untagged	0	□ Enable
5	FE	□	○ Tagged ○ Untagged	0	□ Enable
6	FE	☑	● Tagged ○ Untagged	0	□ Enable
7	FE	□	○ Tagged ○ Untagged	0	□ Enable
8	FE	□	○ Tagged ○ Untagged	0	□ Enable

Add

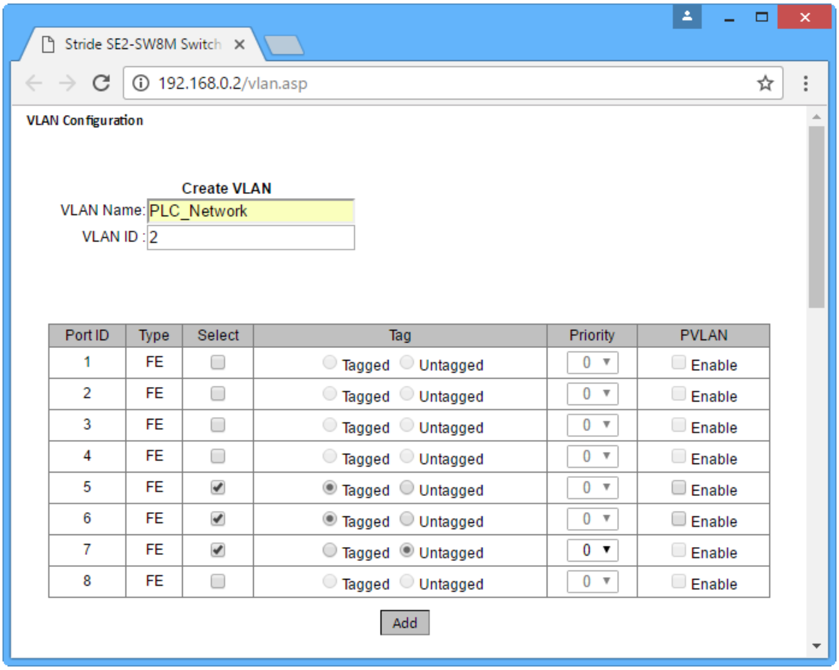
Switch 2 VLAN Configuration:



VLAN Summary

VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag port	GVRP Aware Port
1	1	default	1,2,3,4,5,6, 8		
2	2	PLC_Network	7	5,6	
3	3	HMI_DataLogger		5,6	



VLAN Configuration

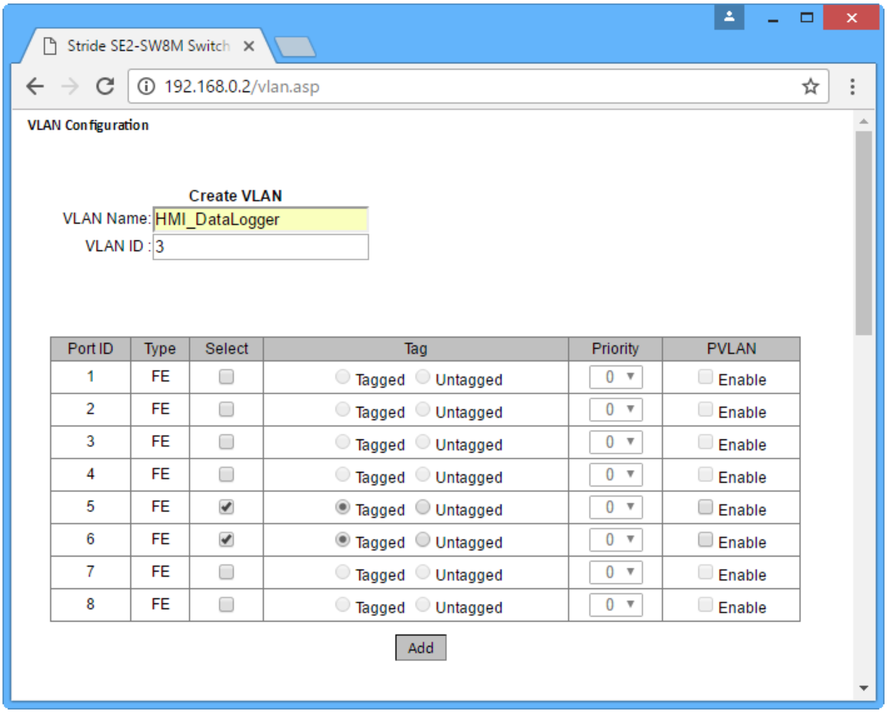
Create VLAN

VLAN Name: PLC_Network

VLAN ID : 2

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☐	○ Tagged ○ Untagged	0	☐ Enable
2	FE	☐	○ Tagged ○ Untagged	0	☐ Enable
3	FE	☐	○ Tagged ○ Untagged	0	☐ Enable
4	FE	☐	○ Tagged ○ Untagged	0	☐ Enable
5	FE	☑	● Tagged ○ Untagged	0	☐ Enable
6	FE	☑	● Tagged ○ Untagged	0	☐ Enable
7	FE	☑	○ Tagged ● Untagged	0	☐ Enable
8	FE	☐	○ Tagged ○ Untagged	0	☐ Enable

Switch 2 VLAN Configuration (cont'd):



VLAN Configuration

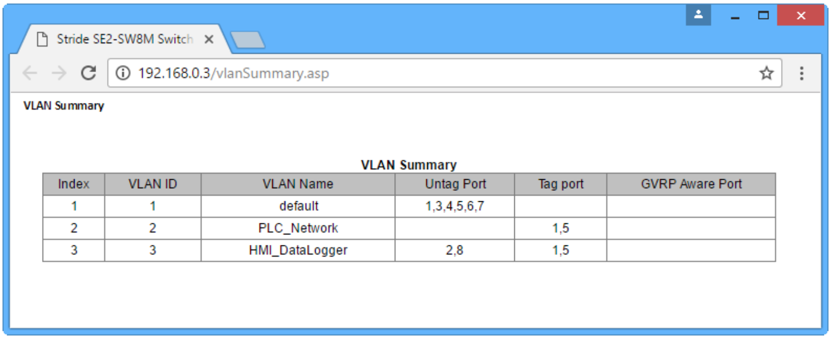
Create VLAN

VLAN Name: HMI_DataLogger

VLAN ID : 3

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
2	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
3	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
4	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
5	FE	☑	● Tagged ○ Untagged	0 ▼	□ Enable
6	FE	☑	● Tagged ○ Untagged	0 ▼	□ Enable
7	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable
8	FE	□	○ Tagged ○ Untagged	0 ▼	□ Enable

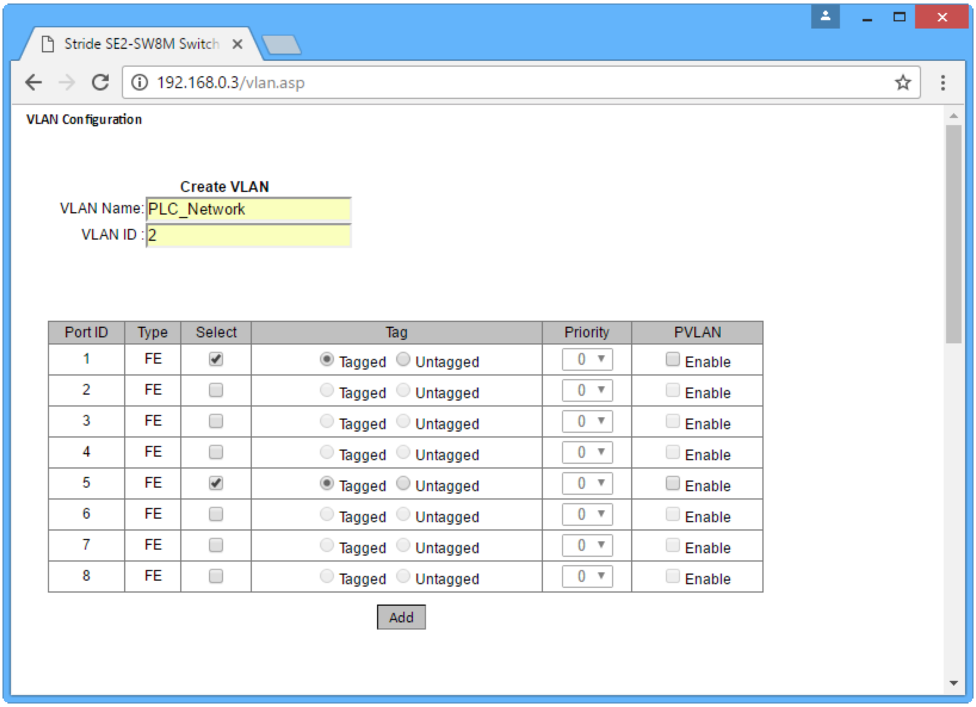
Switch 3 VLAN Configuration:



VLAN Summary

VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag port	GVRP Aware Port
1	1	default	1,3,4,5,6,7		
2	2	PLC_Network		1,5	
3	3	HMI_DataLogger	2,8	1,5	



VLAN Configuration

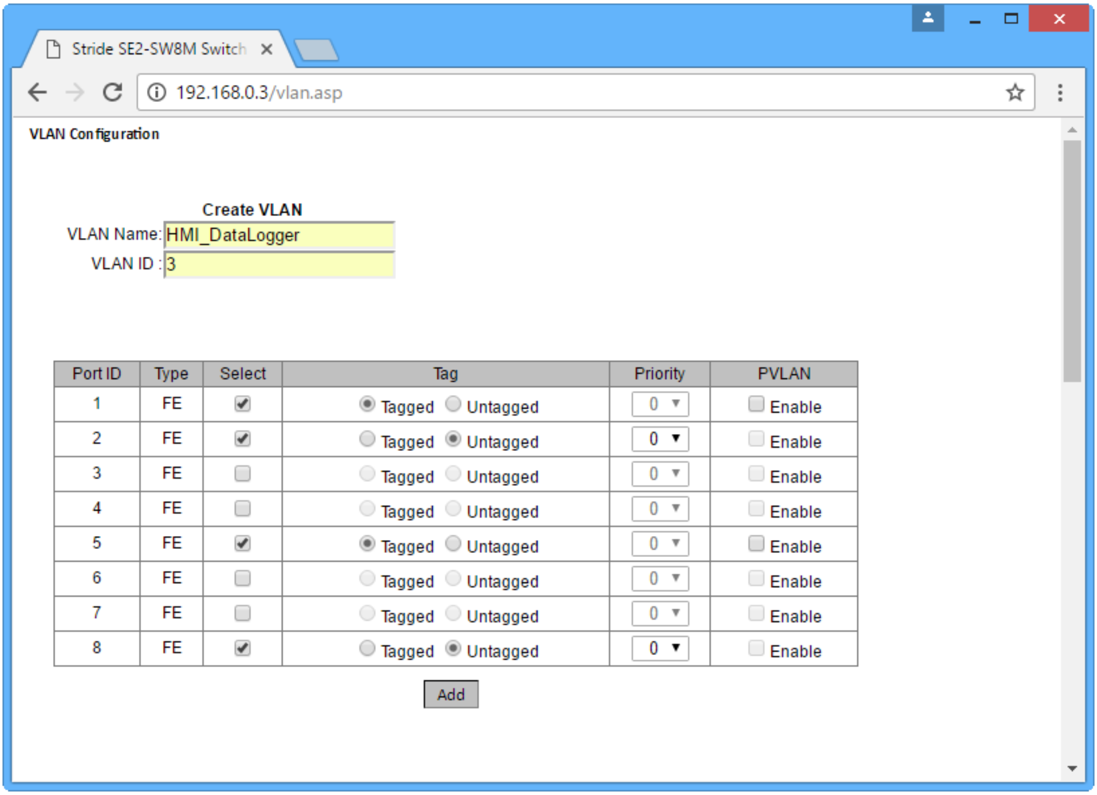
Create VLAN

VLAN Name: PLC_Network

VLAN ID : 2

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☑	● Tagged ○ Untagged	0	□ Enable
2	FE	□	○ Tagged ○ Untagged	0	□ Enable
3	FE	□	○ Tagged ○ Untagged	0	□ Enable
4	FE	□	○ Tagged ○ Untagged	0	□ Enable
5	FE	☑	● Tagged ○ Untagged	0	□ Enable
6	FE	□	○ Tagged ○ Untagged	0	□ Enable
7	FE	□	○ Tagged ○ Untagged	0	□ Enable
8	FE	□	○ Tagged ○ Untagged	0	□ Enable

Switch 3 VLAN Configuration (cont'd):



VLAN Configuration

Create VLAN

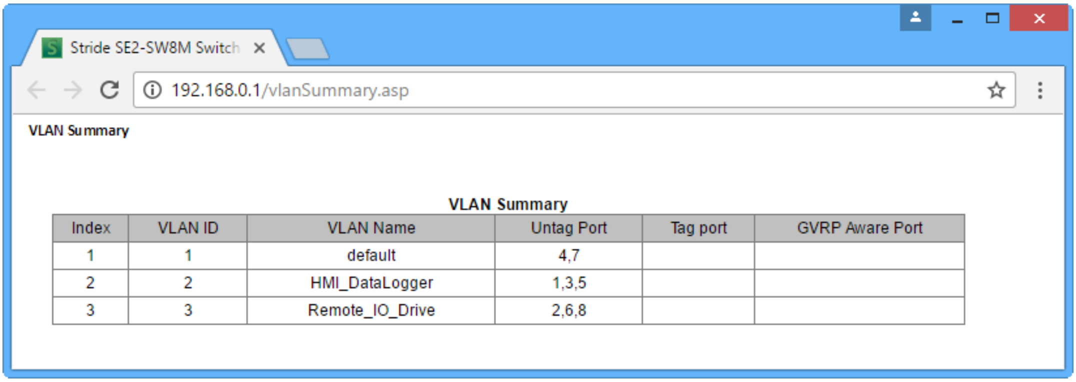
VLAN Name: HMI_DataLogger

VLAN ID : 3

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☑	● Tagged ○ Untagged	0	□ Enable
2	FE	☑	○ Tagged ● Untagged	0	□ Enable
3	FE	□	○ Tagged ○ Untagged	0	□ Enable
4	FE	□	○ Tagged ○ Untagged	0	□ Enable
5	FE	☑	● Tagged ○ Untagged	0	□ Enable
6	FE	□	○ Tagged ○ Untagged	0	□ Enable
7	FE	□	○ Tagged ○ Untagged	0	□ Enable
8	FE	☑	○ Tagged ● Untagged	0	□ Enable

Problem #2: This scenario is very similar to the first. We have the same problem to solve but the logistics are simpler, in that all of the devices are local and can be wired into the same switch.

Solution: We will use a **Stride** managed switch, utilizing the Port-based VLAN feature. The question could be posed, “Why not just use two unmanaged switches?” While this would work, the customer wants to use as few components in the system as possible to minimize points for possible equipment faults and he would like the enhanced diagnostic capabilities that a managed switch provides.

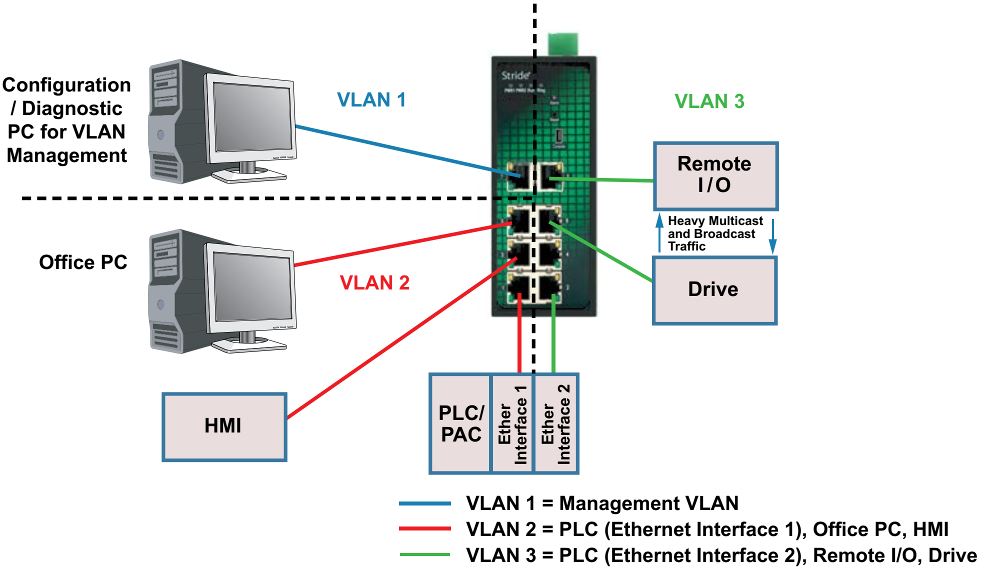


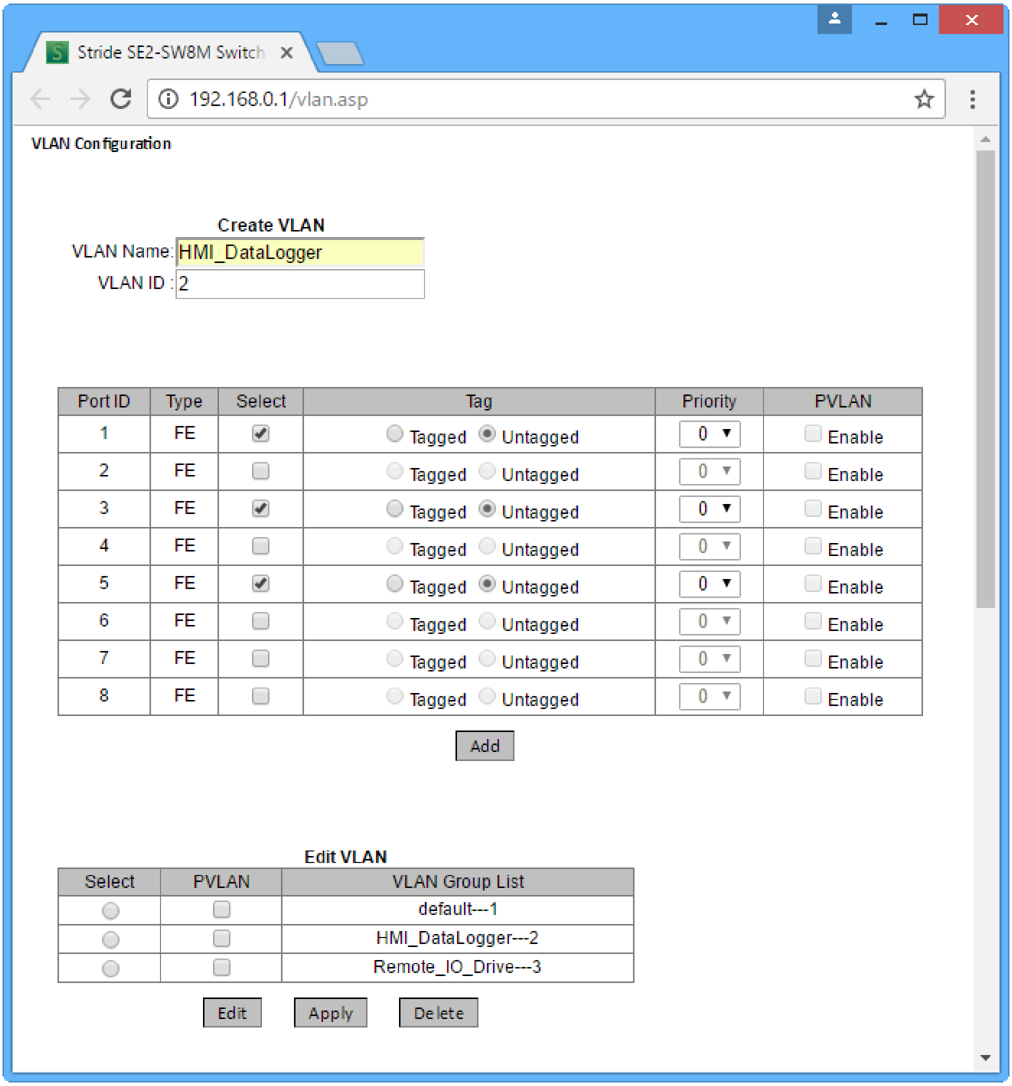
VLAN Summary

VLAN Summary

Index	VLAN ID	VLAN Name	Untag Port	Tag port	GVRP Aware Port
1	1	default	4,7		
2	2	HMI_DataLogger	1,3,5		
3	3	Remote_IO_Drive	2,6,8		

Port-based VLAN example


Configuration / Diagnostic PC for VLAN Management
VLAN 1
VLAN 3
Stride
Remote I/O
Heavy Multicast and Broadcast Traffic
Office PC
VLAN 2
Drive
HMI
PLC/ PAC
Ether Interface 1
Ether Interface 2
VLAN 1 = Management VLAN
VLAN 2 = PLC (Ethernet Interface 1), Office PC, HMI
VLAN 3 = PLC (Ethernet Interface 2), Remote I/O, Drive



VLAN Configuration

Create VLAN

VLAN Name: HMI_DataLogger

VLAN ID : 2

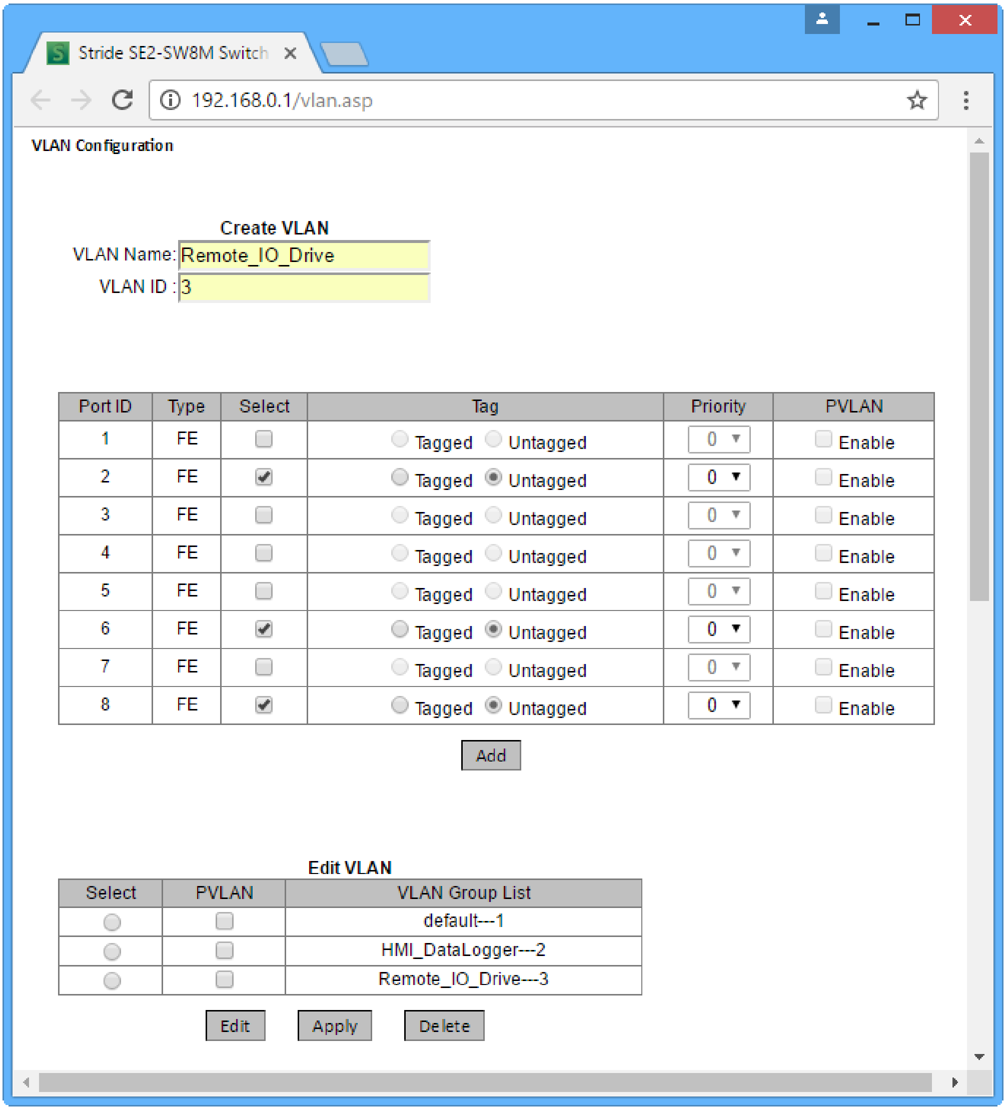
Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	☑	○ Tagged ● Untagged	0	□ Enable
2	FE	□	○ Tagged ○ Untagged	0	□ Enable
3	FE	☑	○ Tagged ● Untagged	0	□ Enable
4	FE	□	○ Tagged ○ Untagged	0	□ Enable
5	FE	☑	○ Tagged ● Untagged	0	□ Enable
6	FE	□	○ Tagged ○ Untagged	0	□ Enable
7	FE	□	○ Tagged ○ Untagged	0	□ Enable
8	FE	□	○ Tagged ○ Untagged	0	□ Enable

Add

Edit VLAN

Select	PVLAN	VLAN Group List
○	□	default---1
○	□	HMI_DataLogger---2
○	□	Remote_IO_Drive---3

Edit Apply Delete



VLAN Configuration

Create VLAN

VLAN Name: Remote_IO_Drive

VLAN ID : 3

Port ID	Type	Select	Tag	Priority	PVLAN
1	FE	□	○ Tagged ○ Untagged	0	□ Enable
2	FE	☑	○ Tagged ● Untagged	0	□ Enable
3	FE	□	○ Tagged ○ Untagged	0	□ Enable
4	FE	□	○ Tagged ○ Untagged	0	□ Enable
5	FE	□	○ Tagged ○ Untagged	0	□ Enable
6	FE	☑	○ Tagged ● Untagged	0	□ Enable
7	FE	□	○ Tagged ○ Untagged	0	□ Enable
8	FE	☑	○ Tagged ● Untagged	0	□ Enable

Edit VLAN

Select	PVLAN	VLAN Group List
○	□	default---1
○	□	HMI_DataLogger---2
○	□	Remote_IO_Drive---3

Alarms

The **Stride** SE2 series switches provide a variety of configurable alarms.

The Alarm LED on the front of the switch will be ON when the following Alarm conditions are Enabled and True:

Power Alarm – Note that when Enabled the Power Alarm is True when EITHER Power 1 OR Power 2 is in the Power-Off state.

Port Alarm – True when a port is Disconnected or there is an abnormal connection.

AD-Ring Alarm – Note that only the MASTER station of an AD-Ring supports the AD-Ring Alarm.

The alarm status for all ENABLED alarms will be available for SNMP, Modbus TCP and EtherNet/IP.

All alarms are Disabled by default.