Stride®

SE2 Series

Industrial Ethernet Switches

USER MANUAL

Manual Number: SE2-USER-M

⚡ WARNING ⚡

Thank you for purchasing automation equipment from **Automationdirect.com®**, doing business as, **AutomationDirect**. We want your new automation equipment to operate safely. Anyone who installs or uses this equipment should read this publication (and any other relevant publications) before installing or operating the equipment.

To minimize the risk of potential safety problems, you should follow all applicable local and national codes that regulate the installation and operation of your equipment. These codes vary from area to area and usually change with time. It is your responsibility to determine which codes should be followed, and to verify that the equipment, installation, and operation is in compliance with the latest revision of these codes.

At a minimum, you should follow all applicable sections of the National Fire Code, National Electrical Code, and the codes of the National Electrical Manufacturer's Association (NEMA). There may be local regulatory or government offices that can also help determine which codes and standards are necessary for safe installation and operation.

Equipment damage or serious injury to personnel can result from the failure to follow all applicable codes and standards. We do not guarantee the products described in this publication are suitable for your particular application, nor do we assume any responsibility for your product design, installation, or operation.

Our products are not fault-tolerant and are not designed, manufactured or intended for use or resale as on-line control equipment in hazardous environments requiring fail-safe performance, such as in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, direct life support machines, or weapons systems, in which the failure of the product could lead directly to death, personal injury, or severe physical or environmental damage ("High Risk Activities"). **AutomationDirect** specifically disclaims any expressed or implied warranty of fitness for High Risk Activities.

For additional warranty and safety information, see the Terms and Conditions section of our catalog. If you have any questions concerning the installation or operation of this equipment, or if you need additional information, please call us at 770-844-4200.

This publication is based on information that was available at the time it was printed. At **AutomationDirect** we constantly strive to improve our products and services, so we reserve the right to make changes to the products and/or publications at any time without notice and without any obligation. This publication may also discuss features that may not be available in certain revisions of the product.

Trademarks

This publication may contain references to products produced and/or offered by other companies. The product and company names may be trademarked and are the sole property of their respective owners. **AutomationDirect** disclaims any proprietary interest in the marks and names of others.

ADVERTENCIA

Gracias por comprar equipo de automatización de **Automationdirect.com**®. Deseamos que su nuevo equipo de automatización opere de manera segura. Cualquier persona que instale o use este equipo debe leer esta publicación (y cualquier otra publicación pertinente) antes de instalar u operar el equipo.

Para reducir al mínimo el riesgo debido a problemas de seguridad, debe seguir todos los códigos de seguridad locales o nacionales aplicables que regulan la instalación y operación de su equipo. Estos códigos varian de área en área y usualmente cambian con el tiempo. Es su responsabilidad determinar cuales códigos deben ser seguidos y verificar que el equipo, instalación y operación estén en cumplimiento con la revisión mas reciente de estos códigos.

Como mínimo, debe seguir las secciones aplicables del Código Nacional de Incendio, Código Nacional Eléctrico, y los códigos de (NEMA) la Asociación Nacional de Fabricantes Eléctricos de USA. Puede haber oficinas de normas locales o del gobierno que pueden ayudar a determinar cuales códigos y normas son necesarios para una instalación y operación segura.

Si no se siguen todos los códigos y normas aplicables, puede resultar en daños al equipo o lesiones serias a personas. No garantizamos los productos descritos en esta publicación para ser adecuados para su aplicación en particular, ni asumimos ninguna responsabilidad por el diseño de su producto, la instalación u operación.

Nuestros productos no son tolerantes a fallas y no han sido diseñados, fabricados o intencionados para uso o reventa como equipo de control en línea en ambientes peligrosos que requieren una ejecución sin fallas, tales como operación en instalaciones nucleares, sistemas de navegación aérea, o de comunicación, control de tráfico aéreo, máquinas de soporte de vida o sistemas de armamentos en las cuales la falla del producto puede resultar directamente en muerte, heridas personales, o daños físicos o ambientales severos ("Actividades de Alto Riesgo"). **Automationdirect.com** específicamente rechaza cualquier garantía ya sea expresada o implicada para actividades de alto riesgo.

Para información adicional acerca de garantía e información de seguridad, vea la sección de Términos y Condiciones de nuestro catálogo. Si tiene alguna pregunta sobre instalación u operación de este equipo, o si necesita información adicional, por favor llámenos al número 770-844-4200 en Estados Unidos. Esta publicación está basada en la información disponible al momento de impresión. En **Automationdirect.com** nos esforzamos constantemente para mejorar nuestros productos y servicios, así que nos reservamos el derecho de hacer cambios al producto y/o a las publicaciones en cualquier momento sin notificación y sin ninguna obligación. Esta publicación también puede discutir características que no estén disponibles en ciertas revisiones del producto.

Marcas Registradas

Esta publicación puede contener referencias a productos producidos y/u ofrecidos por otras compañías. Los nombres de las compañías y productos pueden tener marcas registradas y son propiedad única de sus respectivos dueños. Automationdirect.com, renuncia cualquier interés propietario en las marcas y nombres de otros.

⚡ AVERTISSEMENT ⚡

Nous vous remercions d'avoir acheté l'équipement d'automatisation de **Automationdirect.com**®, en faisant des affaires comme, **AutomationDirect**. Nous tenons à ce que votre nouvel équipement d'automatisation fonctionne en toute sécurité. Toute personne qui installe ou utilise cet équipement doit lire la présente publication (et toutes les autres publications pertinentes) avant de l'installer ou de l'utiliser.

Afin de réduire au minimum le risque d'éventuels problèmes de sécurité, vous devez respecter tous les codes locaux et nationaux applicables régissant l'installation et le fonctionnement de votre équipement. Ces codes diffèrent d'une région à l'autre et, habituellement, évoluent au fil du temps. Il vous incombe de déterminer les codes à respecter et de vous assurer que l'équipement, l'installation et le fonctionnement sont conformes aux exigences de la version la plus récente de ces codes.

Vous devez, à tout le moins, respecter toutes les sections applicables du Code national de prévention des incendies, du Code national de l'électricité et des codes de la National Electrical Manufacturer's Association (NEMA). Des organismes de réglementation ou des services gouvernementaux locaux peuvent également vous aider à déterminer les codes ainsi que les normes à respecter pour assurer une installation et un fonctionnement sûrs.

L'omission de respecter la totalité des codes et des normes applicables peut entraîner des dommages à l'équipement ou causer de graves blessures au personnel. Nous ne garantissons pas que les produits décrits dans cette publication conviennent à votre application particulière et nous n'assumons aucune responsabilité à l'égard de la conception, de l'installation ou du fonctionnement de votre produit.

Nos produits ne sont pas insensibles aux défaillances et ne sont ni conçus ni fabriqués pour l'utilisation ou la revente en tant qu'équipement de commande en ligne dans des environnements dangereux nécessitant une sécurité absolue, par exemple, l'exploitation d'installations nucléaires, les systèmes de navigation aérienne ou de communication, le contrôle de la circulation aérienne, les équipements de survie ou les systèmes d'armes, pour lesquels la défaillance du produit peut provoquer la mort, des blessures corporelles ou de graves dommages matériels ou environnementaux («activités à risque élevé»). La société **AutomationDirect** nie toute garantie expresse ou implicite d'aptitude à l'emploi en ce qui a trait aux activités à risque élevé.

Pour des renseignements additionnels touchant la garantie et la sécurité, veuillez consulter la section Modalités et conditions de notre documentation. Si vous avez des questions au sujet de l'installation ou du fonctionnement de cet équipement, ou encore si vous avez besoin de renseignements supplémentaires, n'hésitez pas à nous téléphoner au 770-844-4200.

Cette publication s'appuie sur l'information qui était disponible au moment de l'impression. À la société **AutomationDirect**, nous nous efforçons constamment d'améliorer nos produits et services. C'est pourquoi nous nous réservons le droit d'apporter des modifications aux produits ou aux publications en tout temps, sans préavis ni quelque obligation que ce soit. La présente publication peut aussi porter sur des caractéristiques susceptibles de ne pas être offertes dans certaines versions révisées du produit.

Marques de commerce

La présente publication peut contenir des références à des produits fabriqués ou offerts par d'autres entreprises. Les désignations des produits et des entreprises peuvent être des marques de commerce et appartiennent exclusivement à leurs propriétaires respectifs. **AutomationDirect** nie tout intérêt dans les autres marques et désignations.

Stride®

SE2 Series Industrial Ethernet Switches
USER MANUAL

AUTOMATIONDIRECT.com

Please include the Manual Number and the Manual Issue, both shown below, when communicating with Technical Support regarding this publication.

Manual Number:	**SE2-USER-M**
Issue:	**2nd Edition, Revision H**
Issue Date:	**05/2021**

Publication History

Issue	Date	Description of Changes
1st Edition	01/17	Original Issue
2nd Edition	04/17	Added SE2 series Managed Switches.
2nd Edition Rev. A	08/17	Added PoE Switches
2nd Edition Rev. B	03/18	Updated EMI Standards, Added new Unmanaged Switch, minor corrections
2nd Edition Rev. C	11/18	Added SFP attenuation requirements. Added PVLAN example.
2nd Edition Rev. D	06/19	Clarified SE2 unmanaged switches use full wave rectifiers on power inputs.
2nd Edition Rev. E	01/20	Added voltage ranges to specifications tables.
2nd Edition Rev. F	02/20	Added Appendix F: Security Considerations for Control Systems Networks
2nd Edition Rev. G	09/20	Clarified size of Jumbo Frames.
2nd Edition Rev. H	05/21	Merged Com Port Access and CLI Commands Appendices, and corrected CLI commands.

Table of Contents

Chapter 1: Hardware

Chapter 2: Managed Switch Introduction

Chapter 3: Managed Switch Basic Features

Chapter 4: Advanced Network Behavior Features

Chapter 5: Switch Management and Network Information

Appendix A: Default Settings

Appendix B: Console Port Access & CLI Commands

Appendix C: Troubleshooting

Appendix D: Ethernet IP

Appendix E: Modbus TCP

Appendix F: Security Considerations for Control Systems Networks

CHAPTER 1

HARDWARE

In this Chapter...

Introduction

The Purpose of this User's Manual

Thank you for purchasing our **Stride**® SE2 series Industrial Ethernet Switches. This manual describes AutomationDirect.com's **Stride** industrial Ethernet switches, their specifications, included components, and provides you with important information for installation, connectivity and setup. The manual shows you how to install, wire and use the products.

Technical Support

We strive to make our manuals the best in the industry. We rely on your feedback to let us know if we are reaching our goal. If you cannot find the solution to your particular application, or, if for any reason you need technical assistance, please call us at:

770–844–4200

Our technical support group will work with you to answer your questions. They are available Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time. We also encourage you to visit our web site where you can find technical and non-technical information about our products and our company.

http://www.automationdirect.com

If you have a comment, question or suggestion about any of our products, services, or manuals, please let us know.

Conventions Used

*When you see the "notepad" icon in the left-hand margin, the paragraph to its immediate right will be a special note. The word **NOTE:** in boldface will mark the beginning of the text.*

When you see the "exclamation mark" icon in the left-hand margin, the paragraph to its immediate right will be a warning or a caution. This information could prevent injury, loss of property, or even death (in extreme cases). The words WARNING or CAUTION: in boldface will mark the beginning of the text.

General Information

Overview

This user’s manual will help you install and maintain the **Stride** industrial Ethernet switches. Installation of these devices is very easy and they will begin to operate as soon as they are powered up.

Operation

Unlike an Ethernet hub that broadcasts all messages out all ports, these industrial Ethernet switches will intelligently route Ethernet messages only out the appropriate port. The major benefits of this are increased bandwidth and speed, reduction or elimination of message collisions, and deterministic performance when tied with real-time systems.

These industrial Ethernet switches can support 10BaseT (10 Mbps) or 100BaseT (100 Mbps) or 1000BaseT (Gigabit Ethernet) on their RJ45 ports. Each of these ports will independently auto-sense the speed and duplex, mdi/mdix-crossover and polarity allowing you to use patch or crossover cables.

Some models include fiber optic ports, or slots that accept SFP fiber optic transceivers.

Security Considerations

When implementing any method of remote access to your equipment, you need to consider the security exposure in order to minimize the risks to your processes and your equipment. Security should always be carefully evaluated for each installation. Refer to “Appendix F: Security Considerations for Control Systems Networks” for more information.

Installation and Hazardous Area Warnings

WARNING: These products should not be used to replace proper safety interlocking. No software-based device (or any other solid-state device) should ever be designed to be responsible for the maintenance of consequential equipment or personnel safety. In particular, *AutomationDirect.com* disclaims any responsibility for damages, either direct or consequential, that result from the use of this equipment in any application. All power, input and output (I/O) wiring must be in accordance with Class I, Division 2 wiring methods and in accordance with the authority having jurisdiction.

WARNING (EXPLOSION HAZARD)	SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS 1, DIVISION 2 (ZONE 2).
WARNING (EXPLOSION HAZARD)	WHEN IN HAZARDOUS LOCATIONS, DISCONNECT POWER BEFORE REPLACING OR WIRING UNITS.
WARNING (EXPLOSION HAZARD)	DO NOT DISCONNECT EQUIPMENT UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NONHAZARDOUS.
WARNING (EXPLOSION HAZARD)	IN HAZARDOUS OR POTENTIALLY HAZARDOUS LOCATIONS, DO NOT SEPARATE ANY PART OF THE UNIT WHEN ENERGIZED. USE THE UNIT FOR INTERNAL CONNECTIONS ONLY.

FCC Statement

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

***NOTE:** Modifications to this equipment will void the user's authority to operate the equipment.*

Product Overview Stride SE2 Unmanaged Models

Stride SE2 Unmanaged Models

Part Number	Number of Ports				Input power (max.)	Operating Temp	Agency Approvals
	M12 10/100	RJ45 10/100	RJ45 GbE	Fiber			
SE2-MC2U-C1-T	–	1	–	1 SC	3.4 W	-40 to +75°C (-40 to +167°F)	UL/cUL 61010-1 and 61010-2-201, Class 1, Div. 2, Groups A, B, C, D, (UL file #E200031) CE
SE2-MC2U-T1-T	–	1	–	1 ST			
SE2-SW5U	–	5	–	–		-10 to +60°C (+14 to +140°F)	
SE2-SW5U-T	–	5	–	–		-40 to +75°C (-40 to +167°F)	
SE2-SW5UG-T	–	–	5	–	4.5 W		
SE2-SW5U-1C1-T	–	4	–	1 SC	3.4 W		
SE2-SW5U-1T1-T	–	4	–	1 ST			
SE2-SW8U	–	8	–	–	4.6 W	-10 to +60°C (+14 to +140°F)	
SE2-SW8U-T	–	8	–	–		-40 to +75°C (-40 to +167°F)	
SE2-SW8U-2C1-T	–	6	–	2 SC			
SE2-SW8U-2T1-T	–	6	–	2 ST			
SE2-SW8UG-T	–	–	8	–	10W		
SE2-SW10UG-2P-T	–	–	8	2 GbE SFP*			
SE2-SW16U-T	–	16	–	–	8W		
SE2-SW18U-2G-T	–	16	2	–			
SE2-SW5U-N65-T	5	–	–	–	4.6 W	-40 to +75°C (-40 to +167°F)	CE, UL61010-1, UL61010-2-201
SE2-SW8U-N65-T	8	–	–	–			

NOTE: Optional SFP modules sold separately. Use only Gigabit speed SFPs with SE2-SW10UG-2P-T.

Product Overview Stride SE2 PoE Unmanaged Models

Stride SE2 Unmanaged PoE Models						
Part Number	Number of Ports				Operating Temp	Agency Approvals
	RJ45 10/100	RJ45 GbE	RJ45 10/100 PoE	RJ45 GbE PoE		
SE2-SWP5U-T	1	–	4	–	-40 to +75°C (-40 to +167°F)	UL/cUL 61010-1 and 61010-2-201 Class 1, Div. 2, Groups A, B, C, D, (UL file #E200031) CE
SE2-SWP5UG-T	–	1	–	4		

Product Overview Stride SE2 Managed Models

Stride SE2 Series Managed Models

Part Number	***Ethernet Ports***	***Fiber Ports***	***Input Power (max)***	***Operating Temp***	***Agency Approvals***
SE2-SW8M	8	–	8.1 W	-40 to +75°C (-40 to +167°F)	UL/cUL 508, Class 1, Div. 2, Groups A, B, C, D, (UL file #E200031), CE
SE2-SW8M-2P	6	2 GbE SFP*	9.1 W		
SE2-SW8M-2C1		2 SC	8.1 W		
SE2-SW8M-2T1		2 ST			
SE2-SW16M	16	–	18W		
SE2-SW18MG-2P	16, 2 GbE combo	2 GbE SFP combo*			

**** Optional SFP modules sold separately.***

Switch Accessories

SFP Fiber Transceivers

Stride SFP (small form-factor pluggable) transceivers, also called mini-GBIC, are compact, hot-swappable transceivers with LC fiber connectors. Models SE2-SW8M-2P, SE2SW18MG-2P, and SE2-SW10UG-2P-T have ports that accept these optional transceivers to add fiber connectivity at Fast Ethernet or Gigabit Ethernet speed.

NOTE: *SE2-SW10UG-2P-T will only accept Gigbit speed SFPs.*

SFP Fiber Transceivers				
Part Number	***Mode***	***Data Rate***	***Light Source***	***Max Trans. Distance***
SFP-4K-FMF	Multi-mode	Fast Ethernet (155MB)	1310 nm, FP	4km
SFP-30K-FSF	Single-mode			30 km
SFP-500-GMF	Multi-mode	Gigabit (1.25 GB)	850 nm, VCSEL	550m
SFP-2K-GMF			1310 nm, FP	2km
SFP-10K-GSF	Single-mode			10 km
SFP-30K-GSF			1310 nm, DFB	30 km

Mounting Brackets

SE2-PM1 and SE2-PM3 panel mounting brackets allow DIN rail mount models of **Stride** SE2 series Ethernet switches to be mounted to a panel or an appropriate flat surface.

- SE2-PM1 is compatible with SE2-SW5Ux, SE2-SW8U-x, and SE2-MCx
- SE2-PM3 is compatible with SE2-SWPx, SE2-SW8UG-T, SE2-SW10UG-2P-T, SE2-SW16U-T, SE2-SW18U-2G-T and all SE2 managed switches.

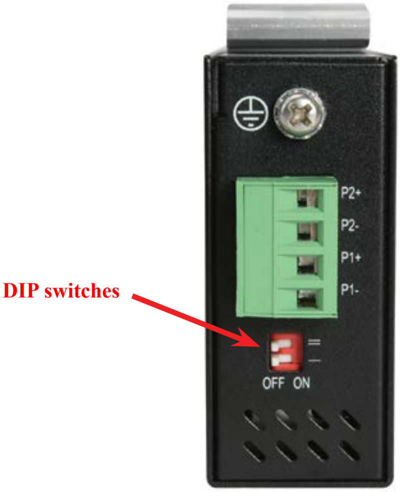
See the **Installation, Optional Panel Mounting** section later in this chapter for specific instructions.

DIP Switch (Unmanaged DIN rail mounted switches)

DIP switch I enables the broadcast storm protection feature on the unmanaged DIN rail mounted switches. A broadcast storm is usually caused by a loop in the network and results in network traffic interruption. The broadcast storm protection feature is especially useful in a more complex network of many unmanaged switches, particularly when cables are disconnected and reconnected frequently.

DIP switch II provides different functions based on the model.

- DIP switch II - GbE switches - ON enables Jumbo frame support
- DIP switch II is not used on other switches.

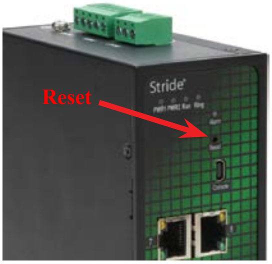


Reset (Managed Switches)

The switch can be reset (power cycle) by pressing the RESET button on the face of the switch for 1-3 seconds.

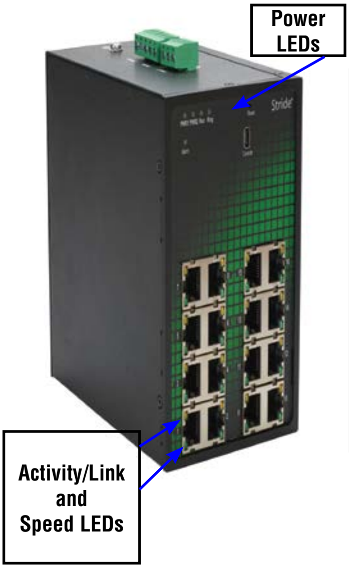
The switch will be RESET to FACTORY DEFAULT by pressing the RESET button on the face of the switch for 5 seconds.

The switch may also be reset or restored to factory defaults via the switch management interface.

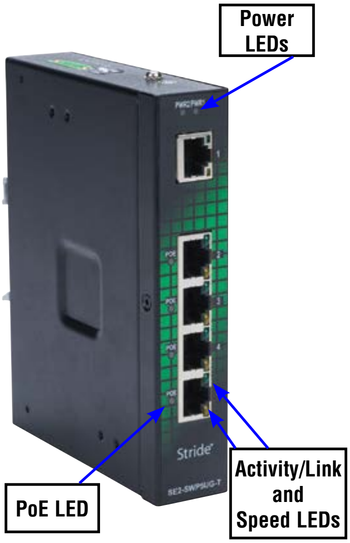


LED Indicators

LEDs on DIN rail Mounted Models



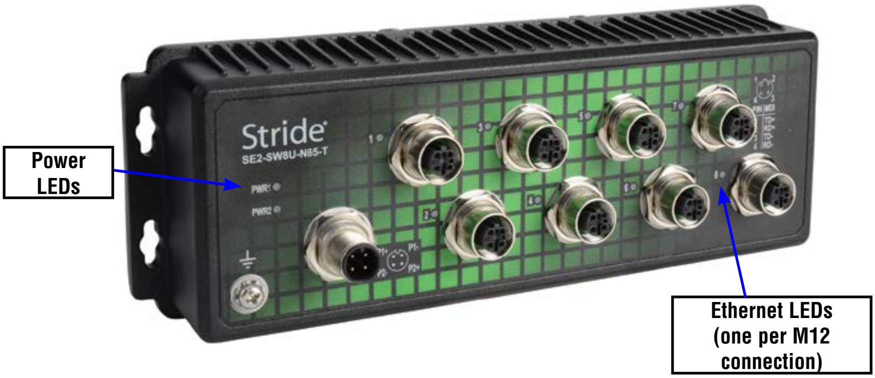
Communication LEDs		
ACT/LNK LED	***On***	Indicates that there is a proper Ethernet connection (Link) between the port and another Ethernet device, but no communications activity is detected.
	Blinking	Indicates that there is a proper Ethernet connection (Link) between the port and another Ethernet device, and that there is communications activity.
	Off	Indicates that there is not a proper Ethernet connection (Link) between the port and another Ethernet device. Make sure the cable has been plugged securely into the ports at both ends.
Speed LED 10/100 Models	***On***	A 100 Mbps (100BaseT) connection is detected.
	Off	A 10 Mbps (10BaseT) connection is detected.
Speed LED 10/100/1000 Models	***On***	A 1000 Mbps (1000BaseT) connection is detected
	Off	A 100 or 10 Mbps (100BaseT or 10BaseT) connection is detected



Front Panel LEDs		
RUN *	***On***	CPU is running abnormally or the switch is starting
	Blinking (1Hz)	CPU is running normally
	Off	CPU is not running
Alarm *	***On***	System alarm
	Off	No system alarm
PWR1 LED	***On***	Power 1 connected and operational
	Off	Power 1 no voltage
PWR2 LED	***On***	Power 2 connected and operational
	Off	Power 2 no voltage
RING *	***On***	Master (AD-Ring mode) / Root (ADP mode)
	Blinking	Slave (AD-Ring mode) / B-Root (ADP mode)
	Off	No ring mode
PoE**	***On***	Port is providing power
	Off	Port is not providing power

* Managed switches only
** PoE switches only

LEDs on IP65 Models



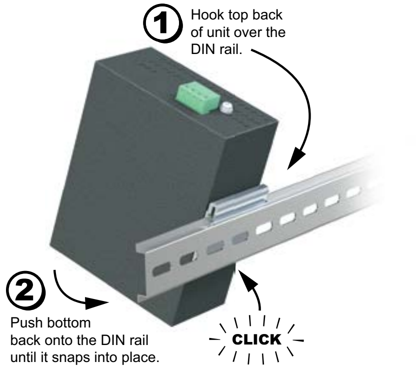
IP65 Models Front Panel LEDs		
Power 1 LED	***On***	Power 1 connected and operational
	Off	Power 1 no voltage
Power 2 LED	***On***	Power 2 connected and operational
	Off	Power 2 no voltage
Ethernet port connection status LED	***On***	Ethernet port connected
	Blinking	Ethernet port active
	Off	Ethernet port no connection

Installation, DIN Rail Mounting

Stride SE2 series switches can be snapped onto a standard 35 mm x 7.5 mm height DIN rail (Standard: CENELEC EN50022) and can be mounted either vertically or horizontally. See **Installation, IP65 Switches Panel Mounting** later in this chapter for mounting IP65 rated switches. Allow 2cm (0.79 in) of clearance between the SE2 switch and other equipment on the DIN rail, side to side and top to bottom.

NOTE: *Make sure to allow enough room to route your Ethernet copper or fiber optic cables.*

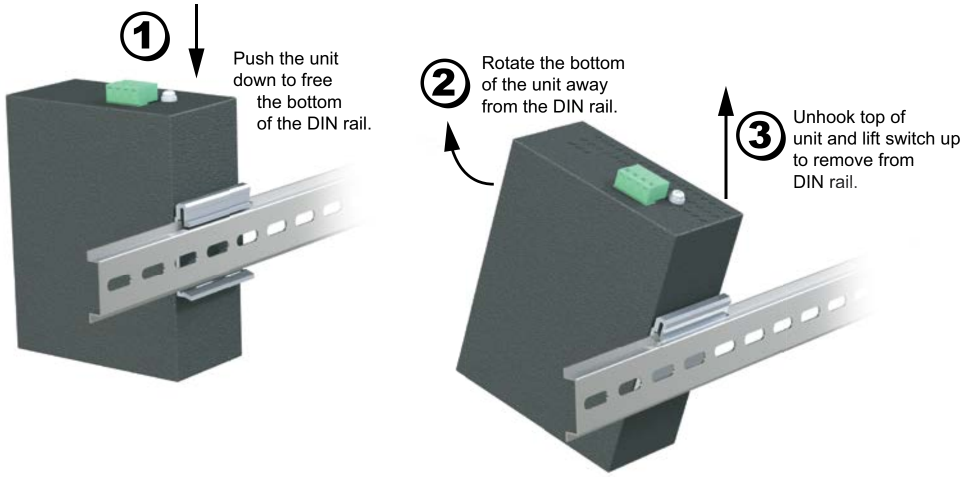
DIN rail installation steps (All Models):



1 Hook top back of unit over the DIN rail.

2 Push bottom back onto the DIN rail until it snaps into place.

DIN rail removal steps (Unmanaged Models):

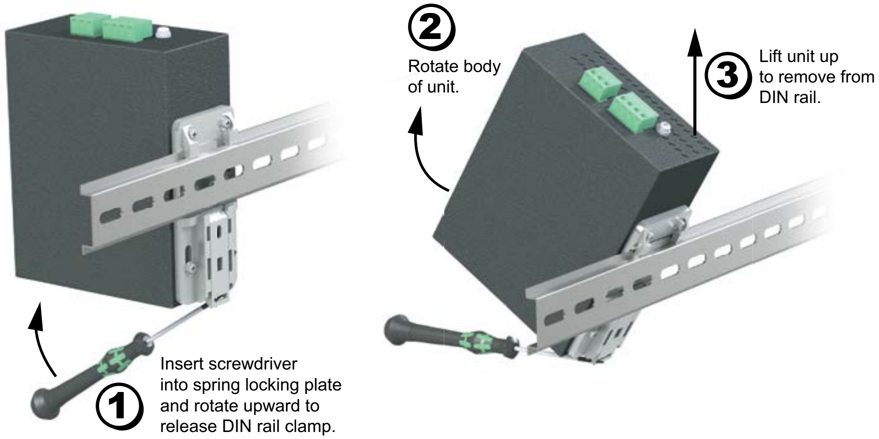


1 Push the unit down to free the bottom of the DIN rail.

2 Rotate the bottom of the unit away from the DIN rail.

3 Unhook top of unit and lift switch up to remove from DIN rail.

DIN rail removal steps (Unmanaged Models):

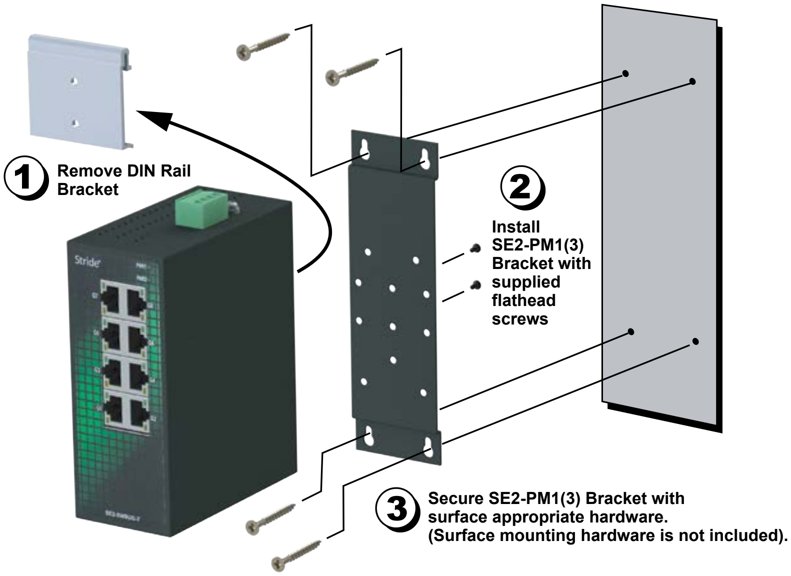

2
Rotate body of unit.
3
Lift unit up to remove from DIN rail.
1
Insert screwdriver into spring locking plate and rotate upward to release DIN rail clamp.

Installation, Optional Panel Mounting

Stride SE2 Din rail series switches can be panel mounted with the addition of the optional panel mounting brackets SE2-PM1 or SE2-PM3.

- SE2-PM1 is compatible with SSE2-SW5Ux, SE2-SW8U-x, and SE2-MCx
- SE2-PM3 is compatible with SE2-SWPx, SE2-SW8UG-T, SE2-SW10UG-2P-T, SE2-SW16U-T, SE2-SW18U-2G-T and all SE2 managed switches.

Mounting Instructions



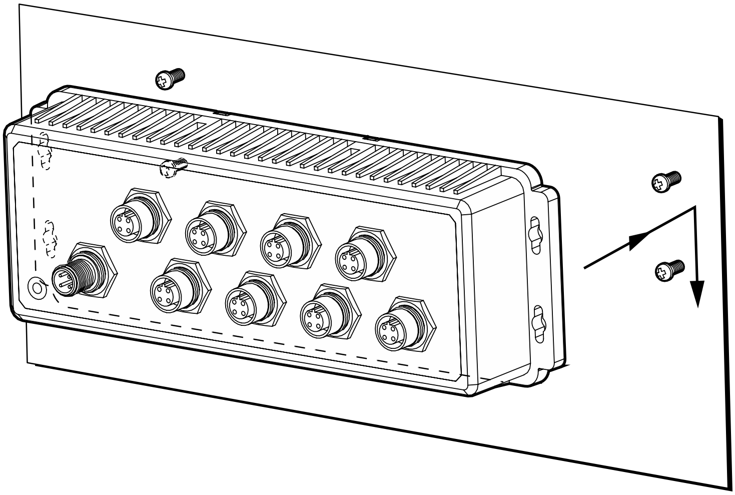
1 Remove DIN Rail Bracket

2 Install SE2-PM1(3) Bracket with supplied flathead screws

3 Secure SE2-PM1(3) Bracket with surface appropriate hardware. (Surface mounting hardware is not included).

Installation, IP65 Switches Panel Mounting

IP65 rated switches are designed to be panel mounted vertically or horizontally using the steps below.



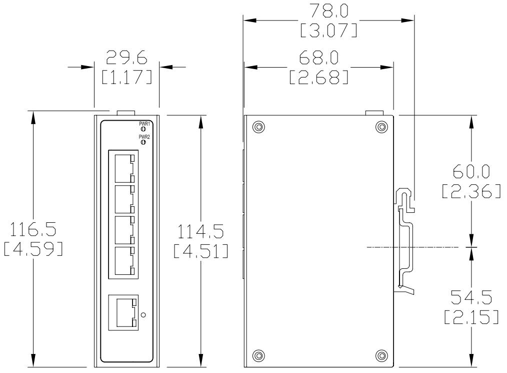
Panel mounting steps:

- Use the dimensional drawing to locate (4) mounting screws on the panel. Recommended screws are #4-40 pan head.
- Install the screws in the panel leaving a gap of 5mm between the head of the screw and the panel.
- Align the (4) mounting holes with the screw heads and move the switch on to the (4) mounting screws. Allow the switch to slide into position.
- Tighten the four mounting screws.

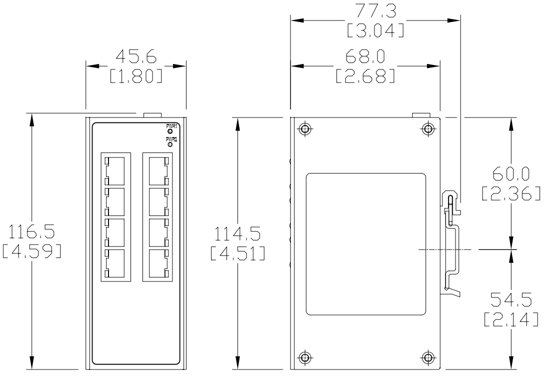
Dimensional Drawings

NOTE: *Allow 20mm (0.79 in) clearance around each switch for proper cooling.*

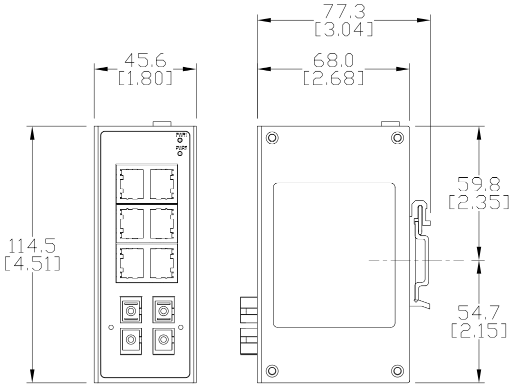
Dimensions mm / [inches]



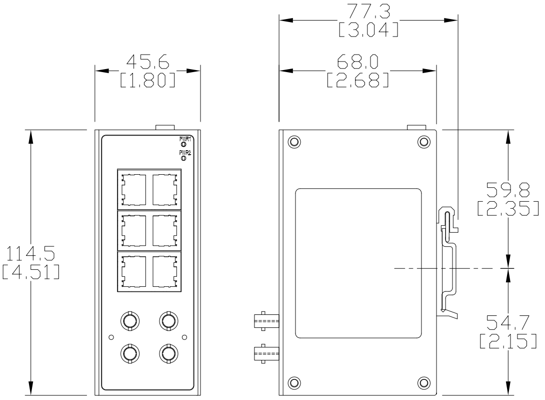
SE2-MC2U-C1-T, SE2-MC2U-T1-T, SE2-SW5U, SE2-SW5U-T, SE2-SW5UG-T, SE2-SW5U-1C1-T, SE2-SW5U-1T1-T



SE2-SW8U SE2-SW8U-T



SE2-SW8U-2C1-T

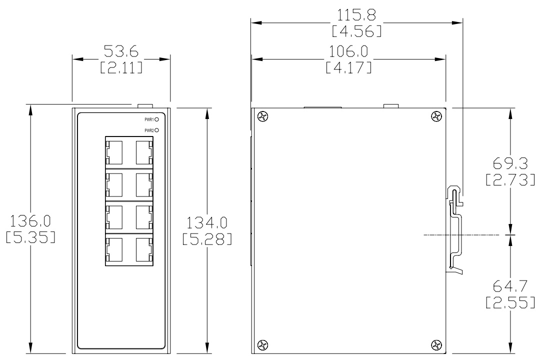


SE2-SW8U-2T1-T

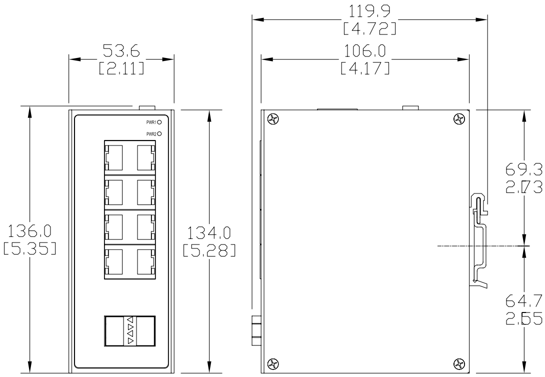
Dimensional Drawings (cont'd)

NOTE: *Allow 20mm (0.79") clearance around each switch for proper cooling.*

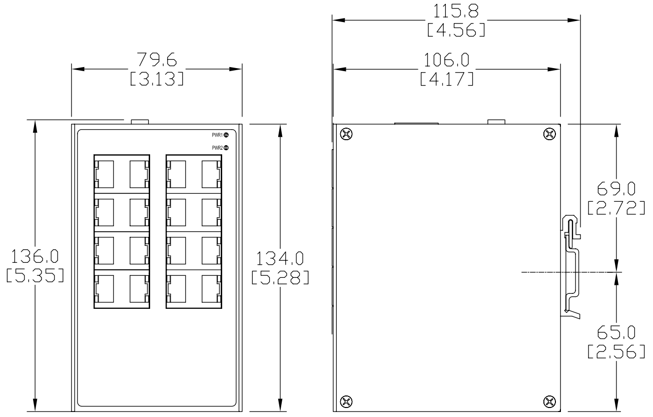
Dimensions
mm / [inches]



SE2-SW8UG-T



SE2-SW10UG-2P-T

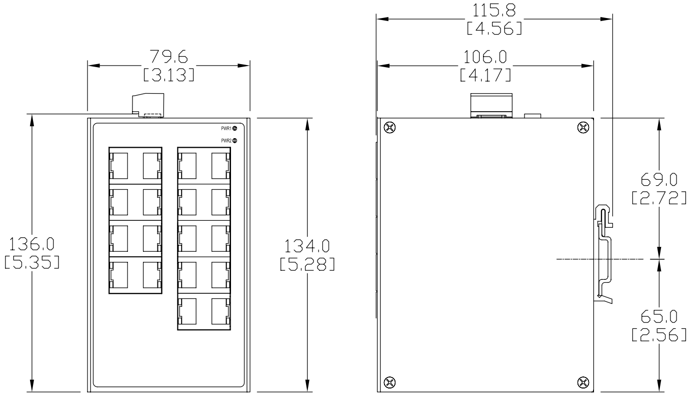


SE2-SW16U-T

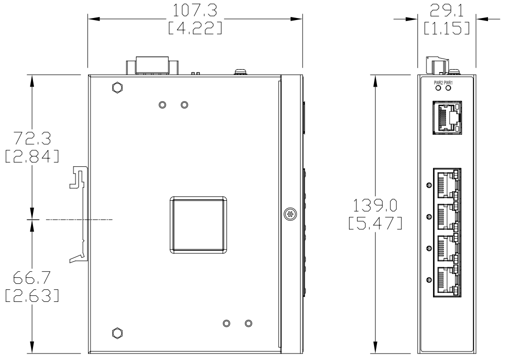
Dimensional Drawings (cont'd)

NOTE: *Allow 20mm (0.79") clearance around each switch for proper cooling.*

Dimensions
mm / [inches]



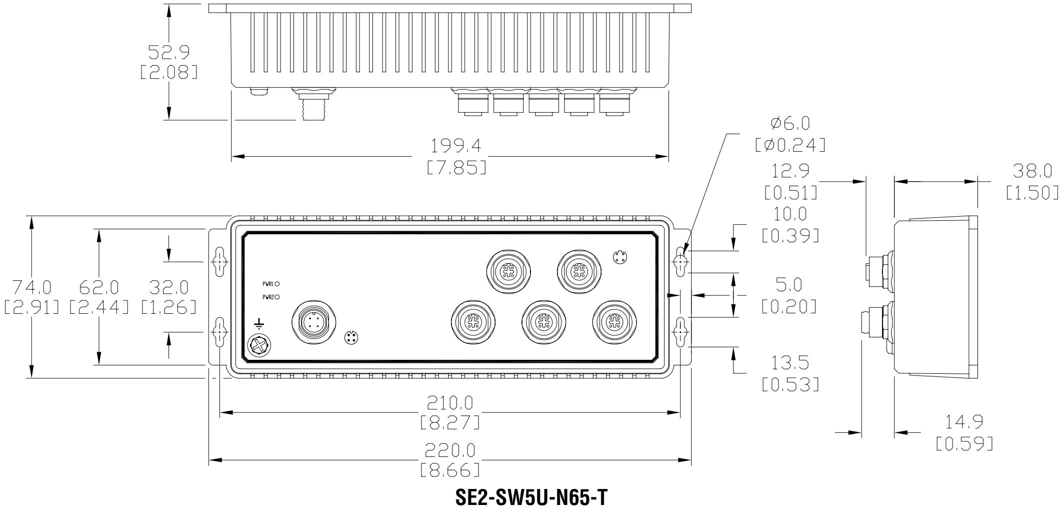
SE2-SW18U-2G-T



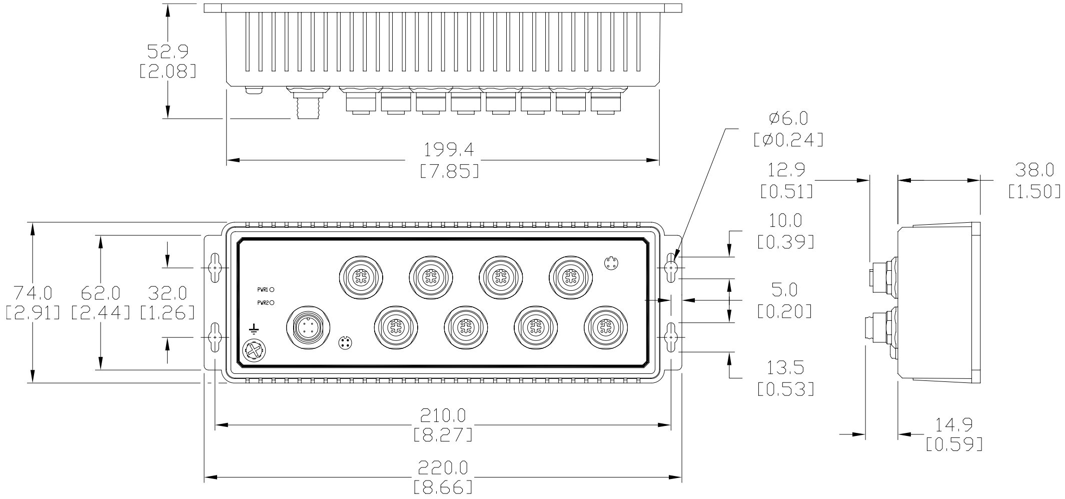
SE2-SWP5U-T
SE2-SWP5UG-T

Dimensional Drawings (cont'd)

Dimensions mm / [inches]



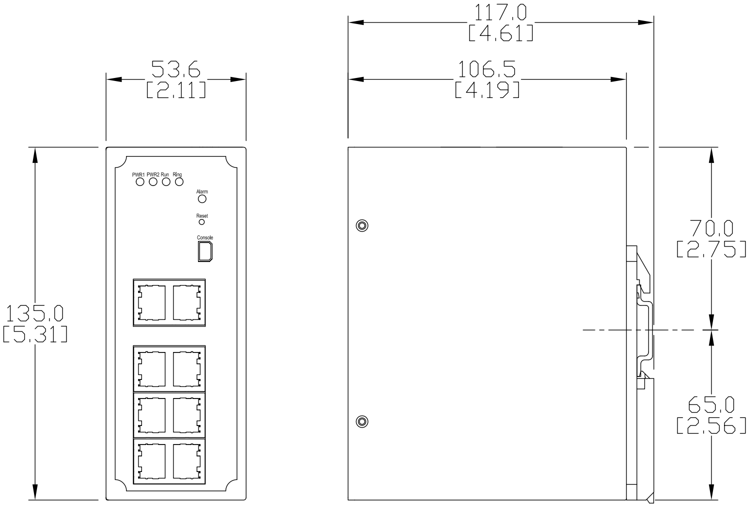
SE2-SW5U-N65-T



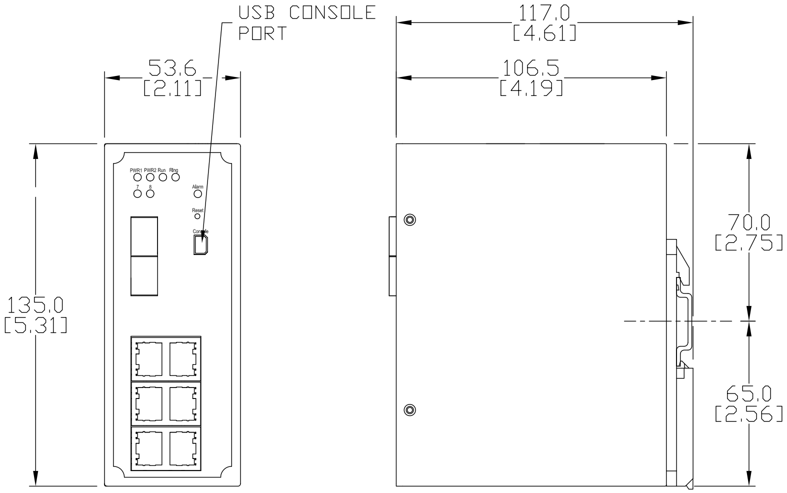
SE2-SW8U-N65-T

Dimensional Drawings (cont'd)

Dimensions
mm / [inches]



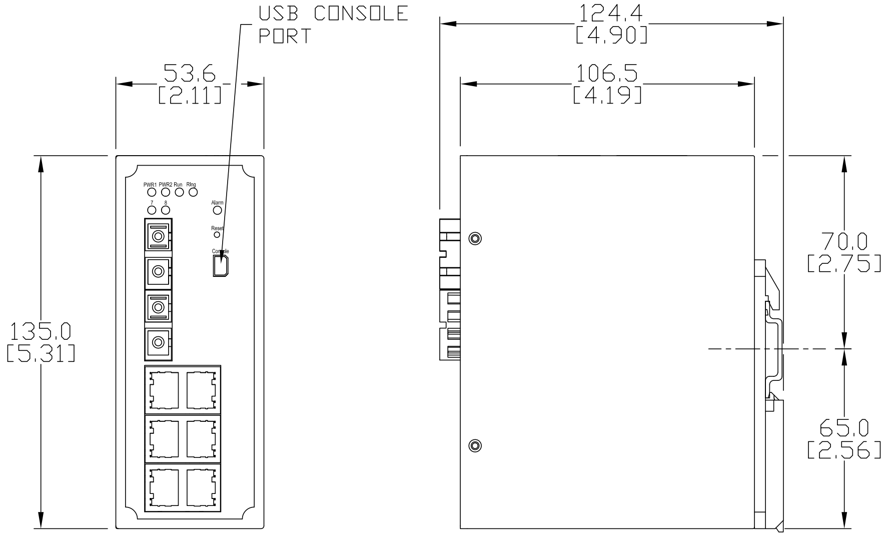
SE2-SW8M



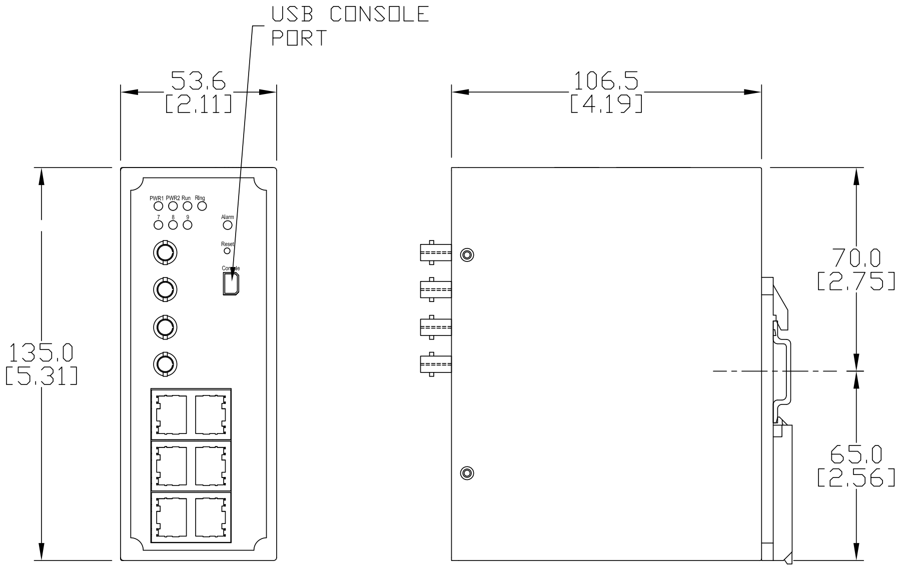
SE2-SW8M-2P

Dimensional Drawings (cont'd)

Dimensions
mm / [inches]



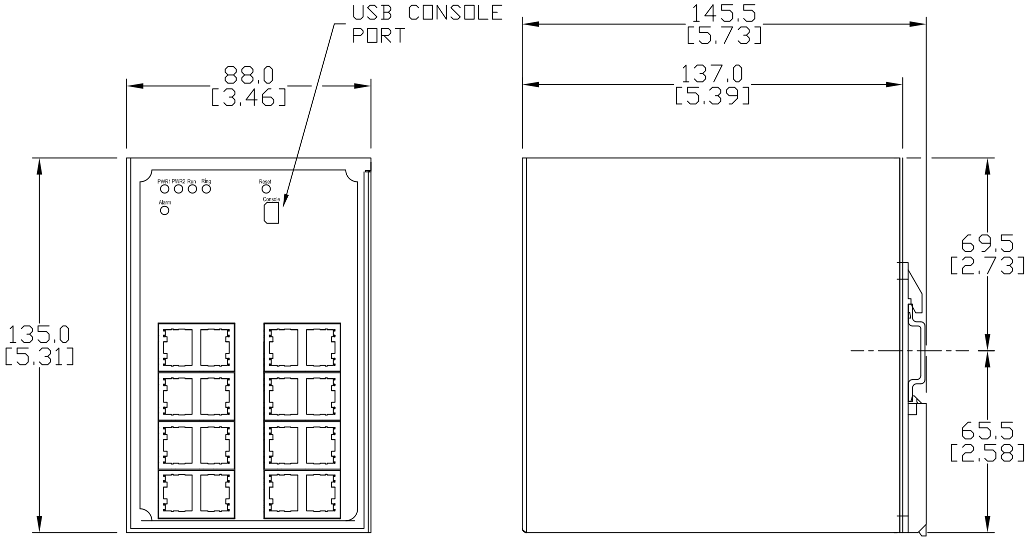
SE2-SW8M-2C1



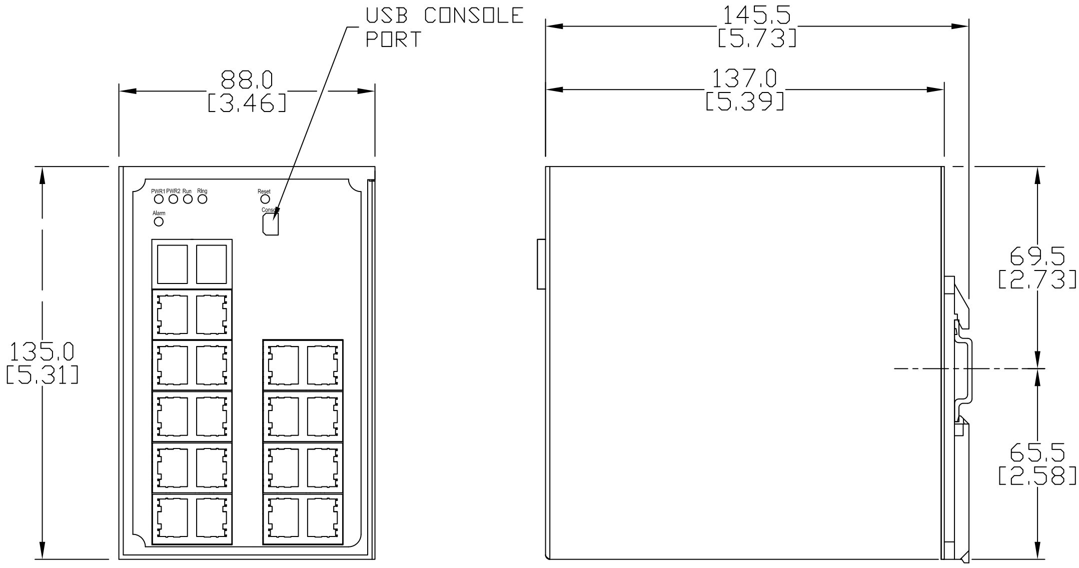
SE2-SW8M-2T1

Dimensional Drawings (cont'd)

Dimensions
mm / [inches]



SE2-SW16M

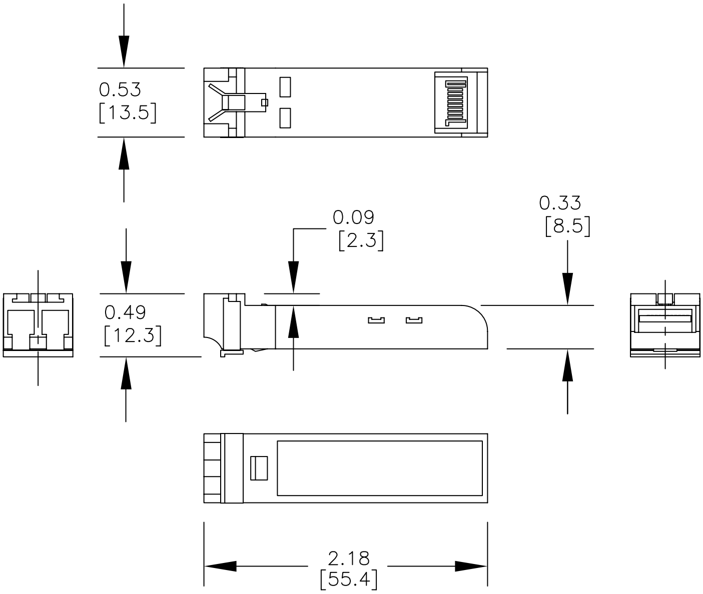


SE2-SW18MG-2P

Dimensional Drawings (cont'd)

Dimensions for SFP Transceiver Modules

Dimensions
mm / [inches]



SFP-4K-FMF, SFP-30K-FSF, SFP-500-GMF, SFP-2K-GMF, SFP-10K-GSF and SFP-30K-GSF

Power Wiring

WARNING: Before performing any wiring to these switches make sure…

- The area is currently nonhazardous (especially when working in Class 1, Div 2 or Zone 2 hazardous locations).
- Power is off to the switch
- The screw terminal block is unplugged. This is especially important on the aluminum housed units. Connecting or disconnecting wires to the screw block when it's in place and power is turned on can allow the screwdriver to short the power to the case.

Unmanaged non-PoE Models (DIN rail mount)

The switch can be powered from the same source that is used to power your other devices. To maintain the UL listing, this must be a Class 2 power supply. 12, 24 or 48 VDC or 24VAC needs to be applied between the P1+ terminal and the P1- terminal as shown below. The chassis screw terminal should be tied to panel or chassis ground. To reduce down time resulting from power loss, the switch can be powered redundantly with a second power supply as shown below. The switch is equipped with reverse power protection, but care should be taken to connect the positive and negative terminals correctly.

A recommended DC power supply is **AutomationDirect.com** part number PSL-24-030.

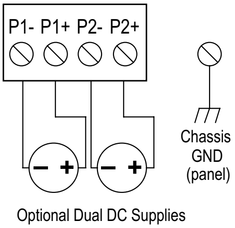
Power Details	
Power Input	Redundant Input Terminals
Input Voltage	Class 2 Power Supply: 12-48 VDC, 18-30 VAC*
Input Voltage Range	9-60 VDC, 18-30 VAC
Reverse Power Protection	Yes

Wire Size and Torque	24-12 AWG, max wire length 3m (9.84 ft);
	Wire strip length 7mm;
	Torque: 4.5-5.0 lb·in (0.51-0.75 N·m)

Power Consumption	Refer to Models tables on previous pages in this chapter.

** The SE2 series unmanaged switches use a full wave rectifier.*

Redundant DC Power



Unmanaged PoE Switches

NOTE: *In order to source power (PSE), a PoE switch must be supplied with 48-58 VDC. When supplied with 12-24 VDC, the switch will communicate properly via Ethernet but will not source power by PoE to a connected device (PD).*

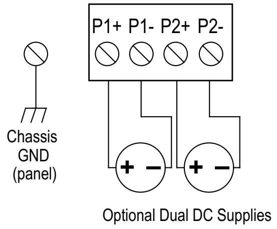
The switch can be powered from the same source that is used to power your other devices. To maintain the UL listing, this must be a Class 2 power supply. 48 VDC must be applied between the P1+ terminal and the P1- terminal as shown.

The chassis screw terminal should be tied to panel or chassis ground. To reduce down time resulting from power loss, the switch can be powered redundantly with a second power supply as shown below. The switch is equipped with reverse power protection, but care should be taken to connect the positive and negative terminals correctly.

A recommended DC power supply is **AutomationDirect.com** part number PSB48-120S.

Power Details	
Power Input	Redundant Input Terminals
	Class 2 Power Supply:
Input Voltage	12 or 24VDC for Ethernet communications only,
	48-58 VDC for PoE (15.4 W per port)
	54-58 VDC for PoE+ (30W per port)
Reverse Power Protection	Yes
Wire Size and Torque	24-16 AWG, max wire length 3m (9.84 ft);
	Wire strip length 7mm;
	Torque: 1.77 lb·in (0.20 N·m)
Power Consumption	switch only = 3W
Power Budget	Ensure power supply to the switch is sized adequately to account for powered devices (PD).
	switch plus PDs = 123 W max
Ground Connection	< 5Ω
	18 - 14 AWG

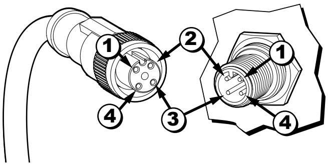
Redundant DC Power



NOTE: *Although the IEEE 802.3af/at standards require the PD to be insensitive to the polarity of the power supply, care should be taken to confirm that the connected PD is fully compliant to the standard. If the connected PD is sensitive to the power polarity, select an appropriate Ethernet cable, straight through or crossover, to meet the requirements of the connected PD.*

M12 Connector Equipped Models

The switch can be powered from the same source that is used to power your other devices. To maintain the UL listing, this must be a Class 2 power supply. 12, 24 or 48 VDC or 24VAC (the SE2 series unmanaged switches use a full wave rectifier) needs to be applied through an M12 (A coded, female, 4-pin) connector as shown in the chart below. The chassis ground screw located on the front of the switch housing should be tied to panel or chassis ground. To reduce down time resulting from power loss, the switch can be powered redundantly with a second power supply as shown in the chart below. The switch is equipped with reverse power protection, but care should be taken to connect the positive and negative terminals correctly.



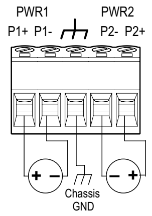
Power Port Pin Definitions			
Pin		**DC Wiring**	**AC Wiring**
1	P1 -	PWR1: -	PWR1
2	P1 +	PWR1: +	PWR1
3	P2 -	PWR2: -	PWR2
4	P2 +	PWR2: +	PWR2

Managed Switches

The switch can be powered from the same DC source that is used to power your other devices. To maintain the UL listing, this must be a Class 2 power supply. A DC voltage in the range of 12 to 24 VDC needs to be applied between the P1+ terminal and the P1- terminal as shown below. The chassis screw terminal should be tied to panel or chassis ground. To reduce down time resulting from power loss, the switch can be powered redundantly with a second power supply as shown below.

A recommended DC power supply is AutomationDirect.com part number PSL-24-030.

Redundant DC Power



Power Details	
Power Input	Redundant Input Terminals
Input Voltage	Class 2 Power Supply: 12-24 VDC
Input Voltage Range	10.2-27.6 VDC
Reverse Power Protection	Yes

Wire Size and Torque	18-12 AWG, max wire length 3m (9.84 ft);
	Wire strip length 7mm;
	Torque: 3.5 lb·in (0.4 N·m)

Power Consumption	Refer to Models tables on previous pages in this chapter

Communication Ports Wiring

Overview

The industrial Ethernet switches provide connections to standard Ethernet devices such as PLCs, Ethernet I/O, industrial computers and much more. RJ45 or M12 (for IP65 locations) Ethernet ports or fiber/SFP option ports are available depending on model.

Ethernet Wiring

Use data-quality (not voice-quality) twisted pair cable rated category 5e (or better) with standard RJ45 or M12 (D coded, male, 4-pin) connectors. Straight-through or crossover Ethernet cable can be used for all devices the switch is connected to because all the ports are capable of auto-mdi/mdix-crossover detection.

The RJ45 Ethernet port connector bodies on these products are metallic and connected to the Chassis GND terminal. Therefore, shielded cables may be used to provide further protection. To prevent ground loops, the cable shield should be tied to the metal connector body at one end of the cable only. Electrical isolation is also provided on the Ethernet ports for increased reliability.

Duplex Operation

The RJ45 and M12 ports will auto-sense for Full or Half duplex operation.

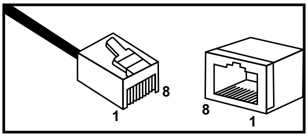
NOTE: *M12 caps (part number: ZP-JBH-CAP) must be used on open (disconnected) ports.*

Ethernet Cable Wiring

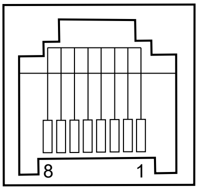
Straight-thru Cable Wiring	
Pin 1	Pin 1
Pin 2	Pin 2
Pin 3	Pin 3
Pin 4	Pin 4
Pin 5	Pin 5
Pin 6	Pin 6
Pin 7	Pin 7
Pin 8	Pin 8

Cross-over Cable Wiring	
Pin 1	Pin 3
Pin 2	Pin 6
Pin 3	Pin 1
Pin 4	Pin 4
Pin 5	Pin 5
Pin 6	Pin 2
Pin 7	Pin 7
Pin 8	Pin 8

NOTE: *For reference only. Either cable wiring will work.*



Ethernet Plug & Connector Pin Positions

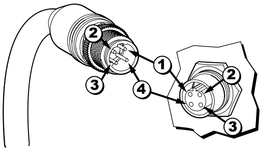


PoE Switch Ethernet Port Pin Definitions			
Pin		***Pin***	
1	V -	5	TRD2 -
2	V +	6	V -
3	V -	7	TRD3 +
4	TRD2 + (transmit / receive data)	8	TRD3 -

Cable Distance

The maximum cable length for 10/100/1000BaseT is 100 meters (328 ft.).

M12 Communication Wiring



Communication Port Pin Definitions	
Pin	***MDI Signal***
1	Transmit Data + (TD+)
2	Receive Data + (RD+)
3	Transmit Data - (TD-)
4	Receive Data - (RD-)

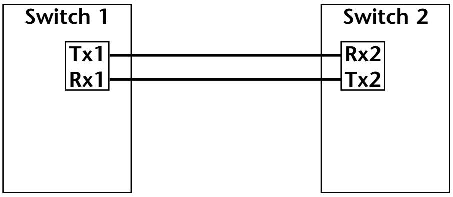
Ethernet Fiber Wiring Guidelines

Some switches include fiber ports, either SC or ST connector, or an SFP option. Refer to the switch specifications for details on the available connection types.

For each fiber port there is a transmit (TX) and receive (RX) signal. When making your fiber optic connections, make sure that the transmit (TX) port of the switch connects to the receive (RX) port of the other device, and the receive (RX) port of the switch connects to the transmit (TX) port of the other device. Use standard fiber optic wiring techniques (not covered by this manual) to make your connections.

It is important to consider the output power and the receiver sensitivity for each end of each fiber connection, especially when the distances that each fiber transceiver in each switch are specified to support differ or when the transceivers (switches) are separated at a distance different than that which the transceivers are specified to support.

It is important to include in your network design an evaluation of the output power and receiver sensitivity based on:



The fiber cable loss (LF) plus attenuator loss (LR) should be greater than the transmit power (TX) minus the receive power (RX).

So, LR = TX1 – RX2 – LF, for the attenuator (LR) placed at RX2 and

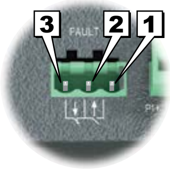
LR = TX2 – RX1 – LF, for the attenuator (LR) placed at RX1.

Verifying Connectivity

After all Ethernet and/or fiber connections are made, check the LEDs corresponding to the ports that each of the devices are connected to. Ensure that for each port that is in use, the LED is on or blinking. If a port LED is off, go back and check for connectivity problems between that port and the network device connected to that port (see prior section on LEDs).

Alarm Wiring

Alarm conditions may be configured in the switch, see Chapter 3 for details. When an alarm condition is true, the normally open contact closes and the normally closed contact opens up.



Technical Specifications

Unmanaged Models

The following specifications refer to these models.

SE2-MC2U-C1-T
SE2-MC2U-T1-T
SE2-SW5U
SE2-SW5U-T
SE2-SW5UG-T
SE2-SW5U-1C1-T
SE2-SW5U-1T1-T
SE2-SW8U
SE2-SW8U-T
SE2-SW8U-2C1-T
SE2-SW8U-2T1-T
SE2-SW8UG-T
SE2-SW10UG-2P-T
SE2-SW16U-T
SE2-SW18U-2G-T

General Specifications	
Operating Mode	Store and forward wire speed switching, non-blocking
Devices Supported	All IEEE 802.3 compliant devices are supported
MAC Addresses	8K for SE2-SWxG-T, SE2-SW16U-T, SE2-SW18U-2G-T 2K
Packet Buffer	1Mbit
Packet Forwarding Rate	0.75 Mpps - SE2-MC2U-x, SE2-SW5U & SE2-SW5U-x 1.2 Mpps - SE2-SW8U-x 7.4 Mpps - SE2-SW5UG-T 14.9 Mpps - SE2-SW8UG-T & SE2-SW10UG-2P-T 5.7 Mpps - SE2-SW16U-T & SE2-SW18U-2G-T
Broadcast Storm Protection*	DIP switch enabled (DIP switch I)
Latency	< 10 µs
Jumbo Frame Support	DIP switch enabled for SE2-SW5UG-T, SE2-SW8UG-T, SE2-SW10UG-2P-T and SE2-SW18U-2G-T only (DIP switch II ON)**
Storage Temperature Range	-40 to +85 °C (-40 to +185 °F)
Humidity (non-condensing)	5 to 95% RH
Environmental Air	No corrosive gases permitted
Vibration, Shock & Freefall	IEC60068-2-6, -27, -32
EMI Emissions	FCC CFR47 Part 15, EN55032/CISPR32, Class A
EMS	IEC61000-4-2 (ESD): +/- 6kV (contact), +/- 8kV (air) IEC61000-4-3 (RS): 10V/m (80MHz ~ 2GHz) IEC61000-4-4 (EFT): Power Port +/- 2kV; Data Port: +/- 1kV IEC61000-4-5 (Surge): Power Port: +/- 1kV/DM, +/- 2kV/CM; Data Port +/- 2kV IEC61000-4-6 (CS): 10V (150kHz ~ 80MHz)
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
Packaging and Protection	Metal case, IP30
Hazardous Locations	ANSI/IS 12.12.01-2015 & CSA 22.2 No. 213-15 (Class I, Div.2) (file #E200031);
Agency Approvals	UL/cUL 61010-1 and 61010-2-201, Class 1, Div. 2, Groups A, B, C, D, (UL file #E200031) CE

**** Broadcast storm threshold value is 2 packets/100ms for 10 Mbps port or 2 packets/10ms for 100 Mbps and 1000 Mbps ports.***

***** DIP switch II is unused on the 10/100 models.***

Unmanaged Models Technical Specifications (cont'd)

Power Details	
Power Input	Redundant Input Terminals
Input Voltage	Class 2 Power Supply: 12-48 VDC, 18-30VAC* 50/60 Hz
Input Voltage Range	9-60 VDC, 18-30 VAC
Reverse Power Protection	Yes
Power Consumption	Refer to Models tables on previous pages in this chapter

**** The SE2 series unmanaged switches use a full wave rectifier.***

RJ45 Ports	
Port Type	Shielded RJ45
Ethernet Compliance	IEEE 802.3i, 802.3u, 802.3x for 10/100 Ethernet IEEE 802.3ab, 802.3z for Gigabit Ethernet
Auto-Crossover	Yes, allows you to use straight-through or crossover wired cables
Auto-Sensing Operation	Yes, full and half duplex
Auto-Negotiating Speed	Yes
Flow Control	Automatic
Cable Requirements	Twisted pair (Cat5e or better) (shielded recommended)
Max. Cable Distance	100 meters

SC/ST Fiber Port: (100BaseFX Multimode)	
100BaseFX Ports	2
Fiber Port Connector	ST or SC, by model
Optimal Fiber Cable	50/125 or 62.5/125 µm
Center Wavelength	1300 nm
Multimode	Links up to 4 km typ. > Transmitter power (dBm): -21 min, -17 typ, -14 max > Receiver sensitivity (dBm): -34 typ, -31 max
Nominal Max. Distance (full duplex)	4 km
Eye Safety (laser)	IEC 60825-1, Class 1; FDA 21 CFR 1040.10 and 1040.11

SFP (Small Form Factor Pluggable) Ports	
Optional SFP modules sold separately. Use only Gigabit speed SFPs with SE2-SW10UG-2P-T.	
Eye Safety	IEC 60825-1, Class 1; FDA 21 CFR 1040.10 and 1040.11

NOTE: *Refer to SFP module specifications for details specific to the SFP installed.*

Unmanaged PoE Models

The following specifications refer to these models.

SE2-SWP5U-T
SE2-SWP5UG-T

General Specifications	
Operating Mode	Store and forward wire speed switching, non-blocking
Devices Supported	All IEEE 802.3 compliant devices are supported
MAC Addresses	2K
Packet Buffer	1Mbit
Packet Forwarding Rate	1.5 Mpps
Broadcast Storm Protection*	DIP switch enabled (DIP switch I)
Latency	< 15 µs
Jumbo Frame	9K
Storage Temperature Range	-40 to +85 °C (-40 to +185 °F)
Humidity (non-condensing)	5 to 95% RH
Environmental Air	No corrosive gases permitted
Vibration, Shock & Freefall	IEC60068-2-6, -27, -32
EMI Emissions	FCC CFR47 Part 15, EN55032/CISPR32, Class A
EMS	IEC61000-4-2 (ESD): +/- 6kV (contact), +/- 8kV (air) IEC61000-4-3 (RS): 10V/m (80MHz ~ 2GHz) IEC61000-4-4 (EFT): Power Port +/- 2kV; Data Port: +/- 1kV IEC61000-4-5 (Surge): Power Port: +/- 1kV/DM, +/- 2kV/CM; Data Port +/- 2kV IEC61000-4-6 (CS): 10V (150kHz ~ 80MHz)
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
Packaging and Protection	Metal case, IP30
Hazardous Locations	ANSI/ISA 12.12.01-2015 & CSA 22.2 No. 213-15 (Class I, Div.2) (file #E200031);
Agency Approvals	UL/cUL 61010-1 and 61010-2-201 Class 1, Div. 2, Groups A, B, C, D, (UL file #E200031) CE

**** Broadcast storm threshold value is 2 packets/100ms for 10 Mbps port or 2 packets/10ms for 100 Mbps and 1000 Mbps ports. DIP switch II is unused.***

Unmanaged PoE Models Technical Specifications (cont'd)

Power Details	
Power Input	Redundant Input Terminals
	Class 2 Power Supply
Input Voltage	12 or 24VDC for Ethernet communications only,
	48-58 VDC for PoE (15.4 W per port)
	54-58 VDC for PoE+ (30W per port)
Reverse Power Protection	Yes
Wire Size and Torque	24-16 AWG, max wire length 3m (9.84 ft);
	Wire strip length 7mm;
	Torque: 1.77 lb·in (0.2 N·m)
Wire Temperature	85°C (185°F) Max.
Power Consumption	switch only = 3W
Power Budget	Ensure power supply to the switch is sized adequately to account for powered devices (PD).
	switch plus PDs = 123 W max
Ground Connection	< 5Ω
	18 - 14 AWG

RJ45 Ports	
Port Type	Shielded RJ45
Ethernet Compliance	IEEE 802.3i, 802.3u, 802.3x for 10/100 Ethernet IEEE 802.3ab, 802.3z for Gigabit Ethernet IEEE 802.3af or 802.3at for PoE
Auto-Crossover	Yes, allows you to use straight-through or crossover wired cables
Auto-Sensing Operation	Yes, full and half duplex
Auto-Negotiating Speed	Yes
Flow Control	Automatic
Cable Requirements	Twisted pair (Cat5e or better) (shielded recommended)
Max. Cable Distance	100 meters

PoE Details	
Max Power per Port	30W at 48-58 VDC
	720mA
	V+ pins 1, 2
	V- pins 3, 6
Power Input	54-58 VDC for PoE+
	48-58 VDC for PoE
PD (Powered Device) Detection	Yes - the switch port will detect the presence of a PoE enabled device before sending power. If a non-PoE device is detected, power will not be sourced on that port but Ethernet connections will be permitted.
PoE Overload Protection	Yes
Reverse Protection	Yes
Redundancy Protection	Yes

Unmanaged IP65 Rated Models

The following specifications refer to these models.

SE-SW5U-N65-T
SE-SW8U-N65-T

General Specifications	
Operating Mode	Store and forward wire speed switching, non-blocking
Devices Supported	All IEEE 802.3 compliant devices are supported
MAC Addresses	2K
Packet Buffer	1Mbit
Packet Forwarding Rate	1.2 Mpps
Latency	< 10 µs
Operating Temperature Range	-40 to +75°C (-40 to +167°F)
Storage Temperature Range	-40 to +85°C (-40 to +185°F)
Humidity (non-condensing)	5 to 95% RH
Pollution Degree	2
Vibration and Shock	IEC60068-2-6, -27, -32
Freefall	IEC60068-2-32
Safety	EN60950-1
EMI Emissions	FCC CFR47 Part 15, EN55032/CISPR32, Class A
EMS	IEC61000-4-2 (ESD): ± 6kV (contact), ± 8kV (air) IEC61000-4-3 (RS): 20V/m (80MHz ~ 2 GHz) IEC61000-4-4 (EFT): Power Port ± 2kV; Data Port: ± 2kV IEC61000-4-5 (Surge): Power Port: ± 1kV/DM, ± 2kV/CM IEC61000-4-6 (CS): 10V (150 kHz ~ 80 MHz) IEC61000-4-8 (Power frequency magnetic field) :50 Hz 100A/m IEC61000-4-9 (Pulsed magnetic field) :300A/m IEC61000-4-29 (Voltage short interruptions) :10ms 100%
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
Packaging and Protection	Metal Case, IP65
Agency Approvals	UL/cUL 61010-1 and UL/cUL 61010-2-201 (UL file #E157382), CE, EN50155, EN50121

Power Details	
Power Input	Redundant Input M12 connector
Input Voltage	Class 2 Power Supply: 12-48 VDC, 18-30VAC* 50/60 Hz
Input Voltage Range	9-60 VDC, 18-30 VAC
Power Input Ports	M12, male, A-coding, 4-pin
Reverse Power Protection	Yes

** The SE2 series unmanaged switches use a full wave rectifier.*

Unmanaged IP65 Rated Models (cont'd)

M12 Ethernet Ports	
10/100BaseT ports	M12, female, D-coding, 4-pin
Ethernet Compliance	IEEE 802.3i, 802.3u, 802.3x
Auto-Crossover	Yes, allows you to use straight-through or crossover wired cables
Auto-Sensing Operation	Yes, full and half duplex
Auto-Negotiating Speed	Yes
Flow Control	Automatic
Cable Requirements	Twisted pair (Cat5 or better) (shielded recommended)
Max. Cable Distance	100 meters
M12 caps (ZP-JBH-CAP) need to be used on open (disconnect) ports.	

Managed Models

The following specifications refer to these models.

SE2-SW8M
SE2-SW8M-2C1
SE2-SW8M-2T1
SE2-SW8M-2P

SE2-SW16M
SE2-SW18MG-2P

General Specifications	
Operating Mode	Store and forward wire speed switching, non-blocking
Devices Supported	All IEEE 802.3 compliant devices are supported
MAC Addresses	8K 16K for SE2-SW8M-2P
Ethernet Protocols Supported	SNMP v1 / v2 / v3, RMON, DHCP, SNTP, TFTP, STP, RSTP, QoS / DS, IGMPv1 / v2, VLAN (tag and port based), HTTP, HTTPS (SSL and TSL), Telnet, SSH and more
Industrial Protocols Supported	Modbus TCP, EtherNet/IP, PROFInet, Foundation Fieldbus HSE and others
Packet Forwarding Rate	1.4 Mpps – SE2-SW8M 1.4 Mpps–SE2-SW8M-2C1 1.4 Mpps–SE2-SW8M-2T1 5.5 Mpps–SE2-SW8M-2P 5.4 Mpps–SE2-SW16M 5.4 Mpps–SE2-SW18MG-2P
Latency	< 10 µs
Operating Temperature Range	-40 to +75°C (-40 to +167°F)
Storage Temperature Range	-40 to +85°C (-40 to +185°F)
Humidity (non-condensing)	5 to 95% RH
Environmental Air	No corrosive gases permitted
Vibration, Shock & Freefall	IEC60068-2-6, -27, -32
EMI Emissions	FCC CFR47 Part 15, EN55032/CISPR32, Class A
EMS	IEC61000-4-2 (ESD): ± 8kV (contact), ± 15kV (air) IEC61000-4-3 (RS): 10V/m (80MHz ~ 2GHz) IEC61000-4-4 (EFT): Power Port ± 4kV; Data Port: ± 2kV IEC61000-4-5 (Surge): Power Port: ± 2kV/DM, ± 4kV/CM; Data Port ± 2kV IEC61000-4-6 (CS): 10V (150kHz ~ 80MHz)
Hazardous Locations	ANSI/ISA 12.12.01-2015 & CSA 22.2 No. 213-15 (Class I, Div.2) (file #E200031);
RoHS and WEEE	RoHS (Pb free) and WEEE compliant
Packaging and Protection	Metal case, IP40
Agency Approvals	UL/cUL 508, CE

Managed Models (cont'd)

Power Details	
Power Input	Redundant Input Terminals
Input Voltage	Class 2 Power Supply: 12-24 VDC
Input Voltage Range	10.2-27.6 VDC
Reverse Power Protection	Yes

Wire Size and Torque	18-12 AWG, max wire length 3m (9.84 ft);
	Wire strip length 7mm;
	Torque: 3.5 lb·in (0.4 N·m)

Power Consumption	Refer to Models table on previous pages in this chapter

RJ45 Ports	
Port Type	Shielded RJ45
Ethernet Compliance	IEEE 802.3i, 802.3u, 802.3x for 10/100 Ethernet IEEE 802.3ab, 802.3z for Gigabit Ethernet
Auto-Crossover	Yes, allows you to use straight-through or crossover wired cables
Auto-Sensing Operation	Yes, full and half duplex
Auto-Negotiating Speed	Yes
Flow Control	Automatic
Cable Requirements	Twisted pair (Cat5e or better) (shielded recommended)
Max. Cable Distance	100 meters

SFP Ports
SFP (pluggable) ports accept Mini-GBIC (SFP) transceivers with a speed of 1000Mbps or 100Mbps
See SFP datasheet for optional fiber transceiver specification

SC or ST Fiber Port: (100BaseFX multimode)	
100BaseFX Ports	2
Fiber Port Connector	ST or SC, by model
Optimal Fiber Cable	50/125 or 62.5/125 µm
Center Wavelength	1300 nm
Multimode	Links up to 4 km typ. > Transmitter power (dBm): -21 min, -17 typ, -14 max > Receiver sensitivity (dBm): -34 typ, -31 max
Nominal Max.Distance (full duplex)	4 km
Eye Safety (laser)	IEC 60825-1, Class 1; FDA 21 CFR 1040.10 and 1040.11

CHAPTER
2

MANAGED SWITCH INTRODUCTION

In this Chapter...

Connecting to the Switch the First Time

The SE2 series managed switches may be managed via a mini-USB console port using CLI, or via Ethernet port using CLI, telnet or web browser.

Information on console port access is provided in Appendix B.

Connecting to the switch for the first time over Ethernet is the recommended means of initial access.

- Default IP Address: 192.168.0.1
- User Name: admin
- Default password: admin

Connect to the switch using a Cat5e or better Ethernet cable.

The default browser access protocol is HTTP, port 80. Added security is available by configuring the switch to use SSL. When configured to use SSL, the IP address must be preceded by “https://” in the address field; for example https://192.168.0.1

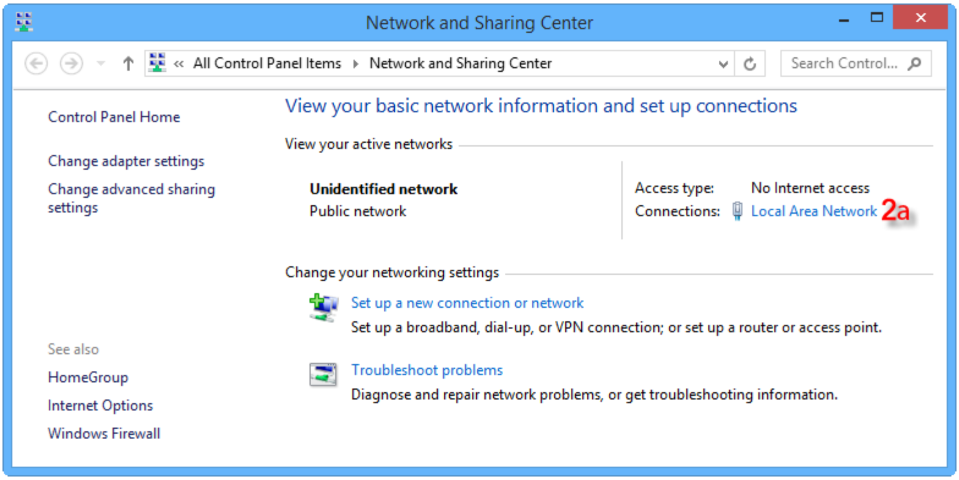
***NOTE**: All configuration changes except IP address and password must be committed to the switch by performing SAVE. If not committed by SAVE, changes will be lost on power cycle. Likewise, changes made by performing LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch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

In order to connect to the switch, the IP address on your PC must be in the same subnet as the IP address on the switch management interface. This section will help you step through:

1. Temporarily changing the PC IP address to an IP address on the same subnet as the switch’s default IP address,
2. Changing the network information for the switch (IP address, subnet mask and default gateway)
3. Changing the PC IP address back to the desired IP address and reconnecting to the switch.

This example shows a switch connected directly to a PC running Windows 8.1.

1. Open Network and Sharing Center:



Network and Sharing Center

All Control Panel Items › Network and Sharing Center

View your basic network information and set up connections

View your active networks

Unidentified network
Public network

Access type: No Internet access
Connections: Local Area Network

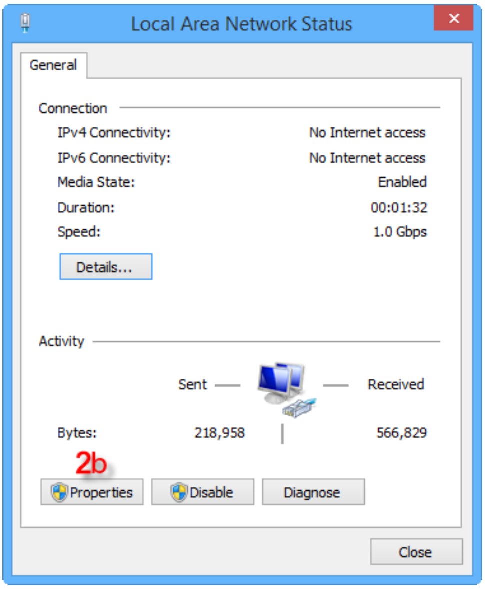
Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

2a. Click on the name of the NIC connected to the switch to open the NIC status window.

2b. Click the Properties button:



Local Area Network Status

General

Connection

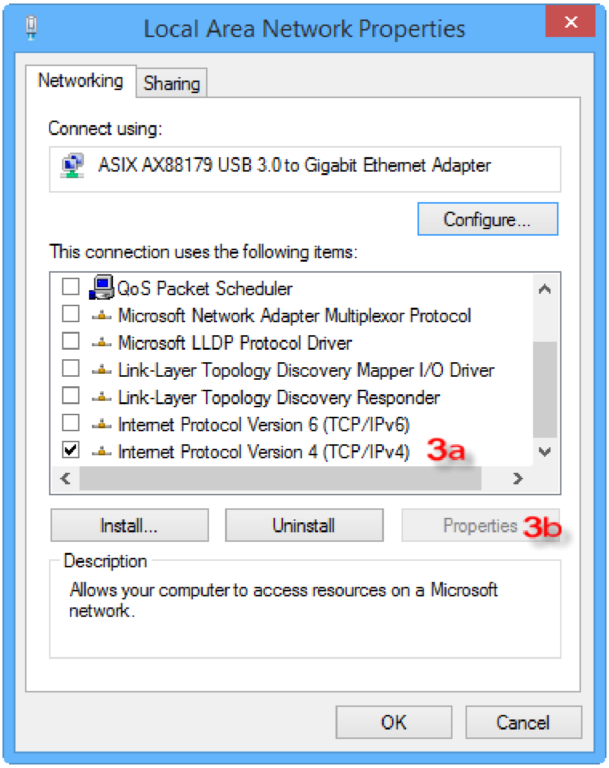
IPv4 Connectivity: No Internet access
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 00:01:32
Speed: 1.0 Gbps

Activity

Sent — Received
Bytes: 218,958 | 566,829

3a. Click to highlight Internet Protocol Version 4 (TCP/IPv4).

3b. Click the Properties button.



Local Area Network Properties

Connect using:

ASIX AX88179 USB 3.0 to Gigabit Ethernet Adapter

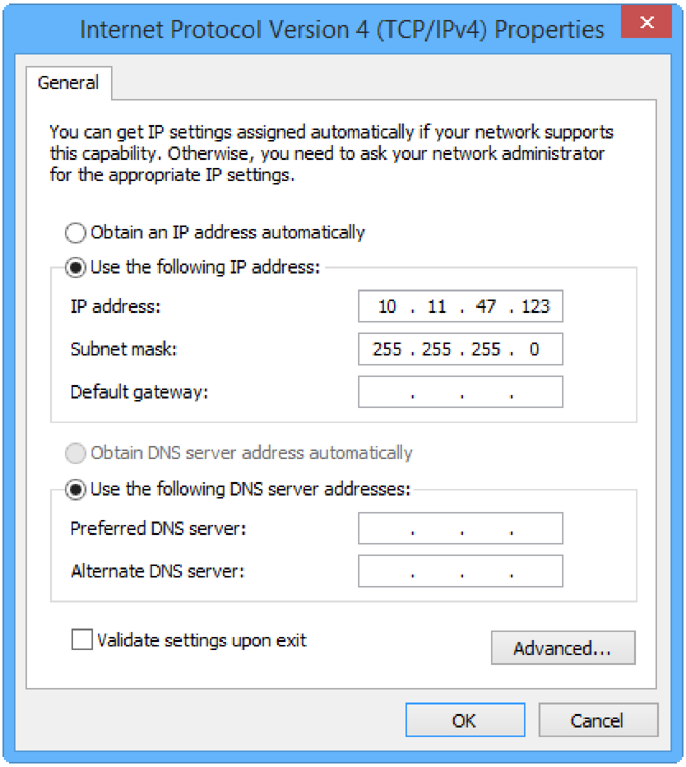
This connection uses the following items:

- ☐ QoS Packet Scheduler
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☐ Microsoft LLDP Protocol Driver
- ☐ Link-Layer Topology Discovery Mapper I/O Driver
- ☐ Link-Layer Topology Discovery Responder
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Allows your computer to access resources on a Microsoft network.

Write down (or screen capture) the existing settings so you can revert to them after we change the switch IP address. For our example, the PC starting IP address is 10.11.47.123, the subnet mask is 255.255.255.0 and there is no default gateway.



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 11 . 47 . 123

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

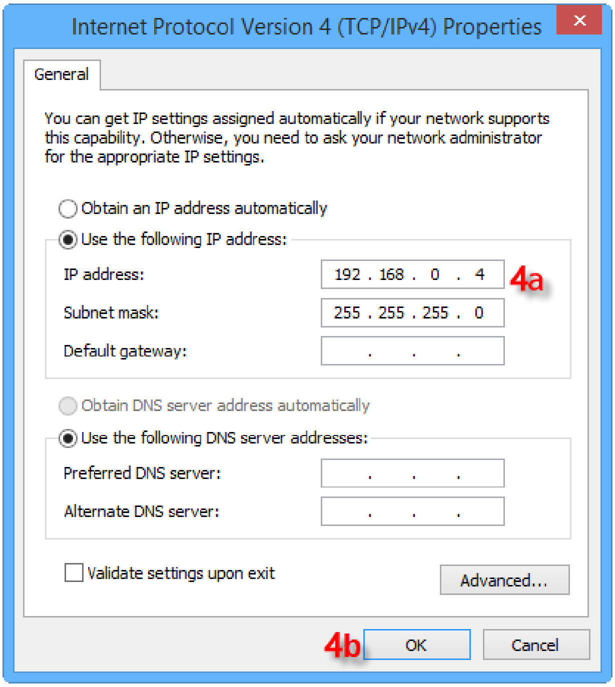
Alternate DNS server: . . .

□ Validate settings upon exit

4a. Select the "Use the following IP address:" radio button, and enter 192.168.0.4 for the IP address and 255.255.255.0 for the subnet mask.

NOTE 1: *Neither the Network Address nor the Broadcast Address for your subnet are valid host addresses. For our example where the Subnet Mask is 255.255.255.0 and the first three octets of the switch address are 192.168.0, neither the PC nor the switch may be assigned 192.168.0.0 or 192.168.0.255 as their IP Address.*
NOTE 2: *No other device connected on this network may share the same address as the switch or the PC (or any other device).*

4b. Click OK on this window, then click OK on the properties window.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 4

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

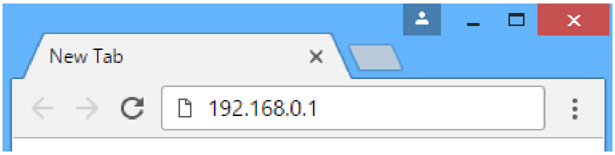
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

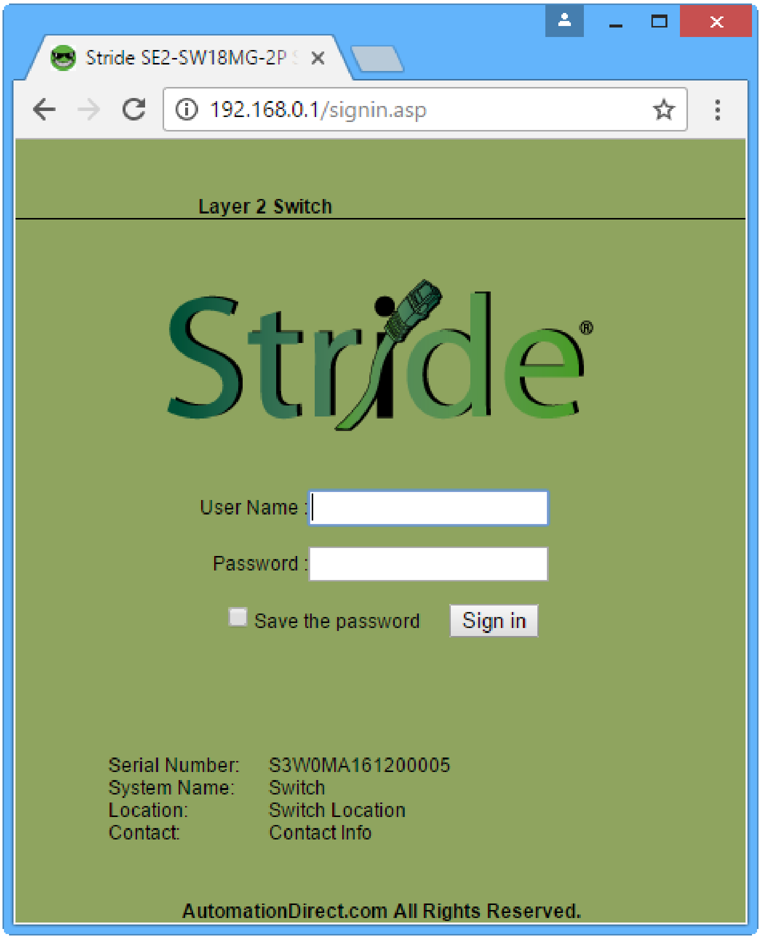
4c. Click CLOSE on the NIC Properties Window.

5. In your browser (we use Google Chrome for this example) type 192.168.0.1 (the switch's IP address) in the address field and Enter.



6. Enter "admin" for the User Name and Password and click Sign In.

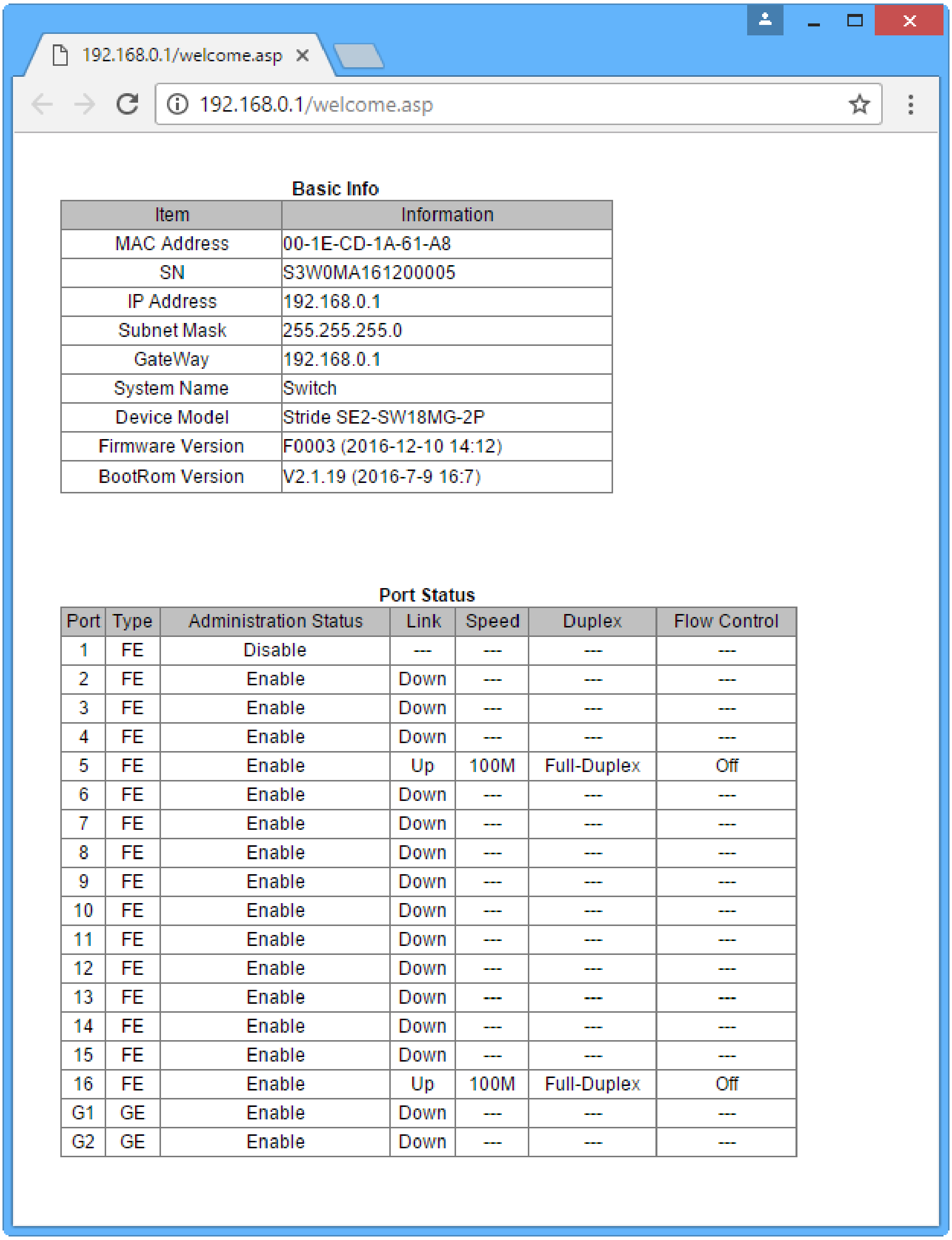
***NOTE**: "admin"* is the default User Name. *"admin"* is the default Password



Serial Number: S3W0MA161200005
System Name: Switch
Location: Switch Location
Contact: Contact Info

AutomationDirect.com All Rights Reserved.

This screen will appear.



Basic Info

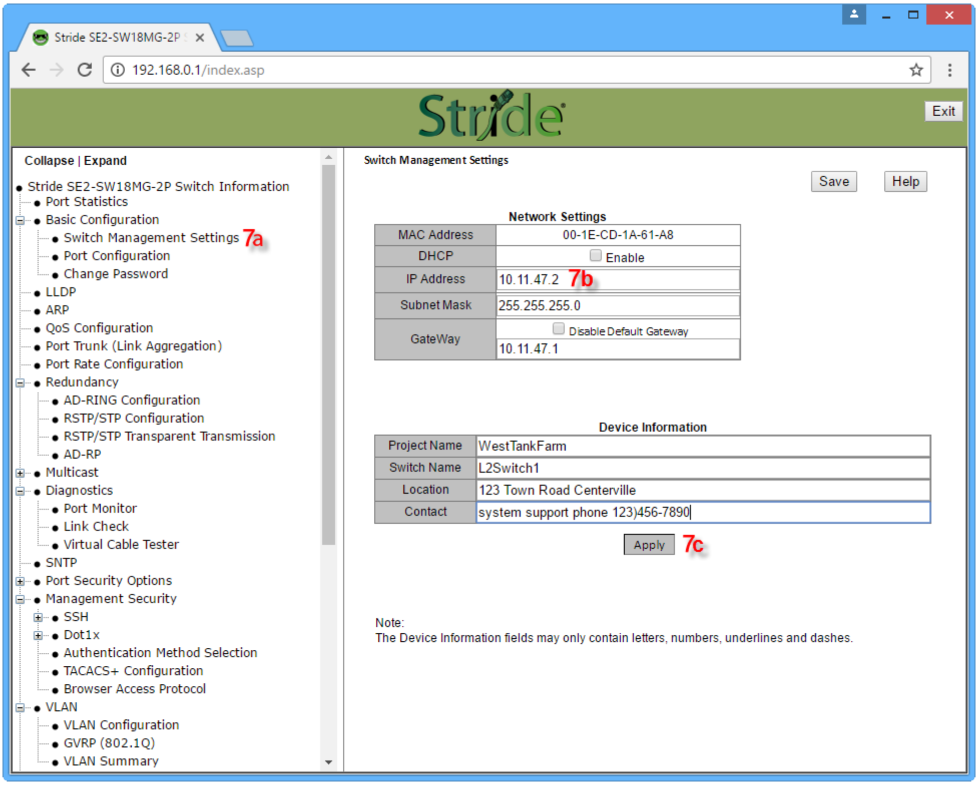
Item	Information
MAC Address	00-1E-CD-1A-61-A8
SN	S3W0MA161200005
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	Switch
Device Model	Stride SE2-SW18MG-2P
Firmware Version	F0003 (2016-12-10 14:12)
BootRom Version	V2.1.19 (2016-7-9 16:7)

Port Status

Port	Type	Administration Status	Link	Speed	Duplex	Flow Control
1	FE	Disable	---	---	---	---
2	FE	Enable	Down	---	---	---
3	FE	Enable	Down	---	---	---
4	FE	Enable	Down	---	---	---
5	FE	Enable	Up	100M	Full-Duplex	Off
6	FE	Enable	Down	---	---	---
7	FE	Enable	Down	---	---	---
8	FE	Enable	Down	---	---	---
9	FE	Enable	Down	---	---	---
10	FE	Enable	Down	---	---	---
11	FE	Enable	Down	---	---	---
12	FE	Enable	Down	---	---	---
13	FE	Enable	Down	---	---	---
14	FE	Enable	Down	---	---	---
15	FE	Enable	Down	---	---	---
16	FE	Enable	Up	100M	Full-Duplex	Off
G1	GE	Enable	Down	---	---	---
G2	GE	Enable	Down	---	---	---

7a. Navigate to the Switch Management Settings page.

7b. Enter the desired Network Information (IP address, Subnet Mask, & Gateway) and Device Information (Project Name, etc).



Switch Management Settings

Network Settings

MAC Address	00-1E-CD-1A-61-A8
DHCP	□ Enable
IP Address	10.11.47.2
Subnet Mask	255.255.255.0
GateWay	□ Disable Default Gateway 10.11.47.1

Device Information

Project Name	WestTankFarm
Switch Name	L2Switch1
Location	123 Town Road Centerville
Contact	system support phone 123)456-7890

Note:
The Device Information fields may only contain letters, numbers, underlines and dashes.

7c. Click Apply.

The management interface will automatically log out.

To log in again, you must change your PC to the new subnet of the switch. For our example, the initial IP Address on the PC was on the desired subnet, so we'll repeat steps 1-4 using the previous network information for the PC and the new IP address of the switch to log in again to begin configuring your switch.

If you're unsure where to start with the configuration options, read the section in this manual called "Why Do You Need a Managed Switch?" to understand more about the **Stride** SE2 series managed switches, their capabilities and how these features may be used.

NOTE: *The default settings enable RSTP on all ports and IGMP which will be adequate for many networks with no further configuration.*

Why Do You Need a Managed Switch?

For many applications, an unmanaged switch will be adequate. In some networks, though, a managed switch is helpful or required. In this chapter, we'll explain some of the most common features that make a managed switch preferable.

Enhanced Traffic Filtering

An unmanaged switch will filter out many packets from an end device but there are still many types of packets that an unmanaged switch cannot determine what to do with and must forward to all ports. Whenever a device receives a packet that is not specifically targeted to that device, it must spend resources processing the unintended communication before discarding it. This delays the processing of communications intended for that device and hurts the determinism and efficiency of a process.

A managed switch can help with this in several different ways:

- **Multicast Filtering (IGMP):** Control systems often see a lot of Multicast packets. These packets cannot be filtered out by an unmanaged switch. The **Stride** managed switch can intelligently 'learn' whether certain Multicast packets should be sent to the devices on its ports and will filter them or not filter them appropriately.
- **VLANs:** A VLAN divides a network in ways that previously required physical separation. It may be difficult to physically group networks that need separation. Setting up VLANs can simplify the setup for these situations.

Troubleshooting

A valuable tool for troubleshooting communications on your Ethernet network is examining the messages that are passed between devices. With hubs, it was possible to see the messages between devices because hubs broadcast every packet to all ports. Unmanaged switches won't allow this since they filter unicast packets to only the intended physical ports. Managed switches can help with this by utilizing the Port Monitoring feature.

With the Port Monitoring feature you simply specify which ports' data you want to view and where to send that data. Plug your PC into the destination port and use Ethernet sniffing software (such as Wireshark) to see the data being sent back and forth.

Redundancy

The downside of any Ethernet switch is the simple fact that it is another electronic component in the system that could be subject to failure. There is also a risk that as a network grows and more switches are added to it, a 'ring' may accidentally be created causing the network to go down. Utilizing the Rapid Spanning Tree or AD-Ring feature of the **Stride** managed switch can reduce these risks.

- **RSTP:** Rapid Spanning Tree Protocol is currently the preferred method to purposely create a ring that allows multiple, redundant paths on the network but intelligently decides one path when the network comes up, and assigns alternate paths if some part of the original path goes down. The manner in which the switch decides the original paths and the time it takes to change to an alternate path is much, much faster than the original Spanning Tree Protocol. It is really only useful to enable the older STP if your legacy network requires this protocol. The RSTP feature is enabled by default.
- **AD-Ring:** In many control systems, the time it takes for the RSTP algorithm to change paths upon some network event is too slow. The AD-Ring is proprietary to the **Stride** SE2 series managed switches which means it will only work in a ring where all switches are SE2 series managed switches. But it has the advantage of changing paths very quickly.

Security

Network security has become a great concern for facilities. While the network devices themselves are only one part of a network security strategy, the **Stride** managed switches have several security features.

Some security features protect access to switch management and will provide one level of protection from the switch being accidentally or maliciously reconfigured.

Other security features provide one level of protection for the traffic on your network as it moves across the switch.

- **Port Control:** In the “Port Security Options” setup, you can disable ports that are not being used. You may also limit the MAC addresses that will be allowed to communicate on a port. These features help limit unauthorized access to your network.
- **Management Security:** You can implement a secure password required to access the switch. You can also set the browser access to https, increasing your security when accessing the switch management configuration through the browser.

Better Network Awareness

The ability of the process to know when something is wrong with the network and what is wrong is a great feature of the **Stride** managed switches. Your PLC or controlling device can make ‘smarter’ decisions as to what alarms or fallback behavior to trigger based upon the diagnostic data that is supplied by the switch.

- **Modbus:** If you have a controlling device on the network that has Modbus TCP or UDP client capability, several diagnostic tags can be read from the switch to indicate the health of the network and certain configuration tags may be written into the switch.
- **EtherNet/IP:** Similar to the Modbus/TCP feature, if you have a controller on the network that has EtherNet/IP client capability, diagnostic tags can be read from the switch and configuration settings may be written into the switch.
- **SNMP:** SNMP stands for Simple Network Management Protocol and is used for just that. There are many commercial software tools that can query or receive ‘traps’ sent by the **Stride** managed switch to ascertain events or health of the switch.
- **Port and Power Status (Alarm Output):** The **Stride** managed switch has two power inputs that can be used for redundancy. If one of the power inputs fails, there is a relay contact that can be configured to report this failure.
- **Spanning Tree Status:** The switch can be configured to report when something in the Spanning Tree has changed,
- **AD-Ring Status:** The AD-Ring status can be ascertained from other devices as well.
- **MAC Table:** The switch keeps a table of the MAC IDs of devices that are communicating across it.

CHAPTER 3

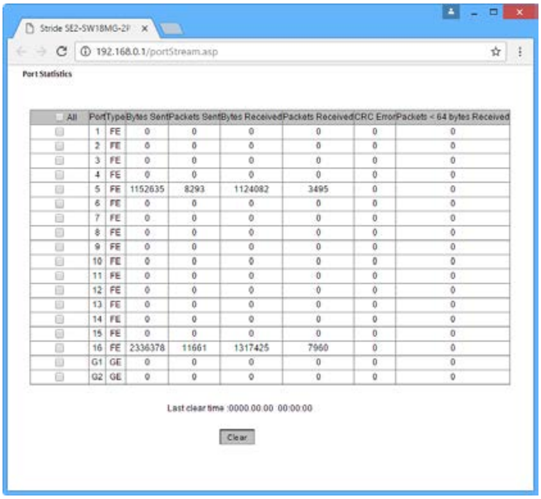
MANAGED SWITCH BASIC FEATURES

In this Chapter...

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.

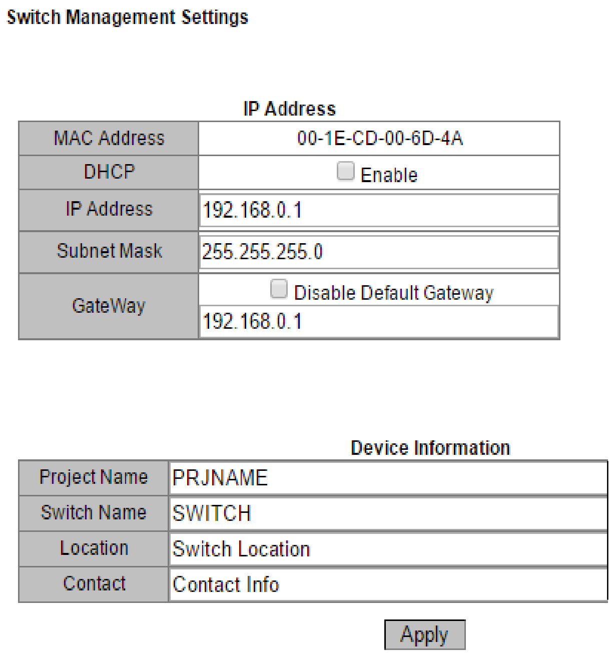
The Port Statistics table identifies each port and port type:

- 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.

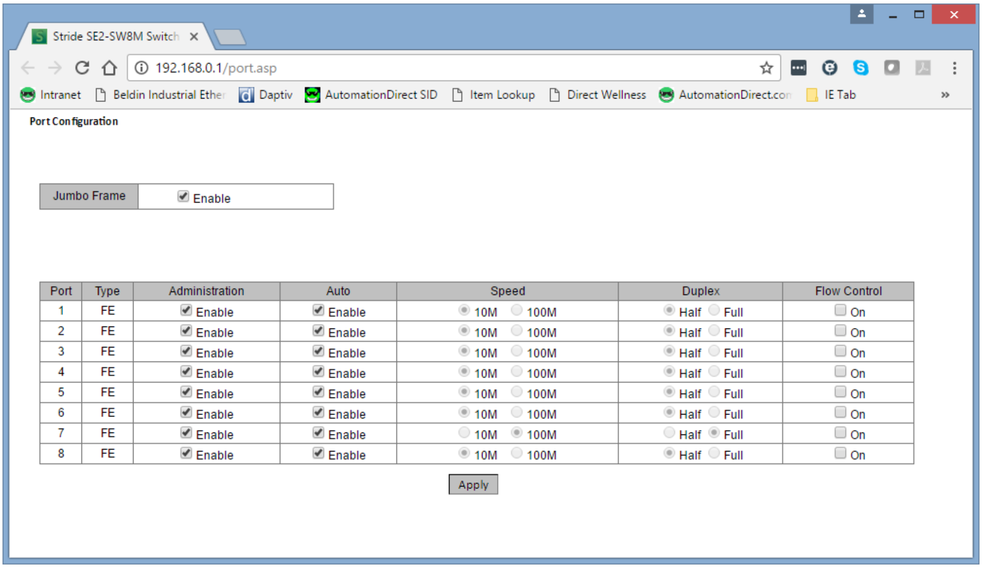
Administration – Also, to provide a level of network security, you may choose to restrict access to the switch by administratively disabling unused ports. Ports that are disabled are virtually non-existent (not visible for switch operation or spanning tree algorithm).

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.



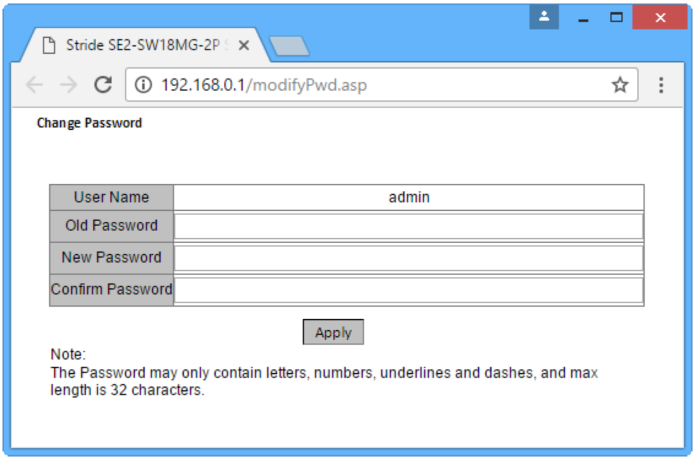
Port Configuration

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.

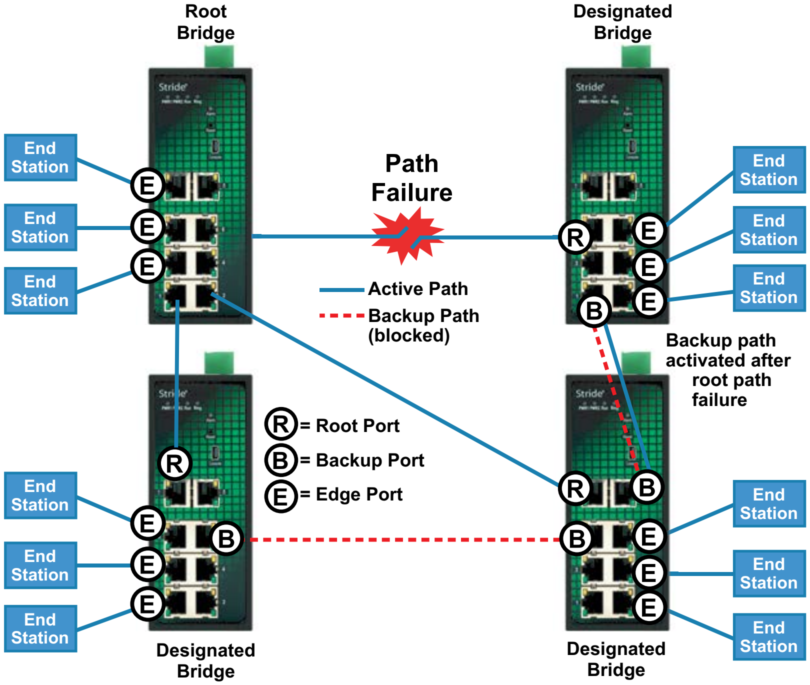
There are four methods of accomplishing redundancy in the **Stride** SE2 series managed switches:

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.

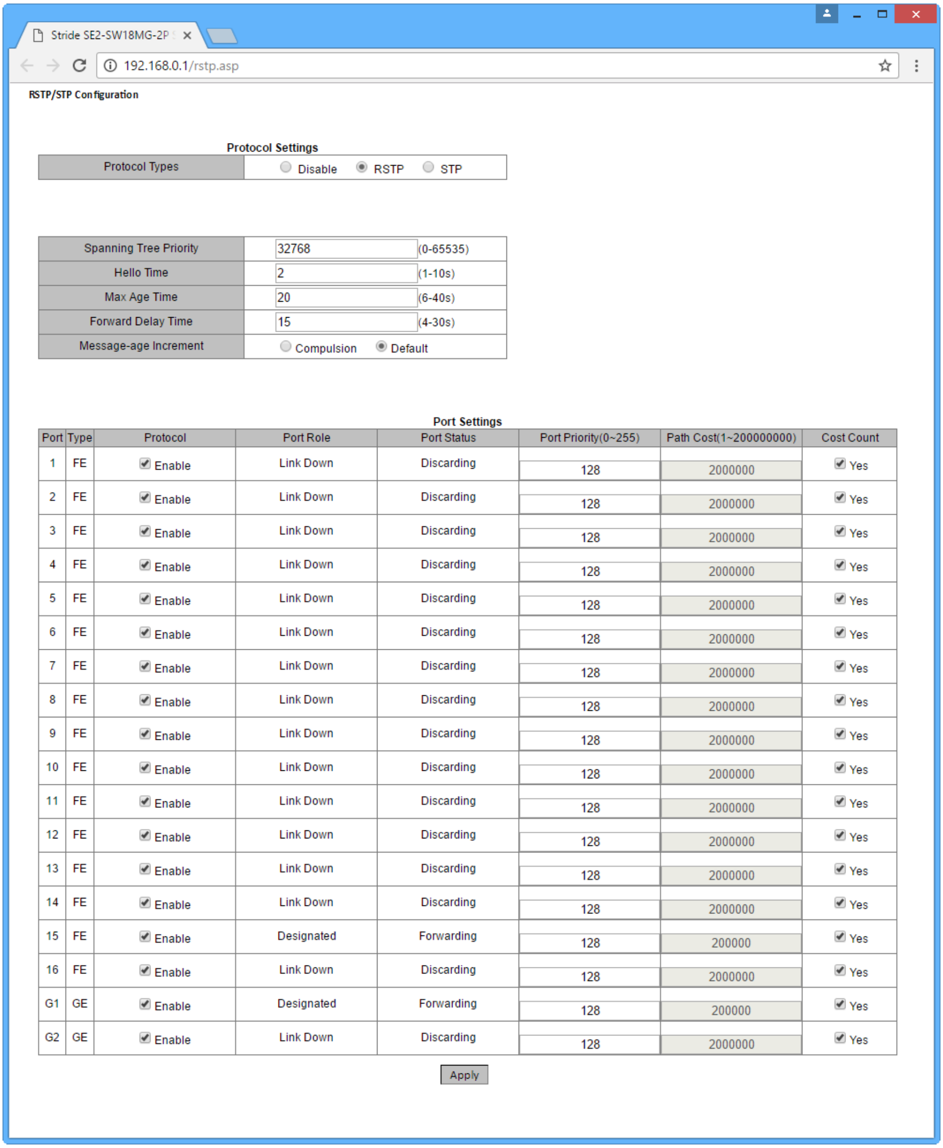
Pairs of ports that are configured for AD-Ring or AD-RP must be Disabled from participating in Spanning Tree.

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

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

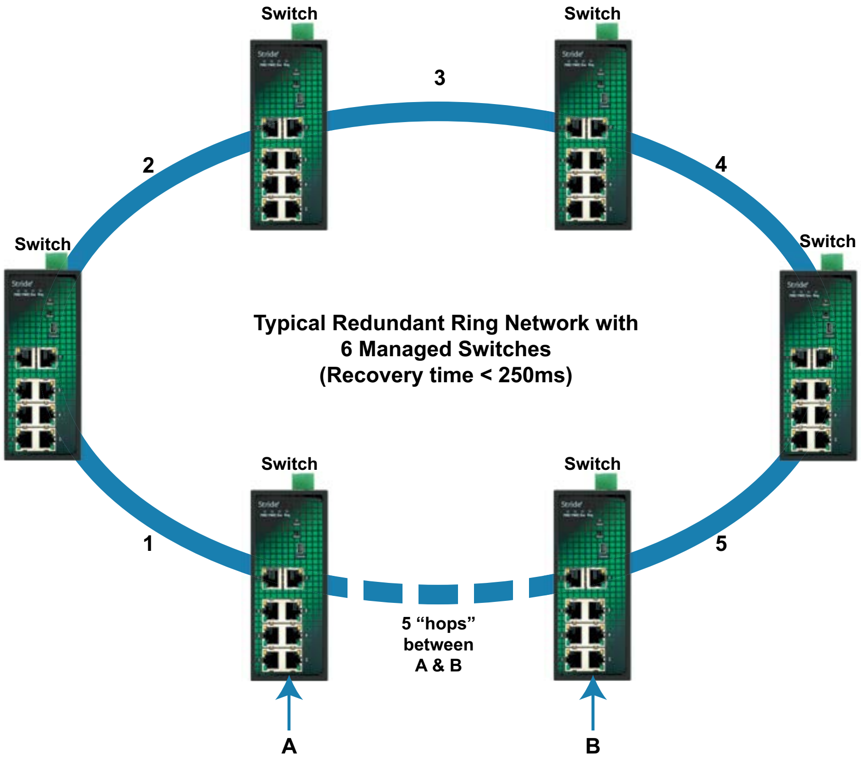
Example 1: Maximum "Hops" and Switches in a Redundant Ring:

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.

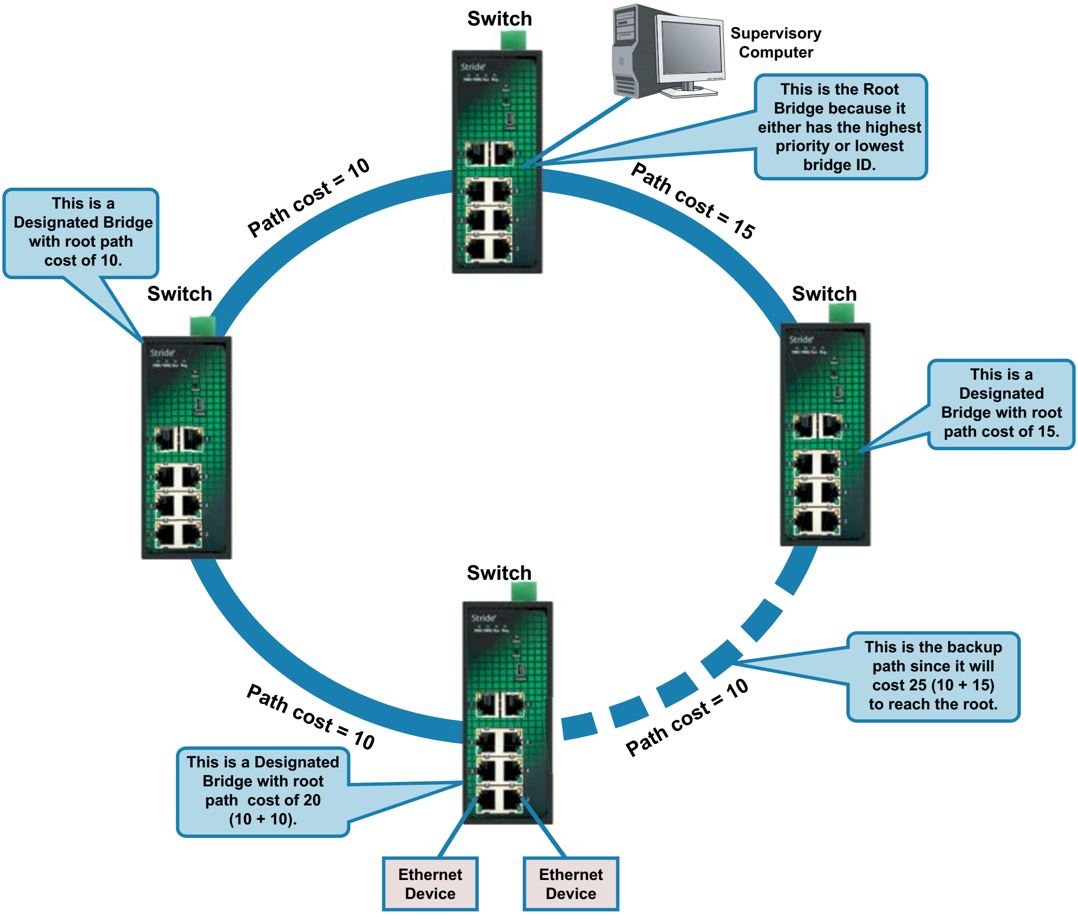
The overall recovery time when there is a network segment failure is dependent on the number of hops. The recovery time is typically less than 50ms per hop. Therefore, in the diagram below of a typical ring with 6 managed switches the overall recovery time would be less than 250ms (5 hops x <50ms).



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

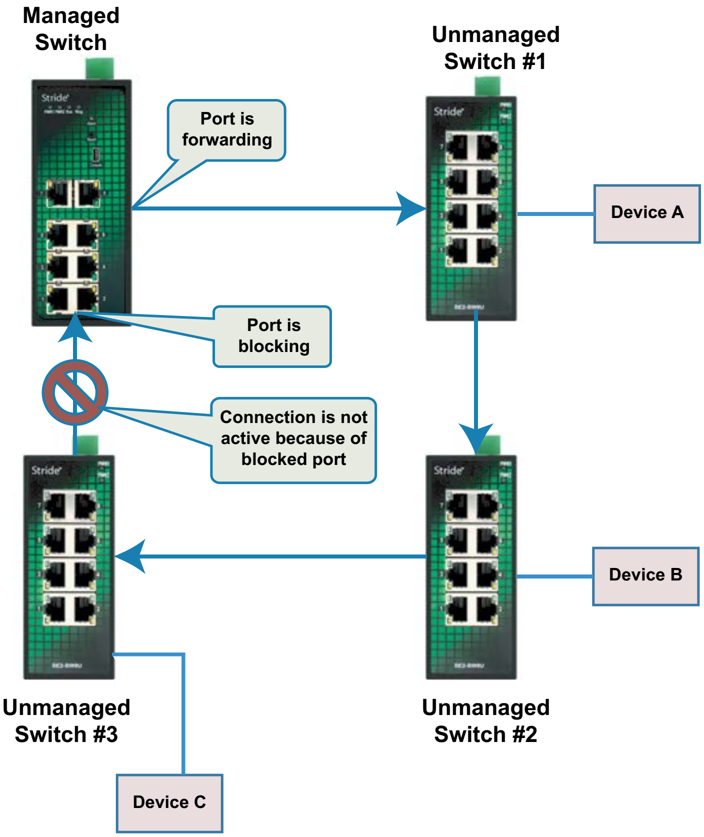
Example 3: Ring Topology with only 1 Managed Switch (Bad idea!)

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.

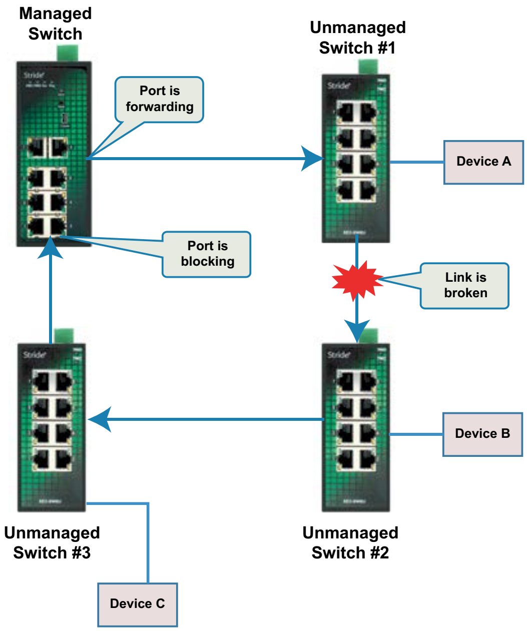
Hypothetical Scenario:

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.

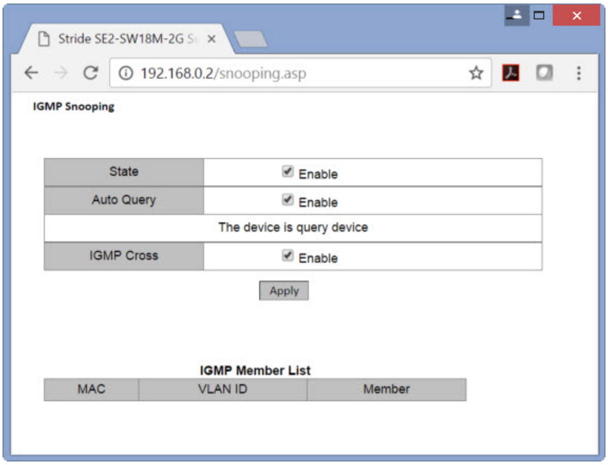
IGMP Snooping State – IGMP Snooping is Enabled by default. The switch will participate in IGMP handling.

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

Apply

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.

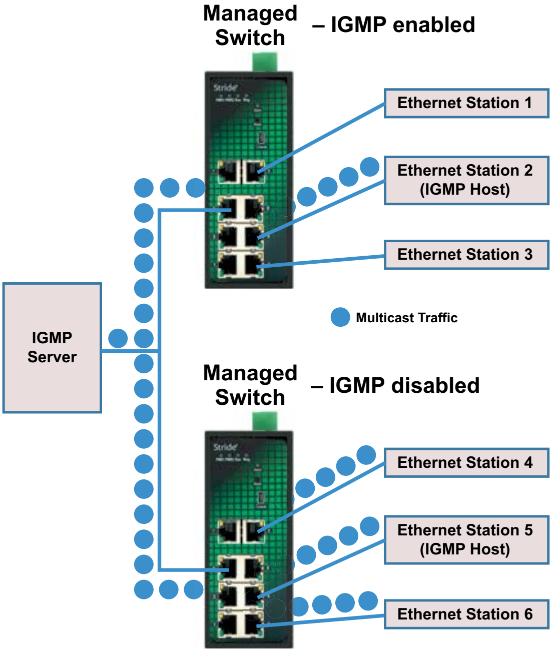
The Benefits of Enabling IGMP

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.

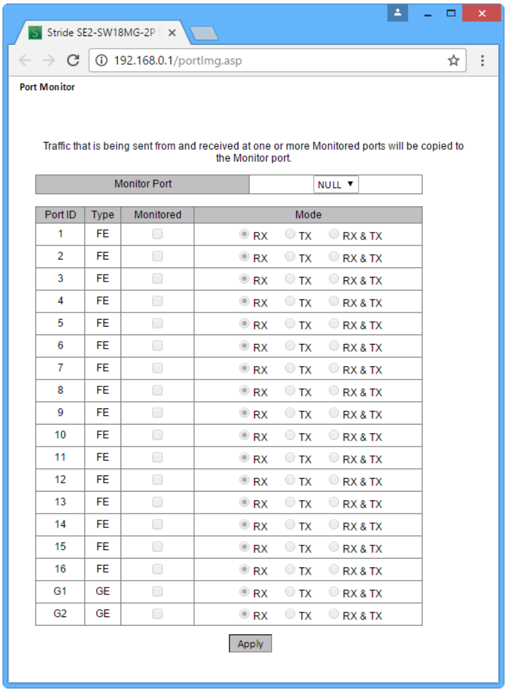
Choose the source ports to be monitored (mirrored).

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.

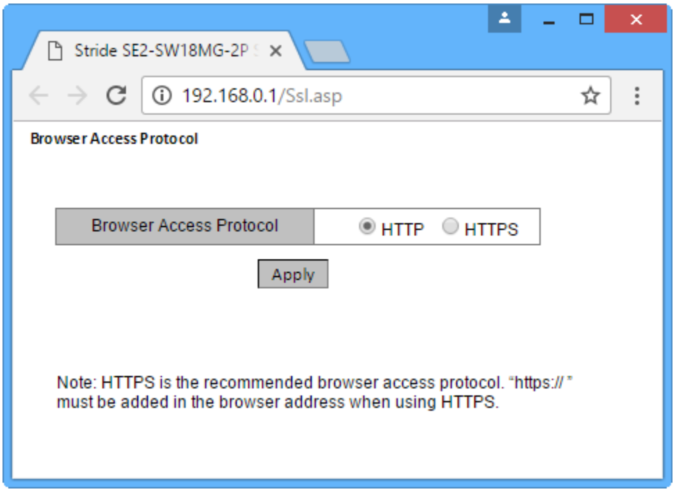
Monitor Port	NULL ▾

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:

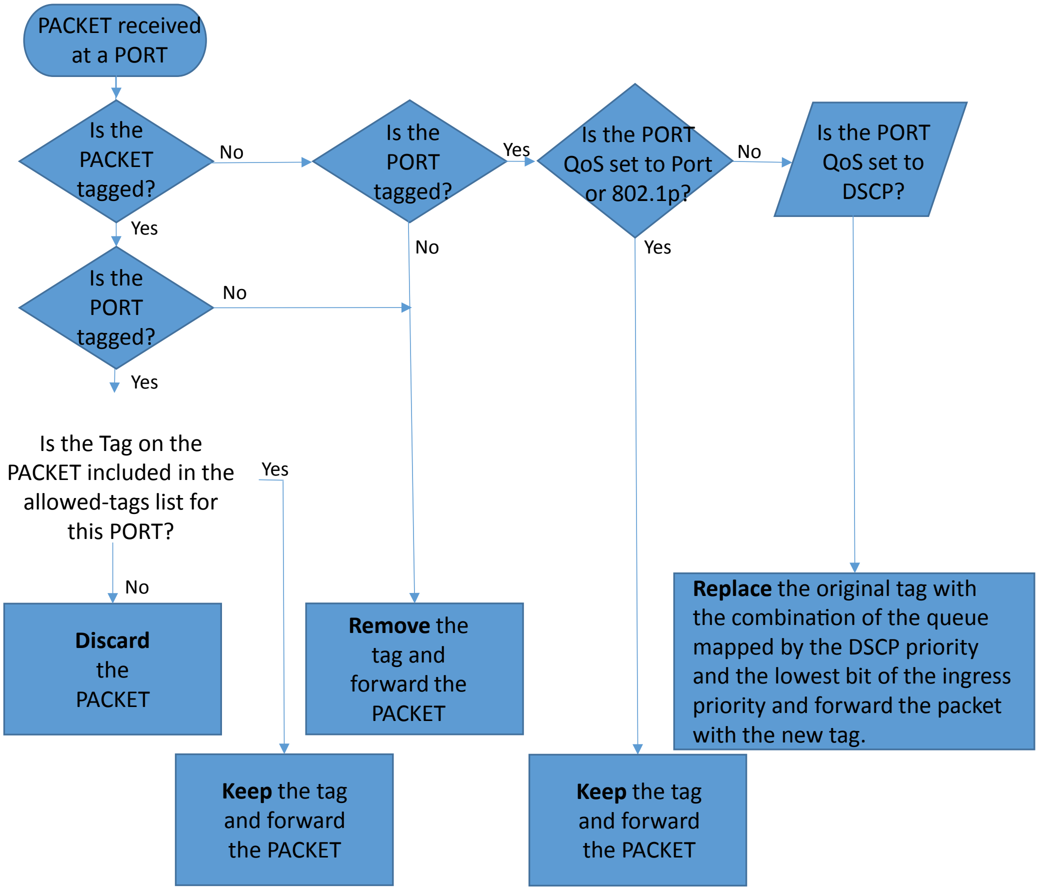
- 0 = Indicates that the tag is not being used for VLAN routing but only to carry priority information. (See QoS topic).
- 1 = Used for switch configuration and management.
- 4095 = Not allowed by the 802.1Q standard.

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 Tag on the PACKET included in the allowed-tags list for this PORT?
Yes
No
Discard the PACKET
Keep the tag and forward the PACKET
Is the PORT tagged?
Yes
No
Remove the tag and forward the PACKET
Is the PORT QoS set to Port or 802.1p?
No
Yes
Keep the tag and forward the PACKET
Is the PORT QoS set to DSCP?
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.

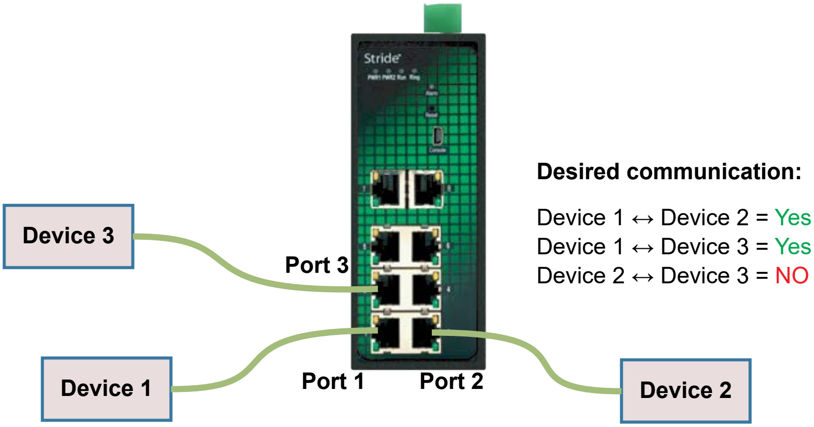
PVLAN – Private VLANs

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)*.

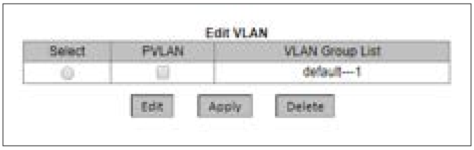
Example PVLAN configuration settings



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.



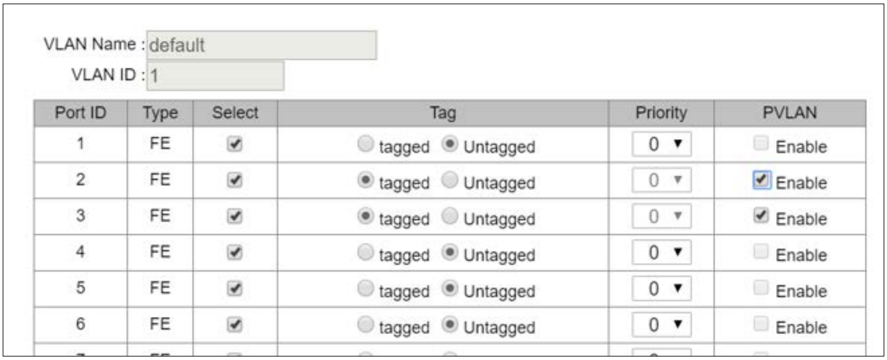
Edit VLAN

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.

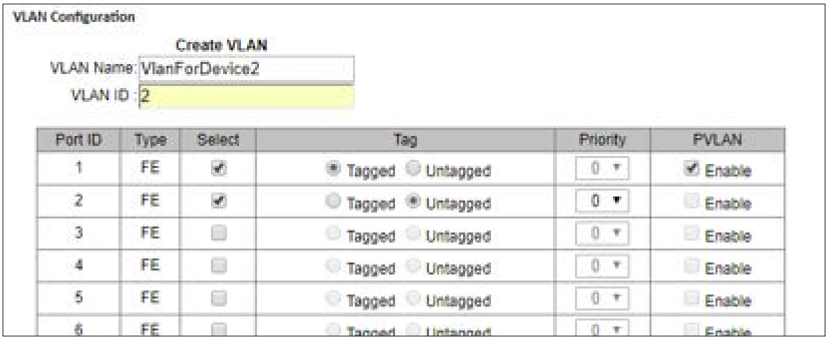


VLAN Name : default

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:



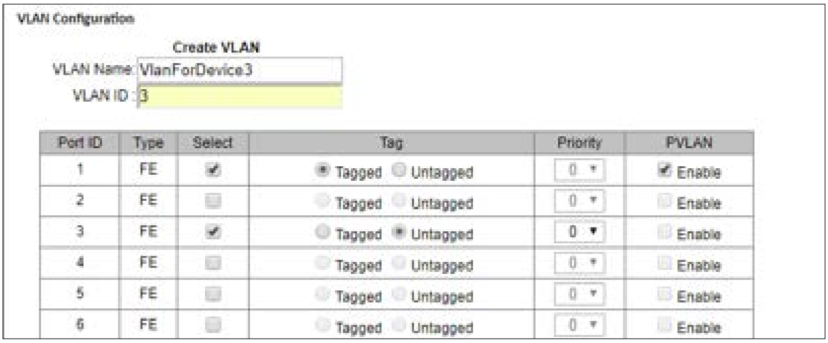
VLAN Configuration

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

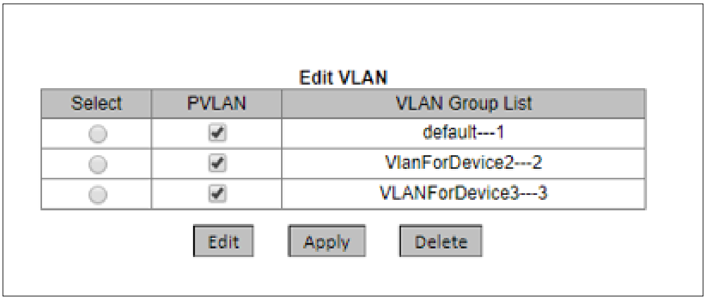
Create VLAN

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:

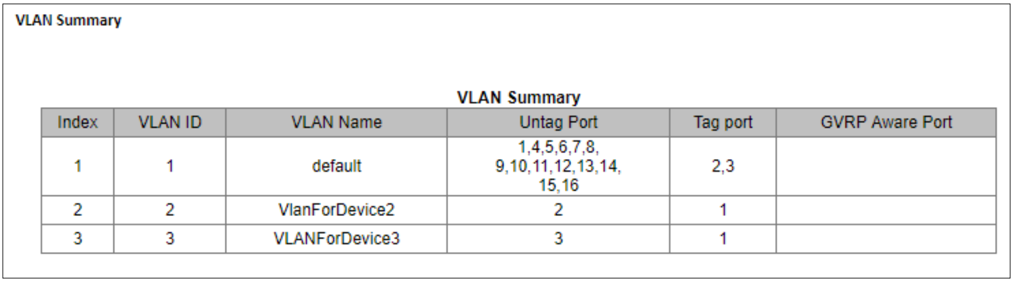


Edit VLAN

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

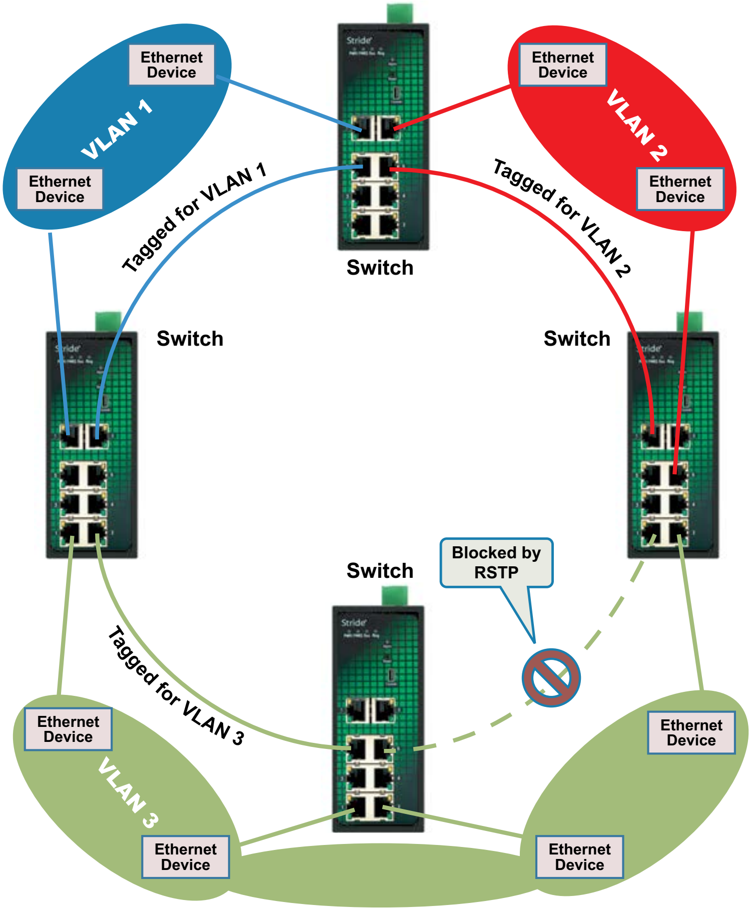
VLAN Summary

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

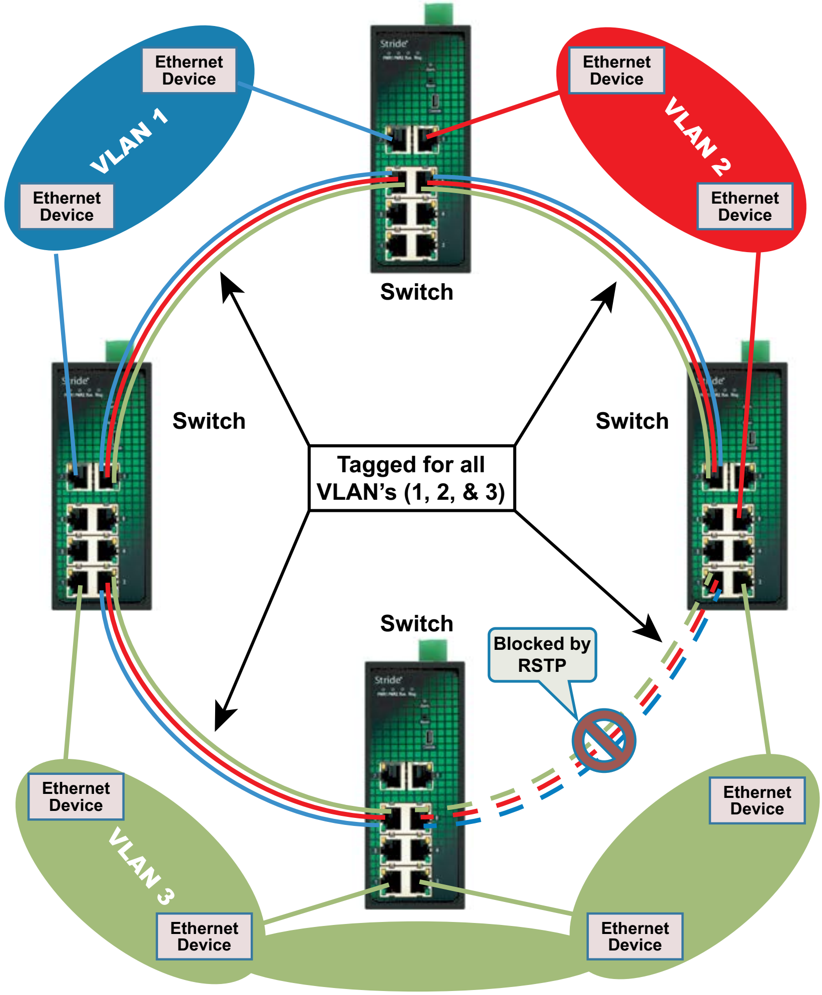
Extra care must be taken when enabling both VLANs and redundancy, or communications failures may occur.

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.



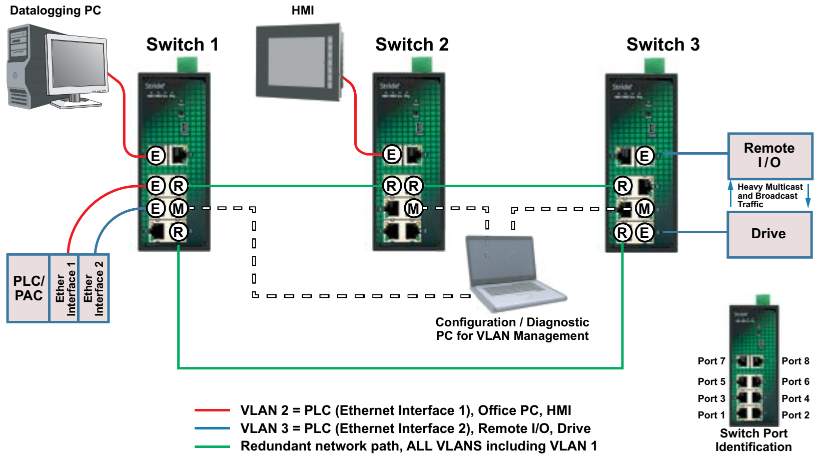
VLAN Examples

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

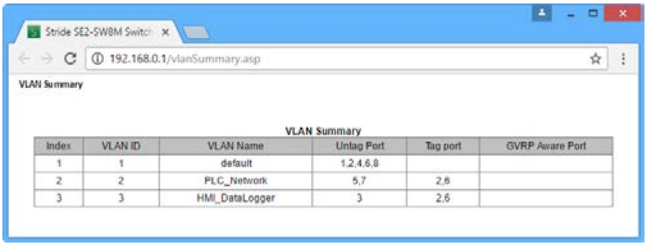
Solution: Use **Stride** managed switches, utilizing the VLAN feature to separate the broadcast and multicast traffic from all the devices except for the PLC. We will also wire the three switches into a Ring configuration so that we can take advantage of the redundancy feature of the switch. In this 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.

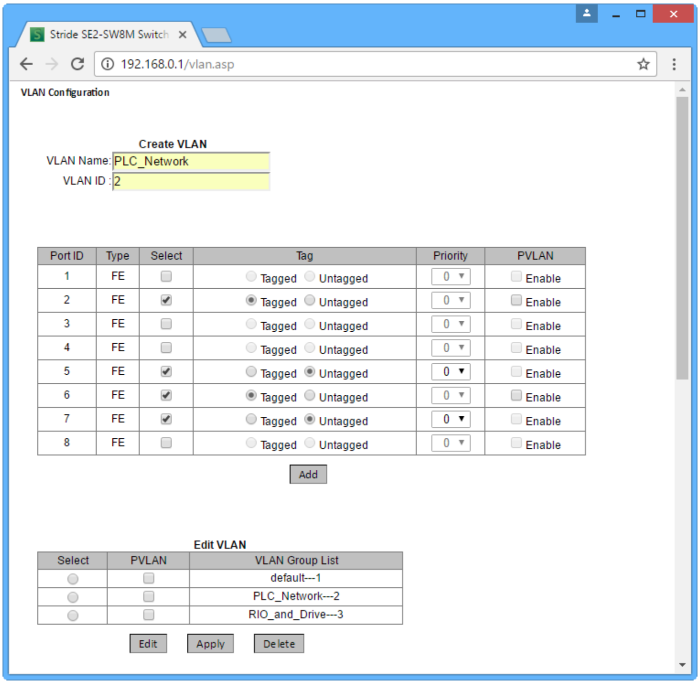
Switch 1 VLAN Configuration:



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

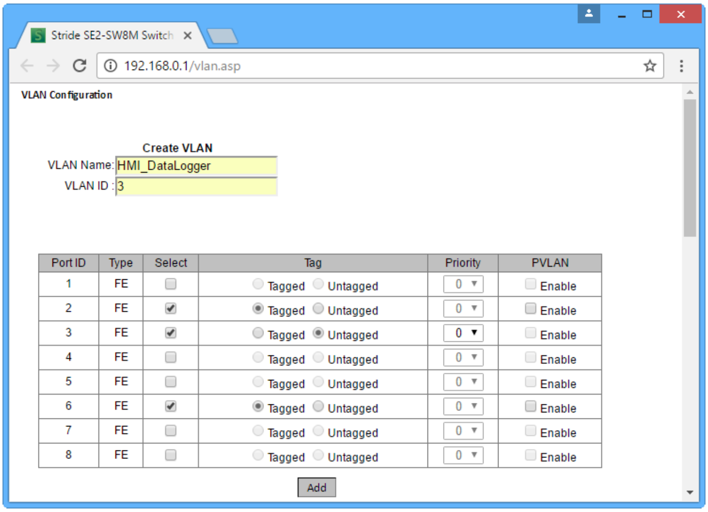
VLAN ID : 2

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

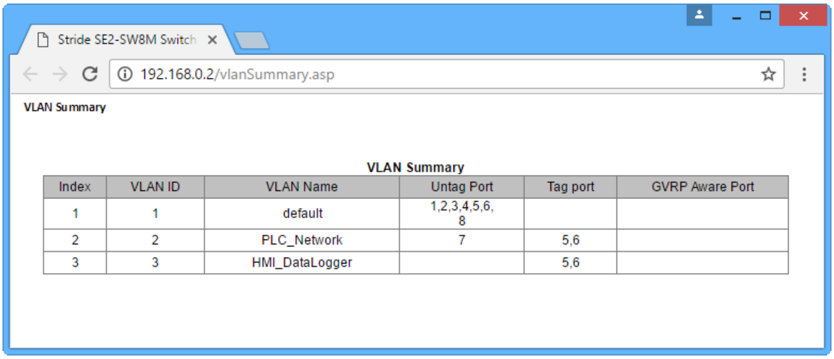
VLAN Name: HMI_DataLogger

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

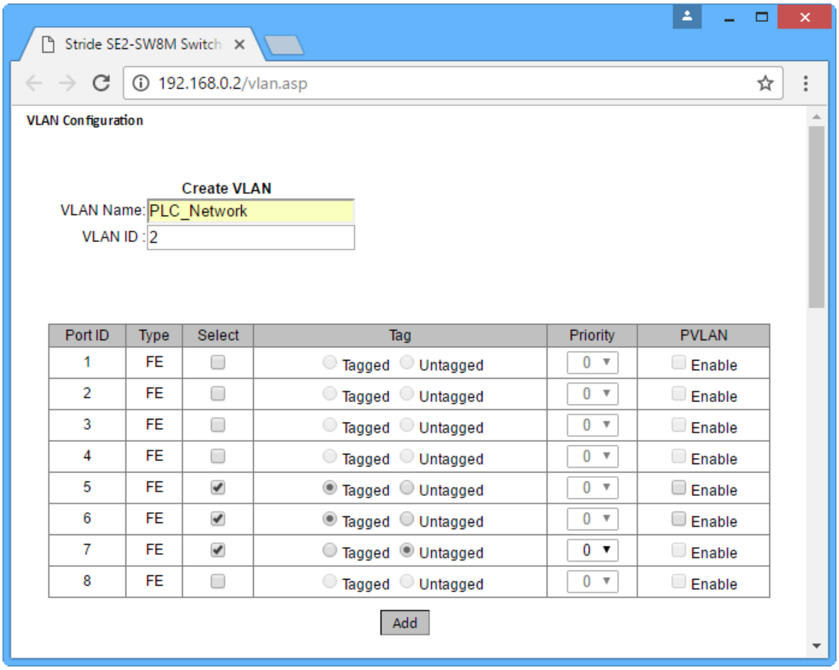
Switch 2 VLAN Configuration:



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

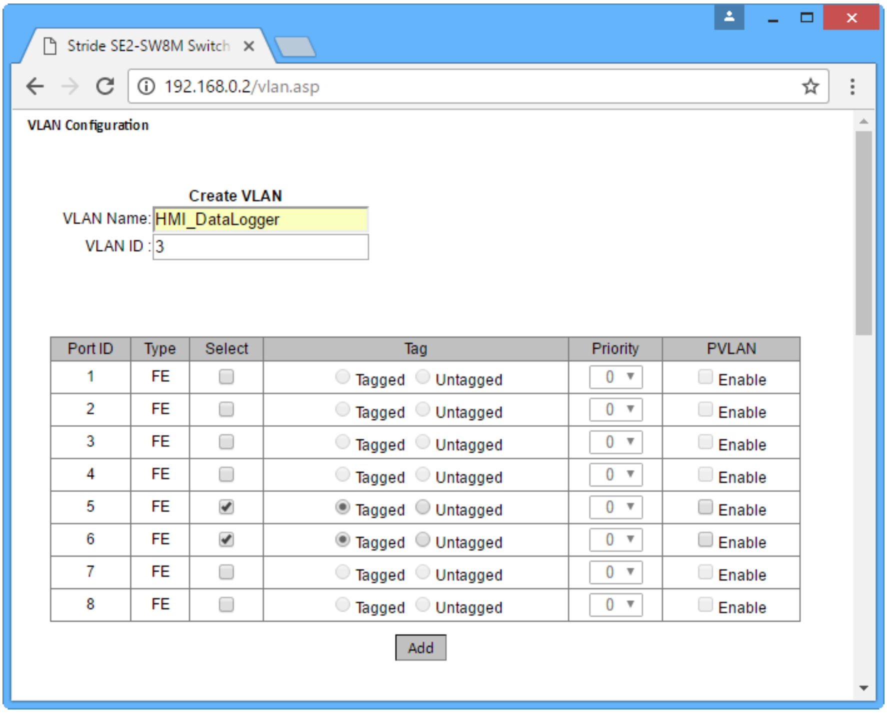
Create VLAN

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

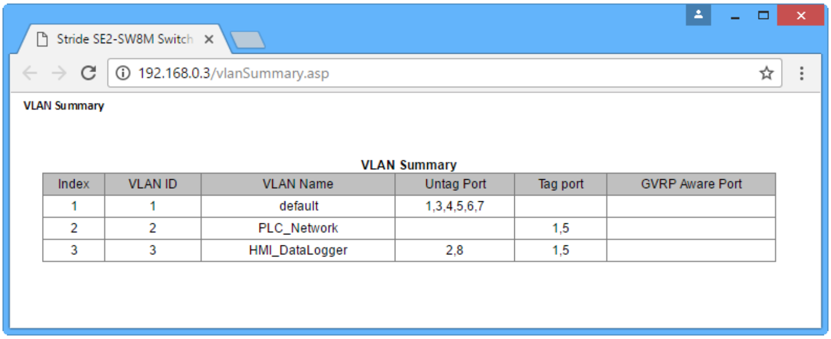
VLAN Name: HMI_DataLogger

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

Add

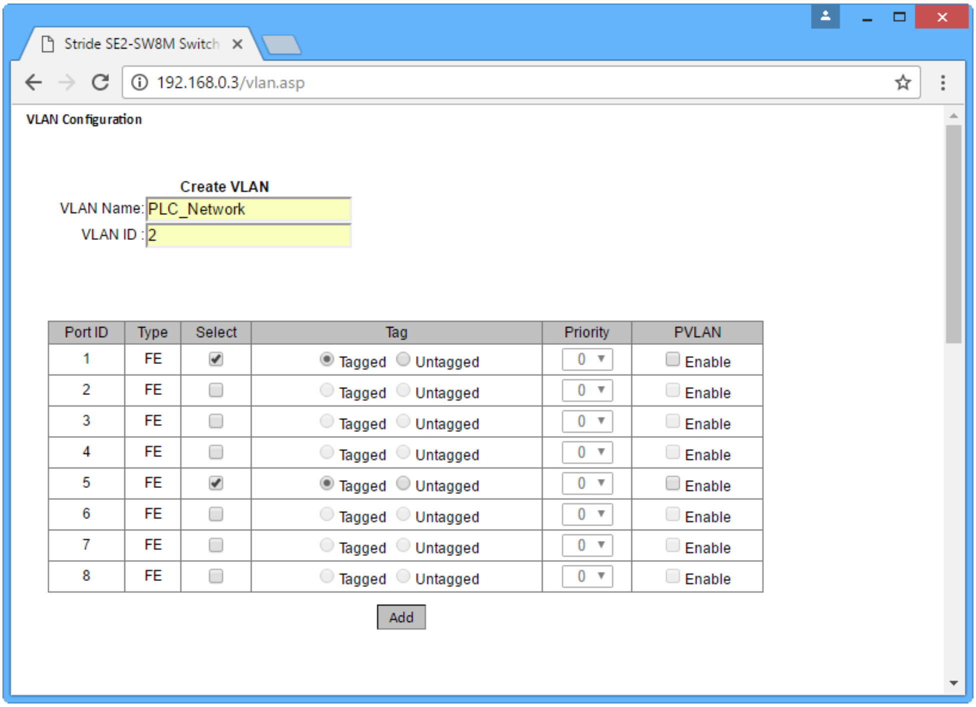
Switch 3 VLAN Configuration:



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

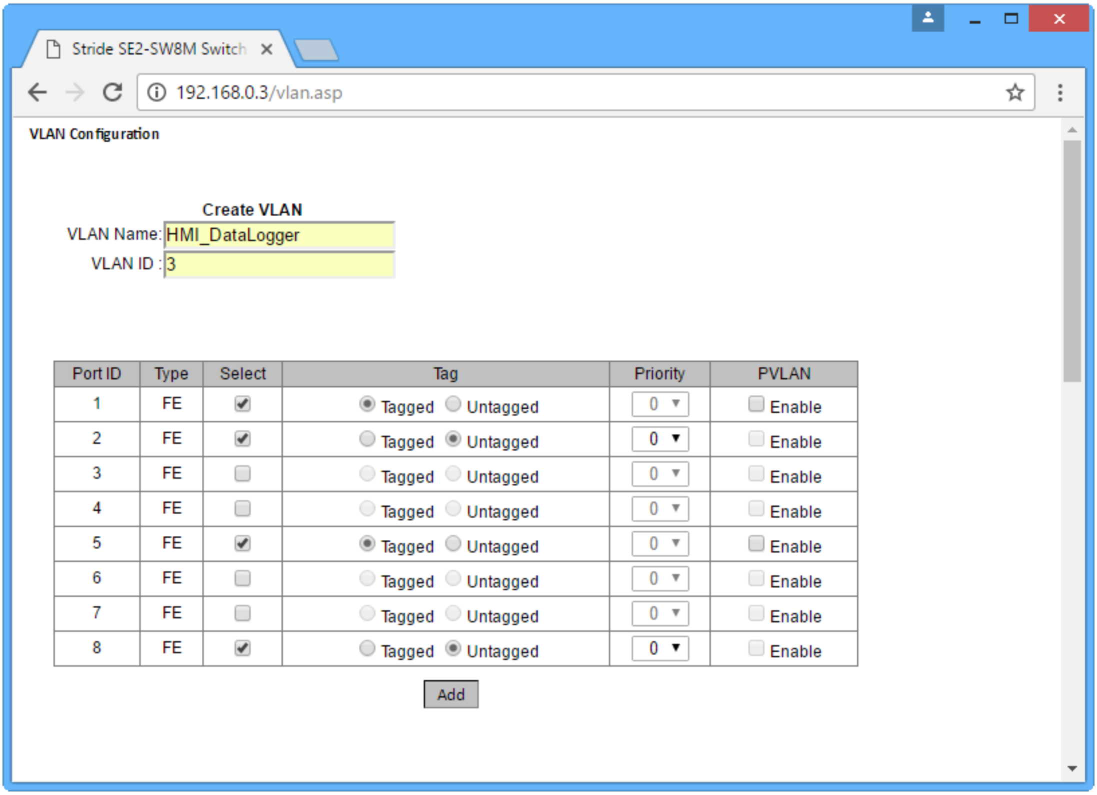
Create VLAN

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

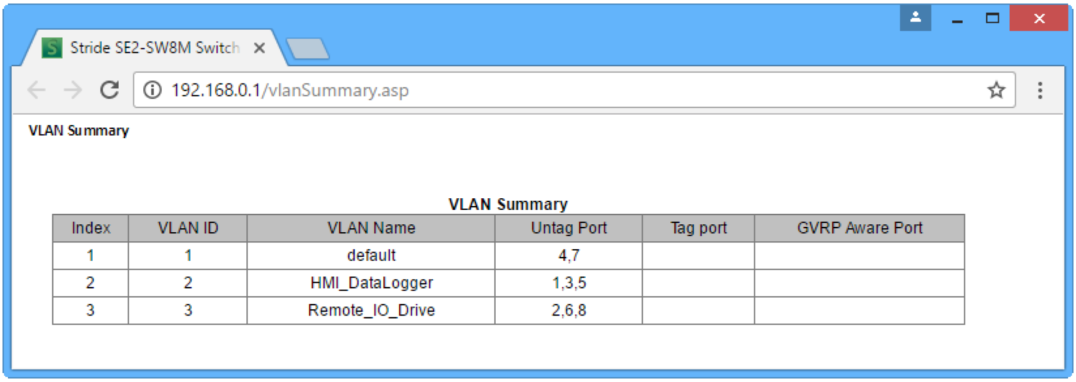
VLAN ID : 3

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

Add

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.

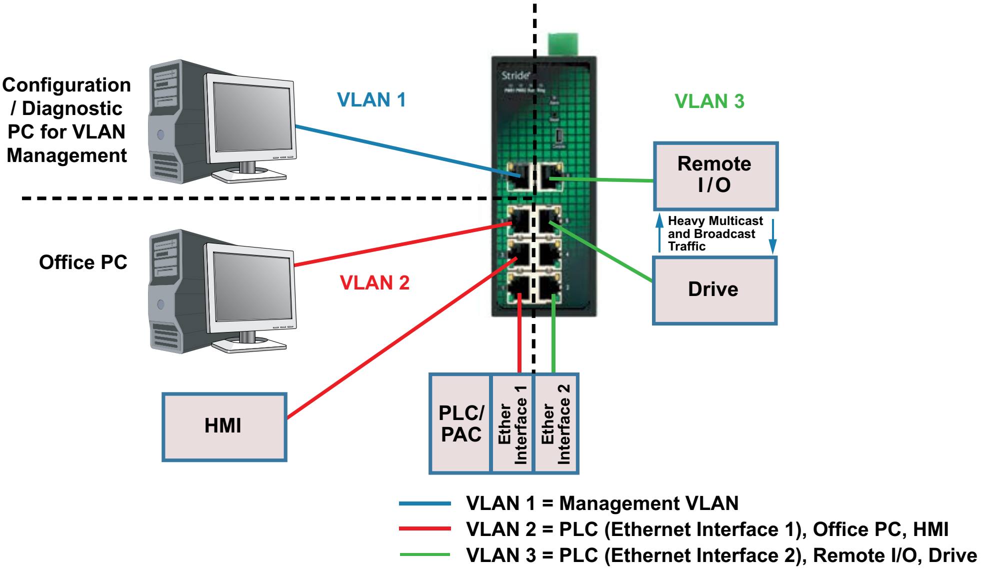


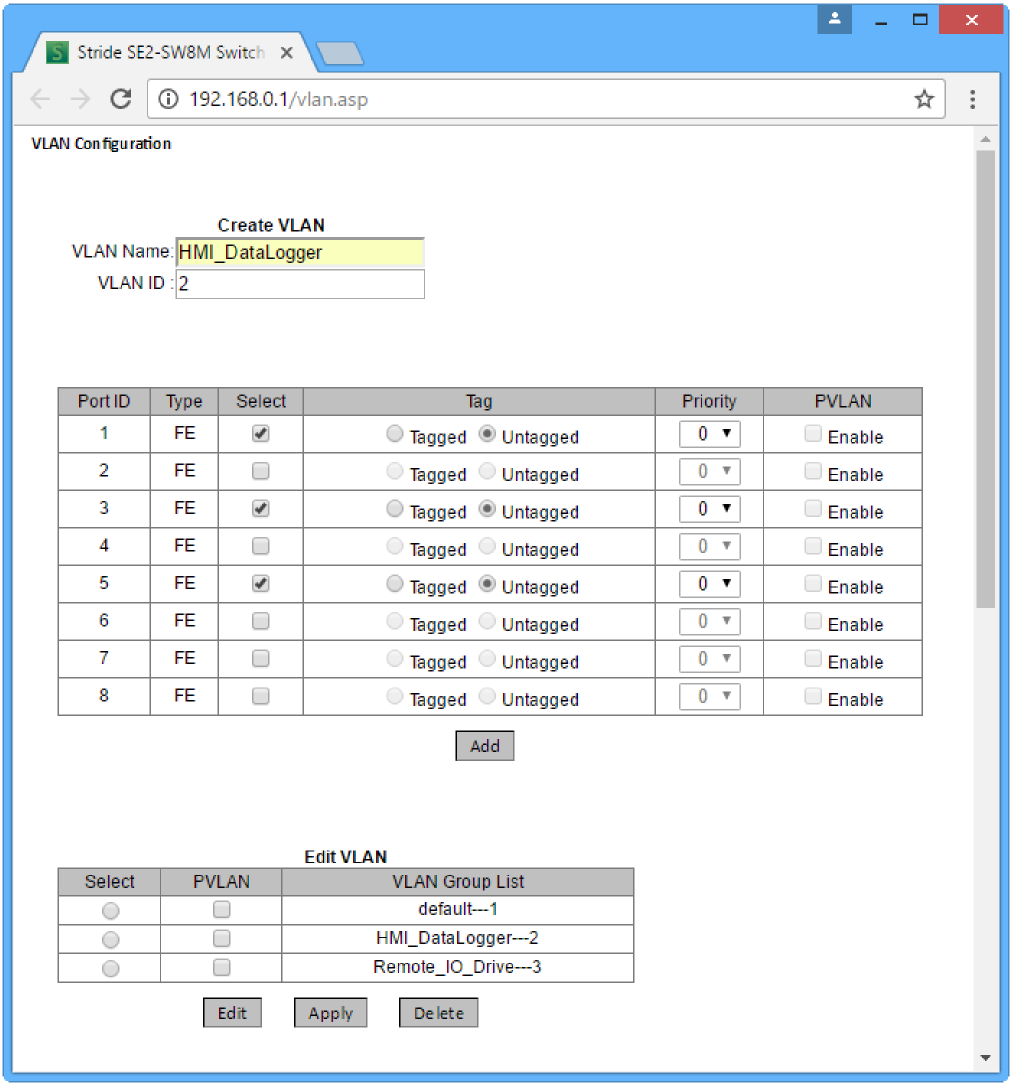
VLAN Summary

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

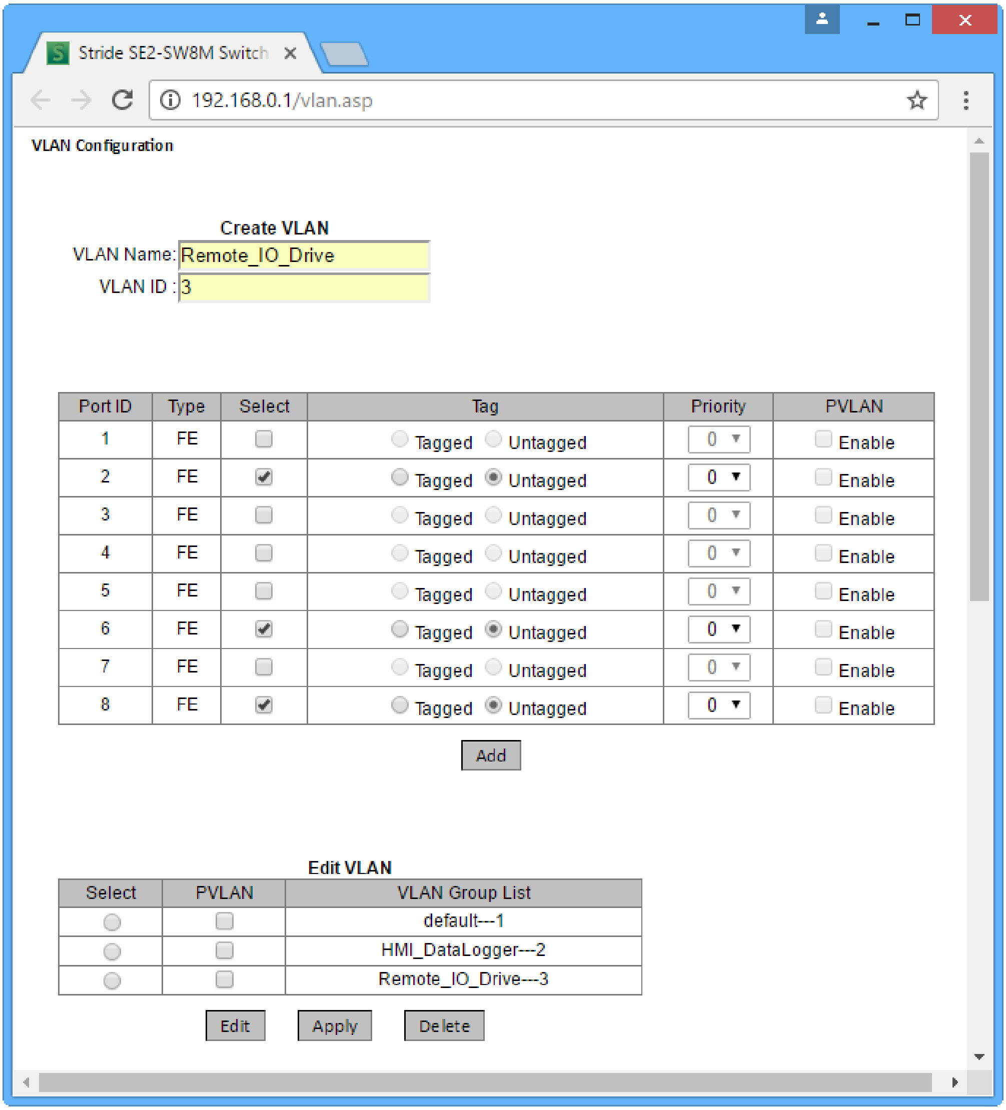
VLAN Name: HMI_DataLogger

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

Edit VLAN

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



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.

Advanced Network Behavior Features

Chapter 4

In this Chapter...

Advanced Network Behavior Features

In addition to the Basic Managed Switch Features detailed in Chapter 3, the **Stride** SE2 series Managed switches include a full list of features that will be valuable to particular networks. This chapter describes the more advanced network features found in the **Stride** managed switches.

Traffic Priority (Priority Queuing QoS, Quality of Service)

Without enabling special handling, a network provides a "best effort" service to all applications. This means that there are no assurances regarding the Quality of Service (QoS) for any particular application because all packets are treated equally at each switch or router.

However, certain applications require deterministic response from the network to assure proper operation.

Consider a drilling machine in a plant that is controlled by a computer on a local network.

The depth of the machine's drill is critical; if the hole is drilled too deep, the material will have to be thrown out. Under normal conditions, the drill process is running smoothly (controller and computer are communicating efficiently over the network) but when another user on the network accesses records from an online database, the large volume of traffic can interfere with timely communication with the drill. A delay in communications between the drill and controller causes the drill to go too far and the material has to be thrown away. To prevent this from happening, we need to provide a certain QoS for all drill controller communications so delay is avoided.

Traffic priority is shaped based on three principals:

1. Identify the type of traffic. This is encoded in the message headers built by the END DEVICE. The end device will encode according to either 802.1p or DSCP rules for creating that header.
2. Manage congestion - Queue traffic then forward it according to the scheduling algorithm as configured on the QoS configuration page.
3. Avoid congestion – apply rules for dropping traffic to alleviate congestion on the network as configured on the Port Rate configuration page.

In this section, we'll discuss the QoS options for MANAGING network congestion.

Since the SE2 switches do not assign priority to traffic, we'll simplify our discussion to consider traffic between switches. That is, traffic at a port that is connected to an end device will have a priority assigned by that end device and we'll assume the network design has considered the rate requirements of that device.

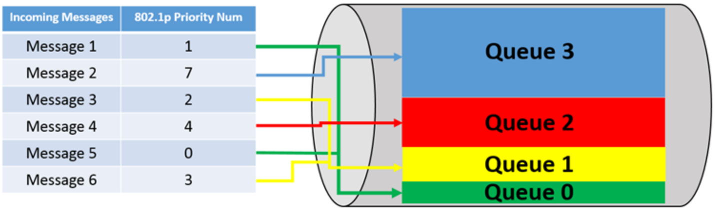
For traffic received at the switch (Ingress), the SE2 managed switches support three types of queue mapping modes to identify traffic priority: port, DSCP and 802.1p

- If the Ingress Type is **Port**, the rules for port ingress rate limiting as configured on the Port Rate configuration page govern traffic priority. Simply put, incoming traffic is accepted until the "bucket" is full, then is dropped. See the Port Rate configuration section in this manual for details.
- If the Ingress Type is **DSCP**, the priority and queue relationship can be configured according to the ToS/DSCP field in the traffic that is received at that port. The choice between DSCP and 802.1p depends on the end devices and how those devices construct the message headers. Configuration of the switch requires understanding of the requirements and behaviors of the end devices. The priority may be managed across the switch by configuring the 64 DSCP priorities as they map to the 4 queues (DSCP Priority table on the switch QoS configuration page).
- If the Ingress Type is **802.1p**, the priority and queue relationship can be configured and will apply to traffic that arrives at the switch tagged in the DSCP field. Untagged traffic will be assigned priority and queue according to 802.1p rules. The priority may be managed across the switch by configuring the 8 priorities as they map to the 4 queues (802.1p Priority table on the switch QoS configuration page).

For traffic that will be transmitted by the switch (Egress), the SE2 managed switches support two types of QoS queue scheduling: Weighted Round Robin (WRR) and Strict Priority (SP).

- If the Egress type is **SP**, high priority messages will be guaranteed preferential forwarding. This is especially useful when network traffic includes sensitive signals. Once a message is added into the high priority queue, the SP mechanism stops traffic from the lower priority queues and processes the data in the high priority queue. Only when the high priority queue is empty will the switch return to processing data in the lower priority

- If the Egress type is **WRR**, traffic will be scheduled according to the configured weight ratio; Queue 3 is allotted half the bandwidth, Queue 2 is allotted 1/4 the bandwidth, Queue 1 and Queue 0 split the remaining quarter. More bandwidth (traffic) is allocated to the queue with the largest ratio. See the graphic below.



Incoming Messages	802.1p Priority Num
Message 1	1
Message 2	7
Message 3	2
Message 4	4
Message 5	0
Message 6	3

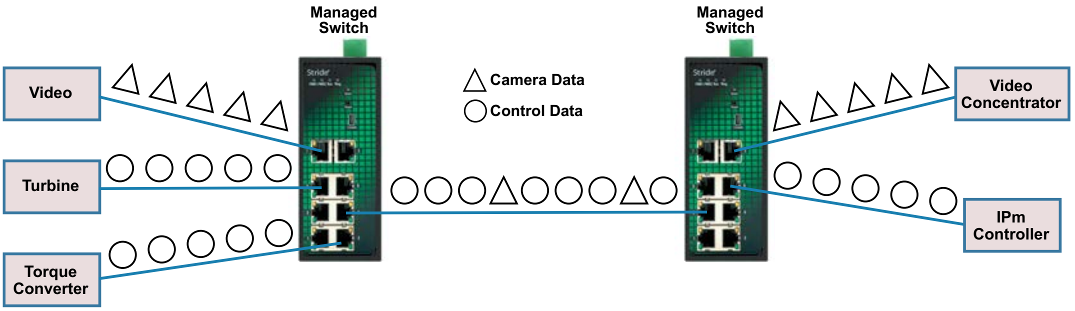
802.1p Example

The 802.1p configuration requires the end device to insert an Ethernet frame header containing the priority embedded in an 802.1p tag. It will contain a value of 0 (lowest) – 7 (highest). The 802.1p Priority configuration allows for translation of the 802.1p priority levels to the switch's queueing levels.

The DSCP configuration is similar in concept to the 802.1p configuration but uses a different Ethernet frame header with a priority level ranging from 0 – 63. The DSCP priority table allows for configuration of the 0 – 63 range of the DSCP header to the 0 – 3 Queue levels of the switch.

Let's consider an example network. There is a power plant that is controlled by a central control system. In addition, because of security concerns, cameras have been mounted and installed at each location of mechanical control. The mechanical control devices and video cameras at each site communicate via Ethernet to their own switch. (For reasons of simplicity and clarity, we will assume that only video and control data reside on the network).

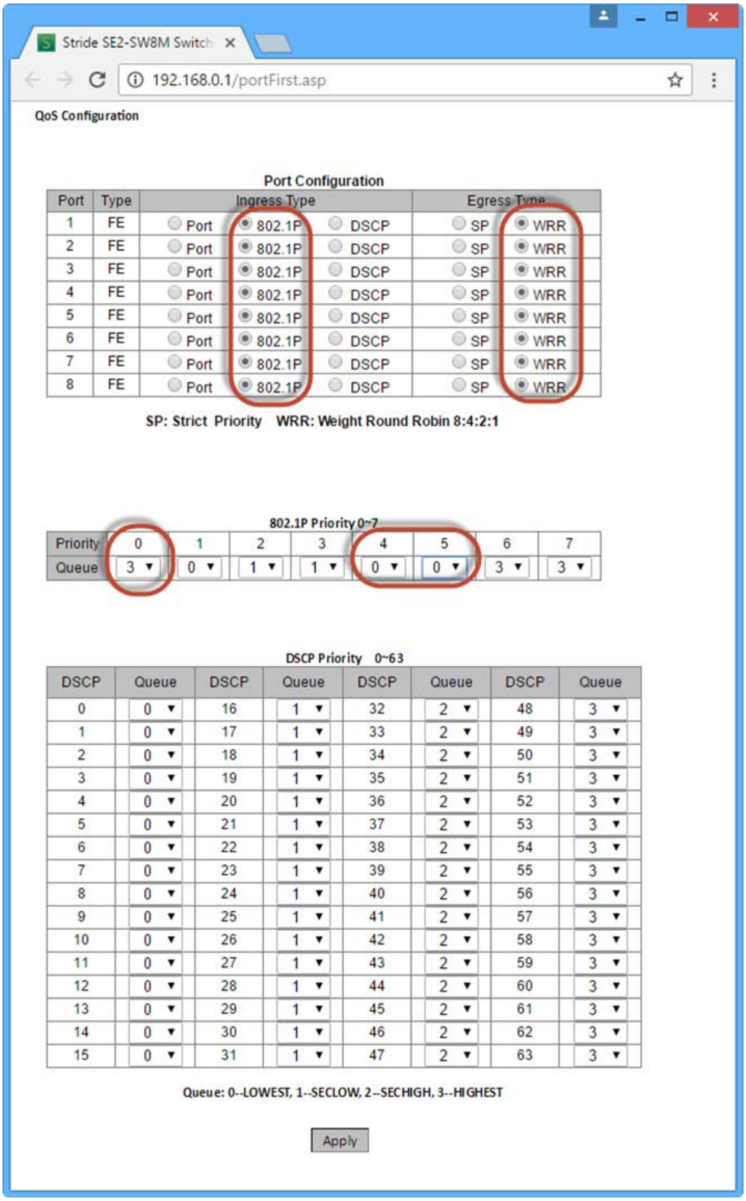
Should any of the mechanical control devices receive delayed control data from the central control system, the power plant can't generate the maximum energy that it is capable of. Customers will experience brown outs, and the plant will be looked upon with negative scrutiny. It is therefore very important that the video traffic created by the cameras not delay critical data.



Unless we configure the switch's priority queuing abilities, our switches perform to the best-effort network model. This means that the network will try to deliver all packets of information, but will not allocate switch resources according the timeliness of data for specific applications. Considering our control/video example, there is no guarantee that we can get the response time needed for control data if the video cameras are sending data at the same time. Our switches, though, are capable of prioritizing network traffic even if the devices (video cameras and control systems) do not support configuration of Quality of Service parameters

In our network, the control traffic is highest priority and the video traffic is low priority. In a more general network (commercial or enterprise rather than industrial control,) video traffic is usually given a high priority (4 or 5.) We'll adjust this by configuring the 802.1 priority-to-queue mapping. We'll map Priority 4 and 5 to the lowest priority queue, Queue 0.

For our example, the devices creating communication traffic do not have an assigned priority, that is, the control devices don't add a priority tag to the packets. So that traffic has Priority 0. By default in our switches, Priority 0 maps to the lowest priority queue. We will change this to map Priority 0 to the highest queue, Queue 3.



QoS Configuration

Port Configuration

Port	Type	Ingress Type			Egress Type	
1	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
2	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
3	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
4	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
5	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
6	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
7	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR
8	FE	○ Port	● 802.1P	○ DSCP	○ SP	● WRR

SP: Strict Priority WRR: Weight Round Robin 8:4:2:1

802.1P Priority 0~7

Priority	0	1	2	3	4	5	6	7
Queue	3 ▾	0 ▾	1 ▾	1 ▾	0 ▾	0 ▾	3 ▾	3 ▾

DSCP Priority 0~63

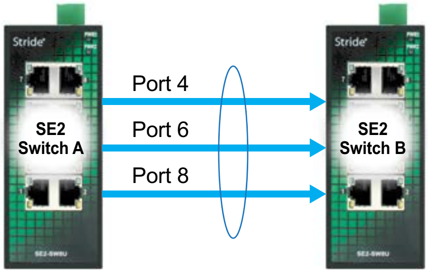
DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0	0 ▾	16	1 ▾	32	2 ▾	48	3 ▾
1	0 ▾	17	1 ▾	33	2 ▾	49	3 ▾
2	0 ▾	18	1 ▾	34	2 ▾	50	3 ▾
3	0 ▾	19	1 ▾	35	2 ▾	51	3 ▾
4	0 ▾	20	1 ▾	36	2 ▾	52	3 ▾
5	0 ▾	21	1 ▾	37	2 ▾	53	3 ▾
6	0 ▾	22	1 ▾	38	2 ▾	54	3 ▾
7	0 ▾	23	1 ▾	39	2 ▾	55	3 ▾
8	0 ▾	24	1 ▾	40	2 ▾	56	3 ▾
9	0 ▾	25	1 ▾	41	2 ▾	57	3 ▾
10	0 ▾	26	1 ▾	42	2 ▾	58	3 ▾
11	0 ▾	27	1 ▾	43	2 ▾	59	3 ▾
12	0 ▾	28	1 ▾	44	2 ▾	60	3 ▾
13	0 ▾	29	1 ▾	45	2 ▾	61	3 ▾
14	0 ▾	30	1 ▾	46	2 ▾	62	3 ▾
15	0 ▾	31	1 ▾	47	2 ▾	63	3 ▾

Queue: 0--LOWEST, 1--SECLOW, 2--SECHIGH, 3--HIGHEST

Port Trunk – Link Aggregation

The **Stride** SE2 series switches include a port trunk (link aggregation) feature that allows multiple ports on a switch to share traffic and provide instant fail over recovery in case one port fails.

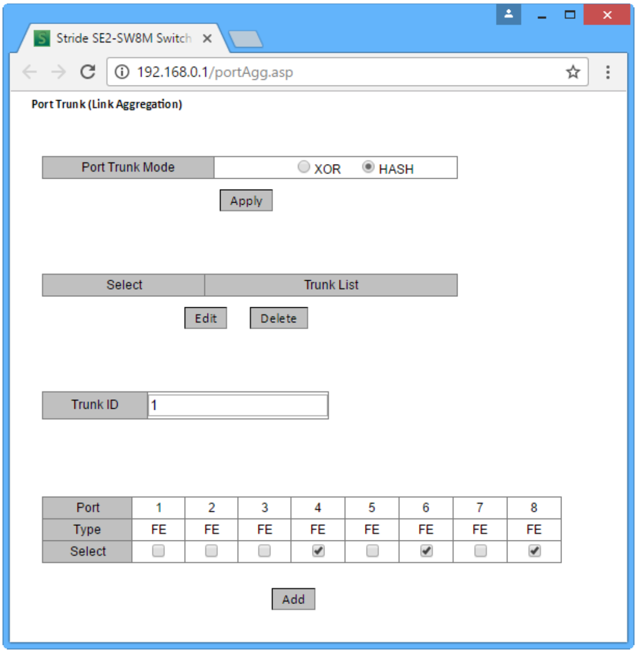
The total bandwidth of the Trunk Group is the combined bandwidth of the ports in the group.



When Switch A transmits to Switch B, Switch A will conduct a flow allocation algorithm to select one member port to transmit the messages. If the connection on one port in the group fails, the traffic borne by the port is reallocated to the other connected port(s) by the recalculated flow algorithm, XOR or HASH.

The allocation algorithms are not configurable. Typically, one would expect the XOR option to result in all traffic from a specific source (for example PLC1) to a specific destination (for example Remote IO 2) to always be allocated to the same port. In a network where two devices have significantly more traffic between them than other traffic on the network, the HASH option may provide more balanced traffic allocation. Neither method will result in a perfectly even distribution of traffic across the ports.

1. Port trunk and the following features are mutually exclusive. That is, to configure a port to participate in a Trunk Group, Disable the following features:
   - Port Monitoring
   - RSTP/STP
   - AD-Ring and AD-RP
   - DHCP Snooping Trust port
   - IGMP
   - GVRP
   - Port static multi-cast, Port static unicast
2. Gigabit ports may not be configured to participate in a Trunk Group.
3. A port may join only one Trunk Group.



Stride SE2-SW8M Switch

192.168.0.1/portAgg.asp

Port Trunk (Link Aggregation)

Port Trunk Mode	○ XOR ● HASH

Apply

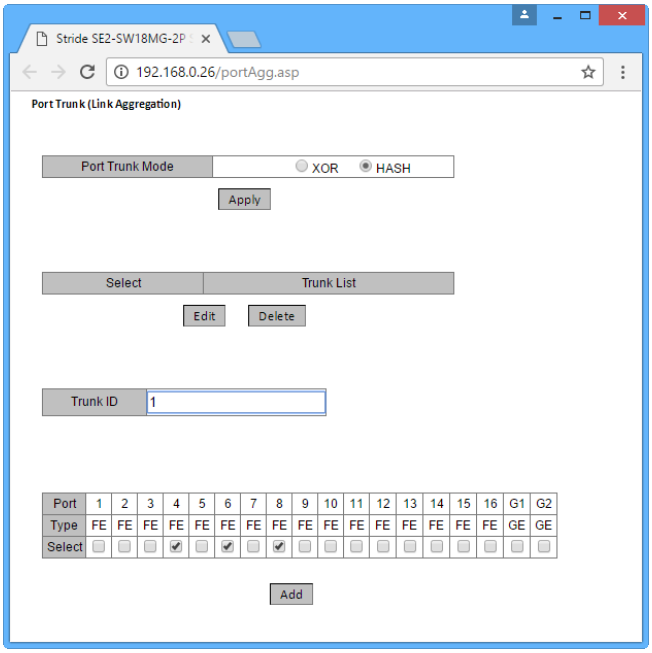
Select	Trunk List

Edit Delete

Trunk ID	1

Port	1	2	3	4	5	6	7	8
Type	FE	FE	FE	FE	FE	FE	FE	FE
Select	□	□	□	☑	□	☑	□	☑

Add



Stride SE2-SW18MG-2P

192.168.0.26/portAgg.asp

Port Trunk (Link Aggregation)

Port Trunk Mode	○ XOR ● HASH

Apply

Select	Trunk List

Edit Delete

Trunk ID	1

Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	G1	G2
Type	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	FE	GE	GE
Select	□	□	□	☑	□	☑	□	☑	□	□	□	□	□	□	□	□	□	□

Add

Port Rate

In addition to QoS, Port Rate limiting may be used to manage network traffic flow. Ingress ports limit the rate of selected message types and Egress ports limit the rate of all messages.

Rate limitation can be configured to apply to the following types of messages on Ingress ports:

Unknown Unicast Frame (UUF): messages whose destination MAC has not been learned and has not been statically added to the FDB.

Unknown Multicast Frame (UMF): messages whose destination MAC has not been learned by IGMP Snooping or GMRP and has not been added to the Static FDB Multicast table.

Broadcast Frame (BF): messages with the destination MAC FF: FF: FF: FF: FF: FF.

Multicast Frame (MF): messages whose destination MAC has been learned by IGMP or GMRP, or has been statically added to the Static FDB Multicast table.

Unicast Frame (UF): Messages whose destination MAC address has been learned or has been added to the FDB.

Imagine switch traffic as tokens that are added to a bucket in the switch. Tokens are added to the bucket at a certain rate and the bucket has a certain capacity. If the number of tokens exceeds the capacity of the bucket, the bucket will overflow and the mechanism will stop accumulating tokens.

Each token allows sending a certain number of bits. When a message is transmitted, a number of tokens equal to the length of the message are removed from the bucket. If there aren't enough tokens in the bucket, the message may be held until there are sufficient tokens or the message may be dropped.

Port rate configuration uses token buckets to control flow. If Port Rate is set for a port, the messages at this port will be processed by the token bucket method before forwarding. If there are sufficient tokens, the messages will be transmitted, or else they will be dropped.

AD-Ring

By default, RSTP is Enabled on all ports. When configuring a pair of ports to participate in an AD-Ring, RSTP must be Disabled on those ports.

Like RSTP, an AD-Ring increases network reliability by providing an alternate path for message flow in the event of a network segment failure. When a ring port detects a communications break, it quickly notifies the other switches in the ring. Messages are automatically rerouted through the alternate ring path within milliseconds.

RSTP/STP (Rapid Spanning Tree Protocol) is more flexible than a ring configuration, but recovery times for spanning trees may be in the hundreds of milliseconds. The AD-Ring protocol exchanges topological flexibility for recovery times in the tens of milliseconds.

There are two types of AD-Rings: port-based (AD-Port-Ring) and VLAN-based (AD-VLAN-Ring).

AD-Port-Ring: specifies a port to forward or block packets.

AD-VLAN-Ring: specifies a port to forward or block the packets of a specific VLAN. This allows multiple VLANs on a tangent port, that is, one port is part of different redundant rings based on different VLANs.

AD-Port-Ring and AD-VLAN-Ring cannot be used together.

Concepts

Master station: A ring has only one master station. The master station forwards AD-Ring packets and detects the current status of the ring.

Master port: On the master station, the first port whose link status changes to up is called the master port. It is in forwarding state.

Slave port: On the master station, the port whose link status changes to up if a failure is detected is called the slave port. When the ring is closed, the slave port is in blocking state. When a ring is open due to a link or port failure, the status of the slave port changes to forwarding.

Slave station: A ring can include multiple slave stations. Slave stations listen to and forward AD-Ring packets and report fault information to the master station.

Backup port: The port for communication between AD-Rings is called a backup port.

Master backup port: When a ring has two backup ports, the backup port with the larger MAC address is the master backup port. It is in forwarding state.

Slave backup port: When a ring has two backup ports, the backup port with the smaller MAC address is the Slave backup port. It is in blocking state.

Forwarding state: If a port is in forwarding state, the port can both receive and send data.

Blocking state: If a port is in blocking state, it can only receive data, but not send data.

Implementation of AD-Ring

The master port on the master station periodically forwards AD-Ring packets to detect ring status. If the slave port of the master station receives the packets, the ring is closed; otherwise, the ring is open.

When a ring is closed, the master port of the master station is in forwarding state, the slave port in blocking state, and all ring ports of slave stations are in forwarding state.

A ring may be open in the following cases:

- The master port of the master station fails. The statuses of the slave port on the master station and all ring ports of slave stations change to forwarding.
- The slave port of the master station fails. The statuses of the master port on the master station and all ring ports of slave stations change to forwarding.
- Another port or link fails. The statuses of the two ports of the master station and all up ports of slave stations change to forwarding.

AD-Ring configurations must meet the following conditions:

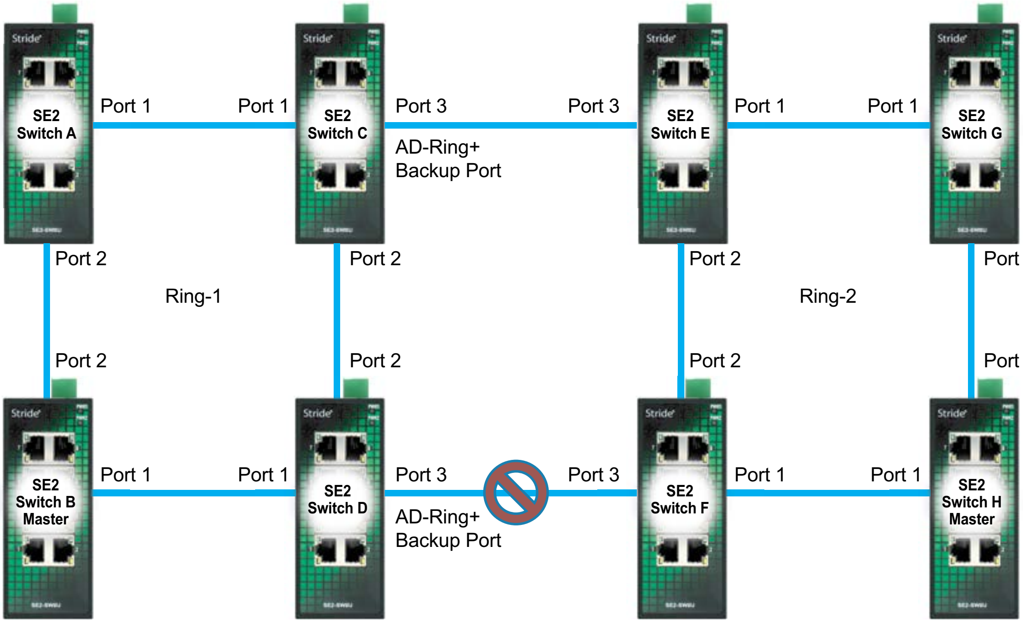
- All switches in the same ring must have the same Domain ID.
- Each ring can have only one master station and multiple slave stations
- Two ports must be configured on each switch for a ring
- For two connected rings, backup ports can be configured only in one ring
- A maximum of two backup ports can be configured in one ring.
- On a switch, only one backup port can be configured for one ring

CAUTION: Port trunk and ring are mutually exclusive. The ports added to a trunk group cannot be configured as a ring port, and a ring port cannot be added to a trunk group.

Implementation of AD-Ring+

AD-Ring+ can provide backup for two AD-rings, as shown below. One backup port is configured on Switch C and on Switch D. Which port performs as the master backup port depends on the MAC addresses of the two ports. If the master backup port or its link fails, the slave backup port will forward packets, preventing loops and ensuring normal communication between redundant rings.

See the example at the end of this section for details on configuring this example network.



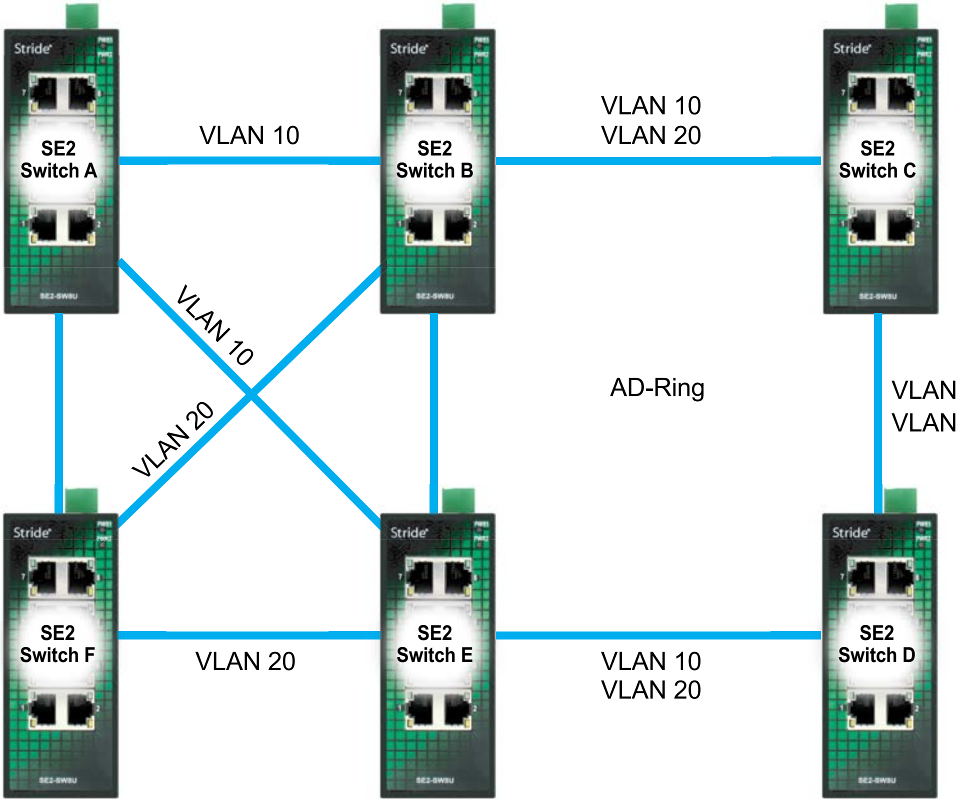
Implementation of AD-VLAN-Ring

AD-VLAN-Ring allows the packets of different VLANs to be forwarded in different paths. Each forwarding path for a VLAN forms an AD-VLAN-Ring. Different AD-VLAN-Rings can have different master stations. As shown below, two AD-VLAN-Rings are configured.

Ring links of AD-VLAN-Ring10: AB-BC-CD-DE-EA.

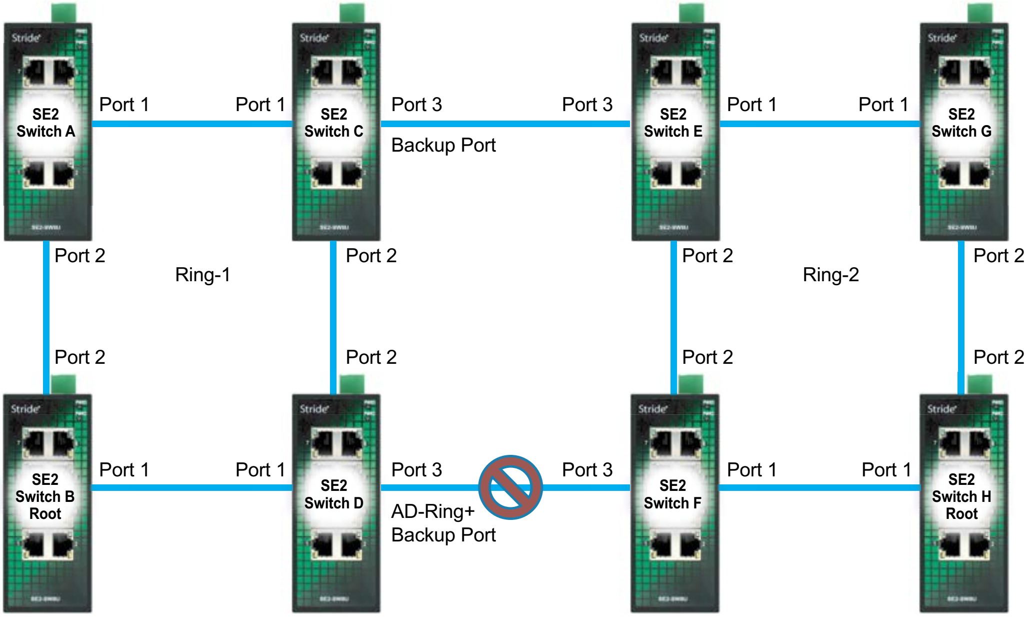
Ring links of AD-VLAN-Ring20: FB-BC-CD-DE-EF.

The two rings are tangent at link BC, CD, and DE. Switch C and Switch D share the same ports in the two rings, but use different logical links based on VLAN.

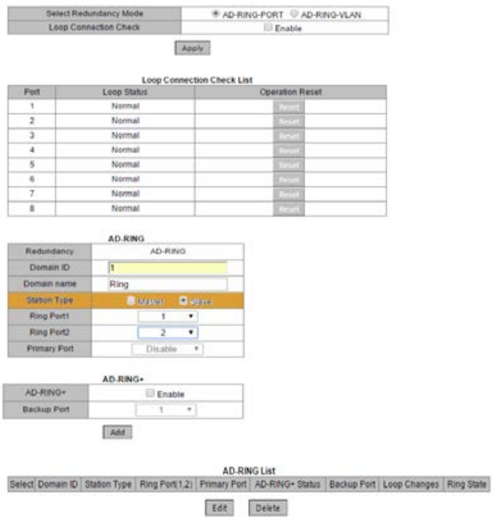


AD-Ring Example

As shown below, Switch A, B, C, and D form Ring 1; Switch E, F, G, and H form Ring 2; CE and DF are the backup links of Ring 1 and Ring 2.



Configuration on Switch A:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	1
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

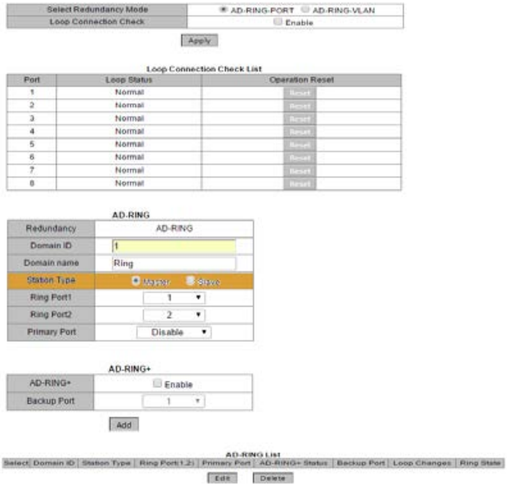
AD-RING+

AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switch B:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	1
Domain name	Ring
Station Type	● Master ○ Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

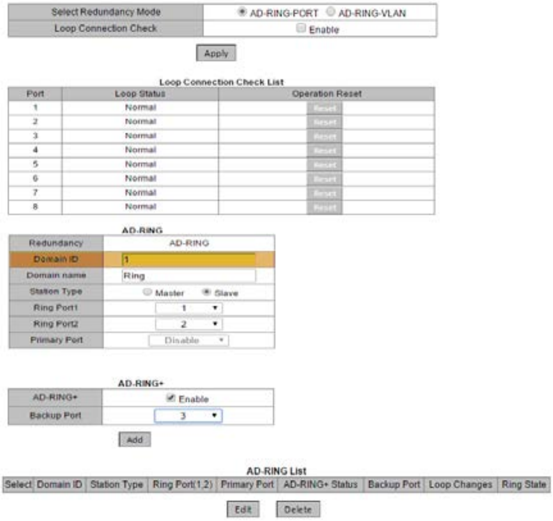
AD-RING+

AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Configuration on Switches C and D:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Apply

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	1
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

AD-RING+

AD-RING+	☑ Enable
Backup Port	3

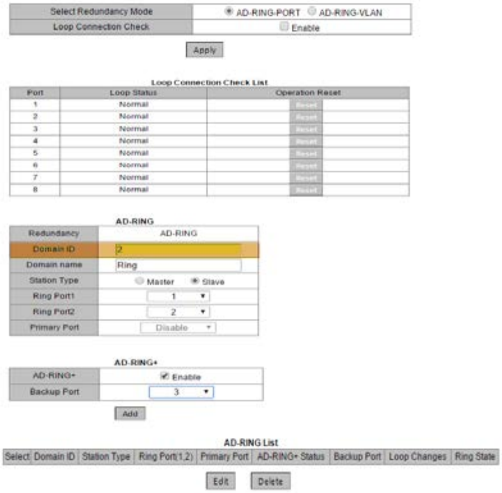
Add

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Edit Delete

Configuration on Switches E and F:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Apply

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	2
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1
Ring Port2	2
Primary Port	Disable

AD-RING+

AD-RING+	☑ Enable
Backup Port	3

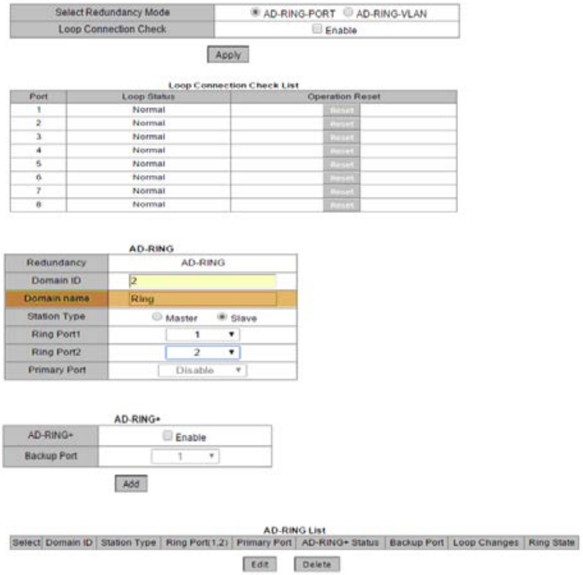
Add

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Edit Delete

Configuration on Switches G:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Apply

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	2
Domain name	Ring
Station Type	○ Master ● Slave
Ring Port1	1 ▾
Ring Port2	2 ▾
Primary Port	Disable ▾

AD-RING+

AD-RING+	□ Enable
Backup Port	1 ▾

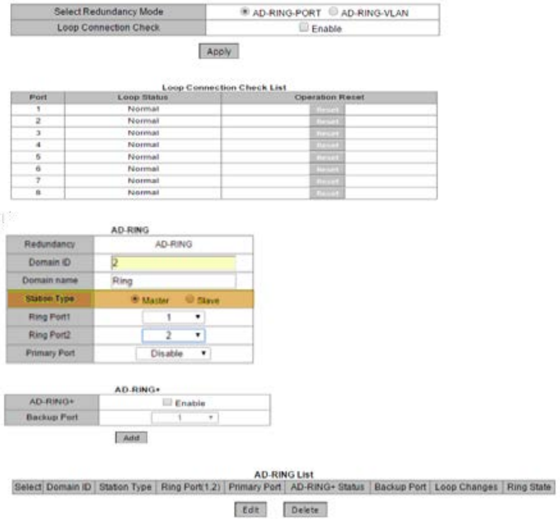
Add

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Edit Delete

Configuration on Switches H:



Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Apply

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Normal	Reset
6	Normal	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	2
Domain name	Ring
Station Type	● Master ○ Slave
Ring Port1	1 ▾
Ring Port2	2 ▾
Primary Port	Disable ▾

AD-RING+

AD-RING+	□ Enable
Backup Port	1 ▾

Add

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State

Edit Delete

AD-RP

AD-RP is an IEC62439-6 compliant redundant ring protocol. It adopts a distributed ring network protection solution for **Stride** SE2 series switches. When a link fails, the network can recover within 20ms to guarantee stable and reliable communication.

One switch may participate in multiple AD-RP rings.

NOTE: *By default, RSTP is Enabled on all ports. When configuring a pair of ports to participate in AD-RP, RSTP must be Disabled on those ports.*

Concept

INIT: the initial state of the switch

Root: there is one and only one root in the ring network. The root is elected by switches in the network and changes with network topology. The root periodically sends out an Announce message and other devices forward this message to guarantee topology stability.

B-Root: The switch in which a ring port is Link-down, or a ring port deteriorates (which means the number of CRC messages exceeds the threshold)

Normal: Except Root and B-Root, the rest are Normal switches in a normal communication ring network

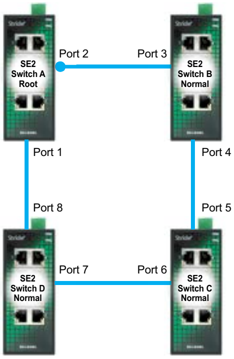
Backup port: the communication ports between AD-RP rings. Two or more backup ports can be configured. All backup ports must be in the same AD-RP ring. The backup port that links up first is the master backup port and is in Forward state, and other backup ports are slave backup ports and are in Block State.

Implementation

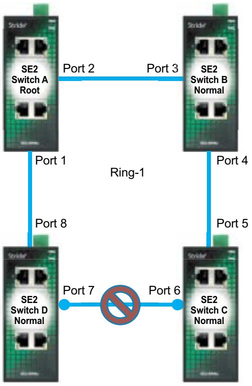
AD-RP protocol determines switch roles by forwarding Announce messages to guarantee a loop-free redundant network.

AD-RP configuration must meet the following conditions:

- All switches in a ring must have a same domain ID
- There is one and only one Root in a ring, but there may be multiple B-Roots or Normals.
- There are only two ring ports in each switch in a ring
- For two connected rings, backup ports can only be set in one ring
- A ring allows multiple backup ports
- Each switch in a ring can only set one backup port



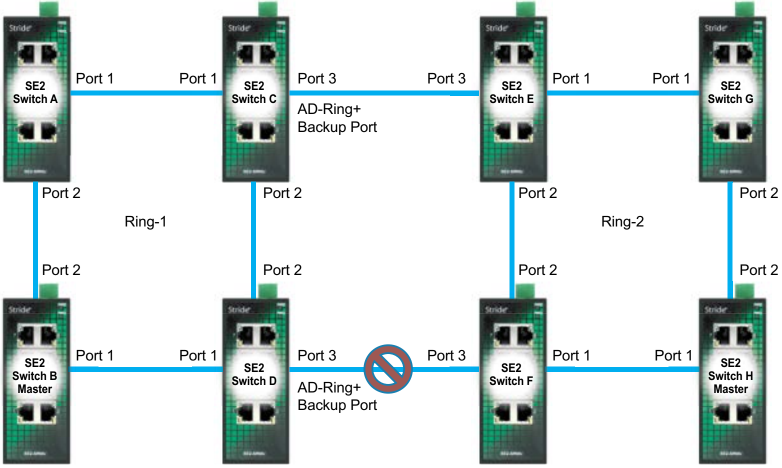
1. In the initial state, all switch are in INIT state
2. In the ring network, switches compare the Announce message forwarded between them, and then elect Switch A to be Root due to its optimum configuration. The ring port 1 in Root that links up first is the Forwarding port, while the ring port 2 is blocked. Other switches are B-Root or Normal. The two ring ports in B-Root/Normal are both in Forward state.



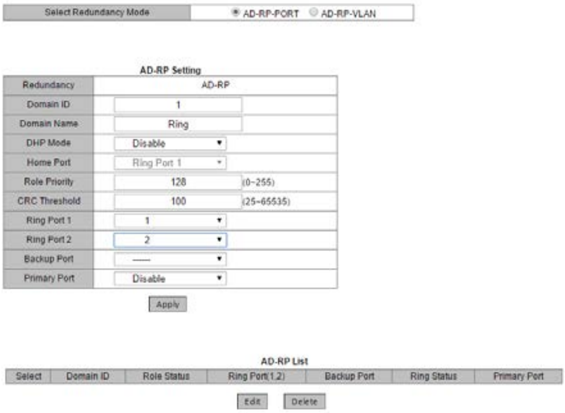
3. If the link between switches C and D fails, for example, immediately switch A will change from Root to Normal AND either switch C or D will be elected the new Root. Ports 6 and 7 will be blocked. If D is root, then C will be B-Root.

CAUTION: Link state changes affect the status of all ring ports.

AD-RP protocol can provide backup between two AD-RP rings; each switch can have a Backup Port configured. The master backup port is the forwarding port, and the other backup ports are blocked. If the master backup port/link fails, the system will select a slave backup port to forward data, guaranteeing the normal communication between redundant rings.



Switch A and Switch B configuration:



Select Redundancy Mode ● AD-RP-PORT ○ AD-RP-VLAN

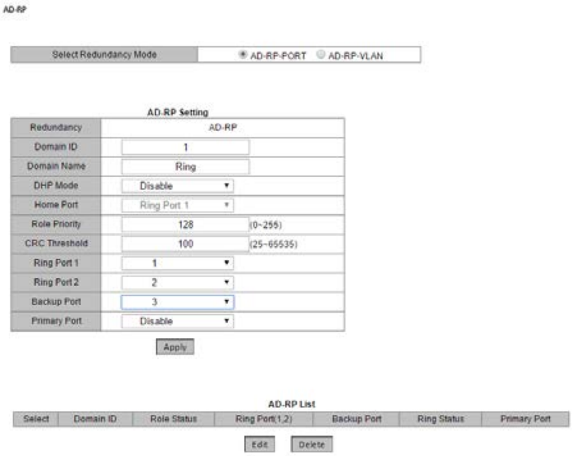
AD-RP Setting

Redundancy	AD-RP
Domain ID	1
Domain Name	Ring
DHP Mode	Disable
Home Port	Ring Port 1
Role Priority	128 (0~255)
CRC Threshold	100 (25~65535)
Ring Port 1	1
Ring Port 2	2
Backup Port	——
Primary Port	Disable

AD-RP List

Select	Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Primary Port

Switch C and Switch D configuration:



AD-RP

Select Redundancy Mode	● AD-RP-PORT ○ AD-RP-VLAN

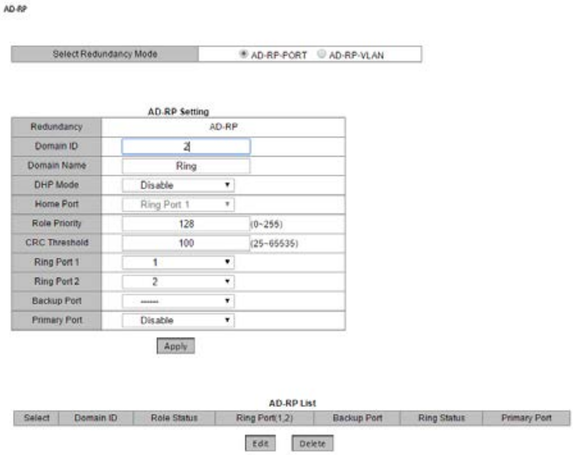
AD-RP Setting

Redundancy	AD-RP	
Domain ID	1	
Domain Name	Ring	
DHP Mode	Disable	
Home Port	Ring Port 1	
Role Priority	128	(0~255)
CRC Threshold	100	(25~65535)
Ring Port 1	1	
Ring Port 2	2	
Backup Port	3	
Primary Port	Disable	

AD-RP List

Select	Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Primary Port

Switch E, F, G, H configuration:



AD-RP

Select Redundancy Mode	● AD-RP-PORT ○ AD-RP-VLAN

AD-RP Setting

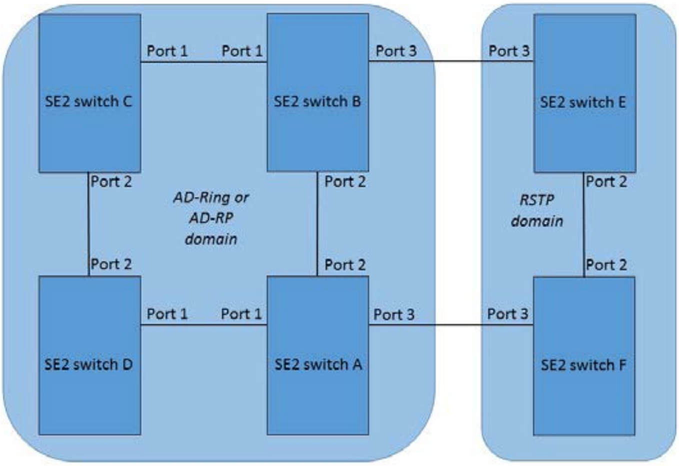
Redundancy	AD-RP	
Domain ID	2	
Domain Name	Ring	
DHP Mode	Disable	
Home Port	Ring Port 1	
Role Priority	128	(0~255)
CRC Threshold	100	(25~65535)
Ring Port 1	1	
Ring Port 2	2	
Backup Port	------	
Primary Port	Disable	

AD-RP List

Select	Domain ID	Role Status	Ring Port(1,2)	Backup Port	Ring Status	Primary Port

RSTP/STP Transparent Transmission

AD-Ring and AD-RP are proprietary redundancy solutions and as such can't coexist with RSTP/STP on a network. But to accommodate traffic to/from an AD-Ring or AD-RP, the **Stride** SE2 series switches provide an RSTP/STP Transparent Transmission feature that will transmit RSTP/STP BPDUs across the ports participating in AD-Ring or AD-RP.



Switches A, B, C, and D form an AD-Ring. When RSTP/STP Transparent Transmission is enabled on Switch A and B ports, Switches E and F can receive RSTP BPDUs from each other, detect loops, and calculate spanning trees.

Link Check

The Link Check feature verifies that ports participating in a redundancy protocol (RSTP/STP, AD-Ring or AD-RP) transmit data normally. Note that only ports configured to participate in a redundancy protocol may enable Link Check.

When Link Check is enabled on a port, the status may be monitored using Modbus TCP, EtherNet/IP or SNMP.

Status:

Normal Link: Link Check is enabled and the port is transmitting/receiving data properly.

Receive Fault: Link Check is enabled and the port is NOT transmitting/receiving data properly.

Disable: Link Check is not enabled on this port.

Virtual Cable Check

The Virtual Cable Tester uses Time Domain Reflectometry to detect twisted pair status. It transmits a pulse signal along the cable and detects the reflection of the pulse signal. If a failure has occurred in the cable, the pulse will be reflected back to the switch port and the user interface will display the distance to the failure in the Distance to Fault column, shown in meters.

The following types of cable faults can be detected and displayed in the status column:

Short: short circuit, two or more wires are shorted.

Open: open circuit, there may be broken wires in the cable.

Imped: impedance mismatch. The characteristic impedance of Cat5e cable is 100 ohms. The impedance of the terminators at both ends of the cable must be 100 ohms to avoid wave reflection and data errors.

Port Security

Port Security is a MAC-address-based security mechanism for network access control. This mechanism compares the source MAC address of received messages to the list of allowable MAC addresses. A message with a source MAC addresses that isn't included in the Allowable MAC address table is dropped.

The switch supports 32 allowable MAC addresses on each port.

Port CRC Protect

The switch can be configured to protect itself from expending effort tending traffic on a port that's experiencing problems. CRC errors are symptoms of a problem with traffic. This may result from a problem with the integrity of the physical condition (failing cable or connector).

- a malfunctioning Network Interface Controller
- software problems on a connected device
- port configured for Half Duplex rather than Full Duplex communications
- other network problems

Loop Detect

If a port is **not** configured to participate in a redundancy protocol, loop detect protects the network from failing due to unintended loops. When loop detect is enabled on a port, the switch will disable that port if traffic indicating a loop in the network is detected. When auto recover is enabled, the switch will re-enable the port and check for loops after a pause.

MAC Address Forwarding Database

Ordinarily the switch will automatically learn the MAC addresses of connected devices by examining the messages it receives. These automatically learned addresses will be deleted from the MAC table if no messages have been received from or transmitted to them for a duration defined by the MAC Aging Time. The MAC Aging Time may be configured between 15 and 3600 seconds, but it must be a multiple of 15.

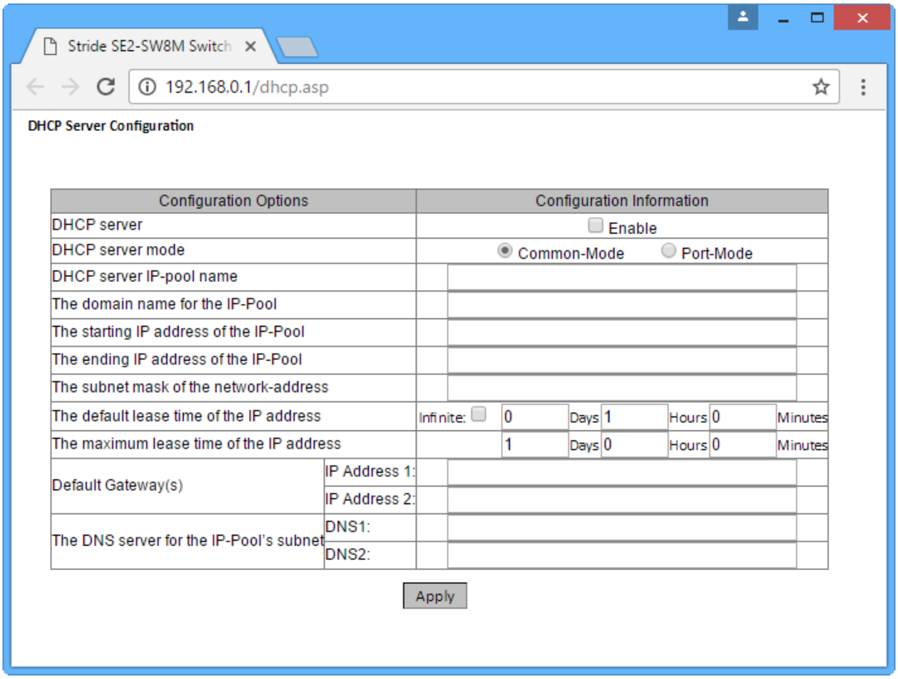
DHCP Server

As networks grew in scale and complexity, DHCP (Dynamic Host Configuration Protocol) was developed as a mechanism to automatically assign IP addresses and subnet masks to devices as they connect to the network.

DHCP employs a client-server communication model. The client sends a configuration request to the server, and then the server replies with configuration parameters such as IP address and subnet mask.

A **Stride** SE2 series switch may be configured to be the DHCP server to a network.

CAUTION: Remember that in DHCP, messages are transmitted as broadcasts, so the DHCP client and the Stride SE2 series switch acting as the DHCP server must be in the same network segment.



DHCP Server Configuration

Configuration Options		Configuration Information
DHCP server		□ Enable
DHCP server mode		● Common-Mode ○ Port-Mode
DHCP server IP-pool name		
The domain name for the IP-Pool		
The starting IP address of the IP-Pool		
The ending IP address of the IP-Pool		
The subnet mask of the network-address		
The default lease time of the IP address		Infinite: □ 0 Days 1 Hours 0 Minutes
The maximum lease time of the IP address		1 Days 0 Hours 0 Minutes
Default Gateway(s)	IP Address 1:	
	IP Address 2:	
The DNS server for the IP-Pool's subnet	DNS1:	
	DNS2:	

DHCP supports two types of IP address allocation mechanisms, Port-Mode and Common -Mode.

Port Mode: the network administrator statically binds a fixed IP address to a port. This is helpful for clients such as a router port configured as a Gateway.

Common Mode: DHCP server dynamically allocates an IP address to a client. The IP address can be allocated to a client permanently or with a limited lease period. When the lease expires, the client needs to request a new IP address.

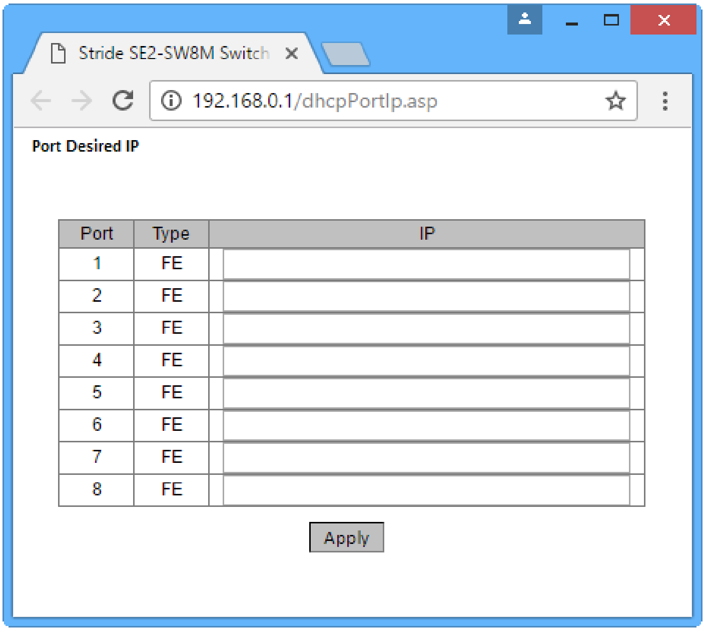
The DHCP server selects an IP address from an address pool and allocates it together with other parameters to the client. The IP address allocation sequence is as follows:

1. The IP address statically bound to the client MAC address or the port ID connecting to the server.
2. The IP address that is recorded in the DHCP server that was previously allocated to the client.
3. The IP address that is specified in the request message sent from the client.
4. The first allocable IP address found in the address pool.

Port Desired IP Configuration

When DHCP Server is Enabled, and Port-Mode is selected as the Server Mode, the Port Desired IP table setting statically assigns an IP address to a port. When a port receives a request message from a client, the IP address bound to the port will be allocated to the client. This IP allocation mode has the highest priority and the lease period is 1000 days 23 hours and 59 minutes.

Caution: The IP address assigned to a port and the DHCP server must be in same segment.



Port Desired IP

Port	Type	IP
1	FE	
2	FE	
3	FE	
4	FE	
5	FE	
6	FE	
7	FE	
8	FE	

If a subnet mask and Default Gateway(s) are entered in the DHCP Server Configuration table, these values will be assigned to devices requesting host configuration from the switch.

The DNS-server for the IP-Pool's subnet

When an address is provided as a name, the name needs to be resolved to an IP address. A DNS server will accomplish this. DHCP address pool can configure max two DNS addresses.

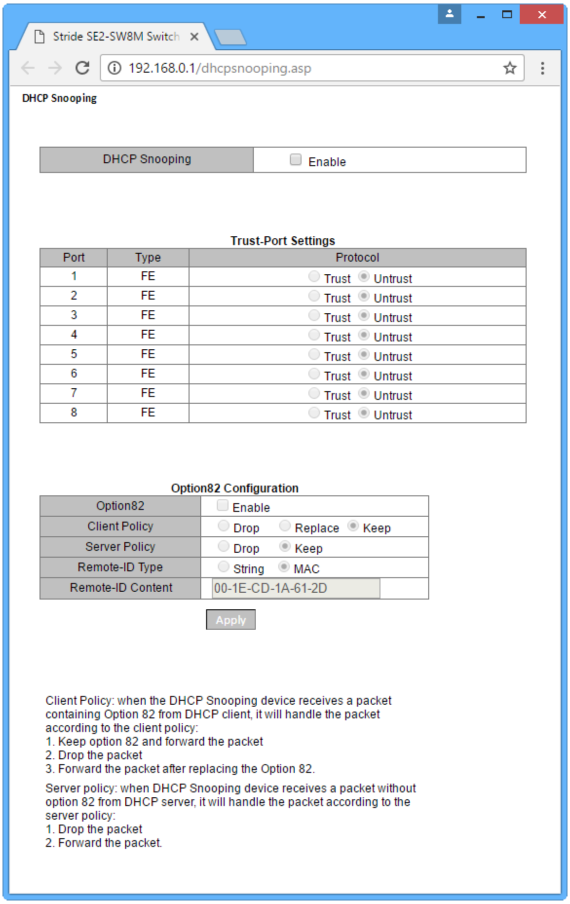
DHCP Snooping

DHCP snooping is a feature to prevent unexpected DHCP servers from providing IP addresses to DHCP clients. Unacceptable DHCP messages will be dropped at Untrusted ports.

Trusted port: a port that connects with the valid DHCP server directly or indirectly. Trusted port normally forwards the request messages of DHCP clients and the response messages of DHCP servers to guarantee that DHCP clients can obtain valid IP addresses.

Untrusted port: any port that is not connected to a known DHCP server. Untrusted ports will not forward DHCP requests and responses.

Note 1: *A switch configured to perform DHCP snooping may not be configured as a DHCP server.*
Note 2: *A switch configured to perform DHCP snooping may not be configured to obtain its IP address by DHCP*
Note 3: *A switch configured to perform DHCP snooping may not be configured to participate in a Trunk Group.*



DHCP Snooping

DHCP Snooping	□ Enable

Trust-Port Settings

Port	Type	Protocol
1	FE	○ Trust ● Untrust
2	FE	○ Trust ● Untrust
3	FE	○ Trust ● Untrust
4	FE	○ Trust ● Untrust
5	FE	○ Trust ● Untrust
6	FE	○ Trust ● Untrust
7	FE	○ Trust ● Untrust
8	FE	○ Trust ● Untrust

Option82 Configuration

Option82	□ Enable
Client Policy	○ Drop ○ Replace ● Keep
Server Policy	○ Drop ● Keep
Remote-ID Type	○ String ● MAC
Remote-ID Content	00-1E-CD-1A-61-2D

Client Policy: when the DHCP Snooping device receives a packet containing Option 82 from DHCP client, it will handle the packet according to the client policy:
1. Keep option 82 and forward the packet
2. Drop the packet
3. Forward the packet after replacing the Option 82.

Server policy: when DHCP Snooping device receives a packet without option 82 from DHCP server, it will handle the packet according to the server policy:
1. Drop the packet
2. Forward the packet.

Option 82 Configuration

Option 82 (Relay Agent Information Entry) allows DHCP traffic from switches that are not directly connected to a DHCP server to successfully negotiate network settings across a more complicated network while maintaining the security that DHCP snooping provides.

Client Policy: when the DHCP Snooping device receives a packet containing Option 82 from DHCP client, it will handle the packet according to the client policy:

1. Keep option 82 and forward the packet
2. Drop the packet
3. Forward the packet after replacing the Option 82.

Server policy: when DHCP Snooping device receives a packet without option 82 from DHCP server, it will handle the packet according to the server policy:

1. Drop the packet
2. Keep the packet and forward it.

The Option 82 field on **Stride** SE2 series switches includes two sub-options: sub-option 1 (Circuit ID) and sub-option 2 (Remote ID). The formats of two sub-options are shown below:

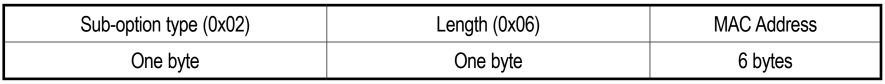
Sub-option 1 contains the VLAN ID and number of the port that receives the request message from the DHCP client. The format of the sub-option 1 field within the message is:

Sub-option type (0x01)	Length (0x04)	VLAN ID	Port Number
One byte	One byte	Two bytes	Two bytes

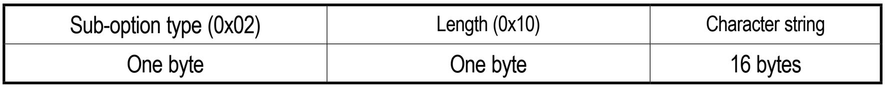
VLAN ID: On a DHCP Snooping device, the VLAN ID of the port that receives the request message from the DHCP client

Port number: On a DHCP Snooping device, the number of the port that receives the request message from the DHCP client

The content of Sub-option 2 includes the MAC address of the DHCP Snooping device that receives the request message from the DHCP client, or the character string configured by users, as shown in below



Sub-option type (0x02)	Length (0x06)	MAC Address
One byte	One byte	6 bytes



Sub-option type (0x02)	Length (0x10)	Character string
One byte	One byte	16 bytes

Sub-option type: 2

Length: the number of bytes that Sub-option 2 content occupies. The MAC address occupies 6 bytes and character string occupies 16 bytes.

MAC address: the MAC address of the DHCP Snooping device that receives the request message from the DHCP client.

Character string: 1-16 characters. This character string is configured. on the DHCP Snooping page.

Chapter 5

Switch Management and Network Information

In this Chapter...

Switch Management and Network Information

Chapters 3 and 4 detail features that affect the traffic across the switch. **Stride** managed switches also have many features that assist in maintaining the network itself. This chapter describes these network management features.

LLDP

Link Layer Discovery Protocol provides a standard network discovery method. Network information is shared among connected devices and saved to respond to queries from network management system devices.

Information can only be displayed when both this switch and neighbor devices have LLDP enabled.

ARP

The switch management interface maintains an ARP table listing hosts that have accessed the switch management interface.

In general, the switch will learn ARP entries automatically without need of static entry configuration.

Max 512 total ARP entries are supported, with no more than 256 static entries. When the number of ARP entries exceeds 512, any new entry will replace the oldest dynamic entry.

IP addresses configured as static entries must be on the same subnet as the switch's IP address.

SNTP

Simple Network Time Protocol calibrates time by requests and responses between servers and clients. The switch will be a client to calibrate time according to the messages from the server. Up to four time servers may be configured on the switch but only a single time server is in an active state, any other configured servers will be inactive. The switch sends a request to all configured servers and the first to respond is assigned as the active server.

SSH Server

SSH (Secure Shell) encrypts switch management messages to prevent information disclosure. SSH encrypts only Command Line interface communications, not browser based switch management communication.

A Local Key Value may be generated by the switch and copied to the devices that will be allowed to access switch management functions. Or, the key may be generated by the connecting device and copied into the switch, typically using a key generation application such as PuTTYgen.

If the key will be generated by the switch and copied to the devices allowed to access switch management:

1. Disable SSH
2. Click the Set SSH Server button
3. Enable SSH
4. Configure:

- Authentication Retry – the number of unsuccessful login attempts that will be allowed before disabling access to the switch management interface.
- Time Out – the number of minutes of inactivity before terminal sessions automatically logout to prevent unauthorized access. The default is 5 minutes.

5. Copy the Local Key Value to the devices that are allowed to access switch management.
6. Add SSH Users on the SSH User Manager page (see below)

If the key will be generated by the connected device:

1. Enter a Name for the new key on the Key Configuration page.
2. Copy the key from the connected device to the Key Value field on the Key Configuration page
3. The key now appears in the Public Key List on the User Manager page.
4. Add SSH Users assigned to that key on the User Manager page.

Adding SSH Users on the User Manager page:

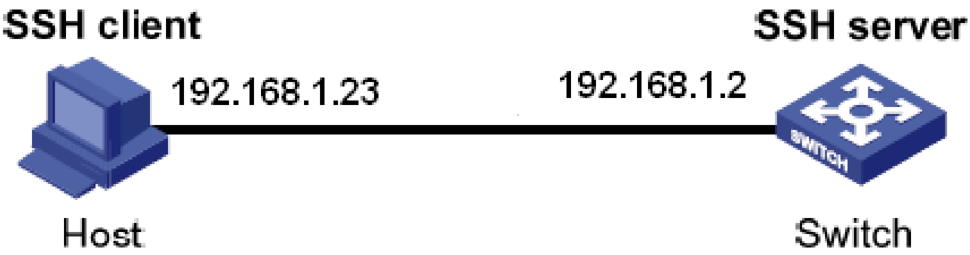
1. Enter a User name (login name)
2. Select either

- Password – Enter the Password that this User will type to login from a connected device
- Public Key – Select a key from the Public Key List of keys configured on the Key Configuration page.

3. Click Add to add this new user.

Typical configuration examples

The Host works as the SSH client to request a local connection with Switch, as shown below.



SSH USER with Authentication Type "Password"

1.On the SSH Server configuration page:

a) Disable SSH.

b) Click the Set SSH Server button to create a new Key Value.

c) Enable SSH.

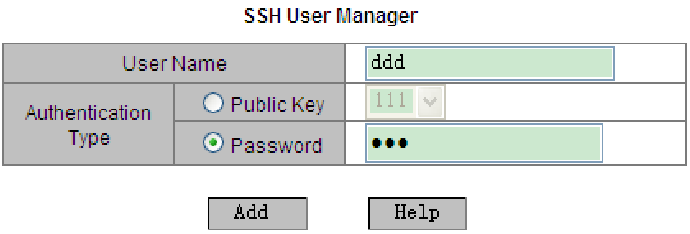
d) Click Apply

2. On the SSH User Manager page:

a) Enter user name ddd.

b) Choose the authentication type of "Password".

c) Enter password 444.



SSH User Manager

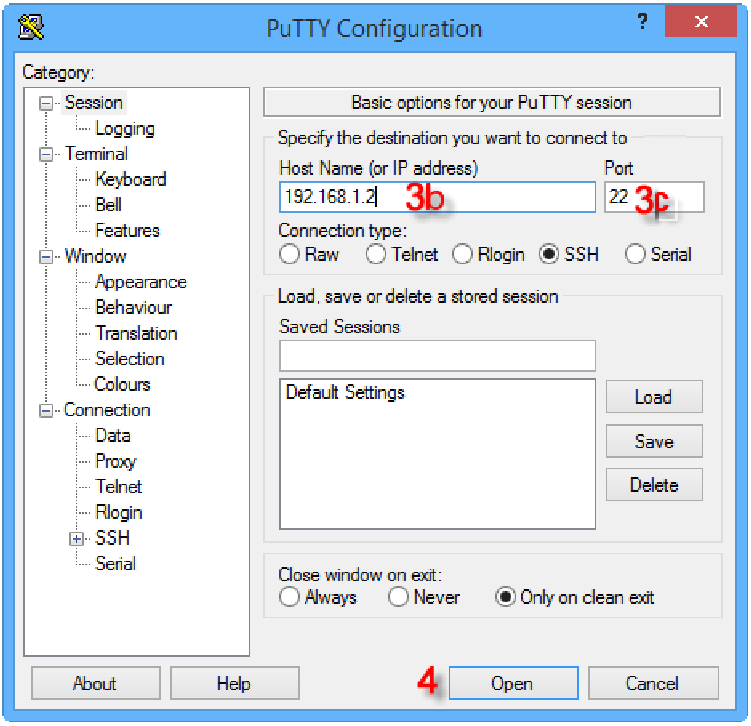
User Name		ddd
Authentication Type	○ Public Key	111
	● Password	•••

3. Establish the connection with the SSH server.

   a) Open the terminal application, PuTTY.exe in our example.

   b) Enter the switch management IP address in the Host Name field, 192.168.1.2 is the default, we are using 192.168.1.2 in this example.

   c) Enter port 22 and select SSH connection type.



PuTTY Configuration

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - Telnet
  - Rlogin
  - SSH
  - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.2 3b

Port: 22 3c

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

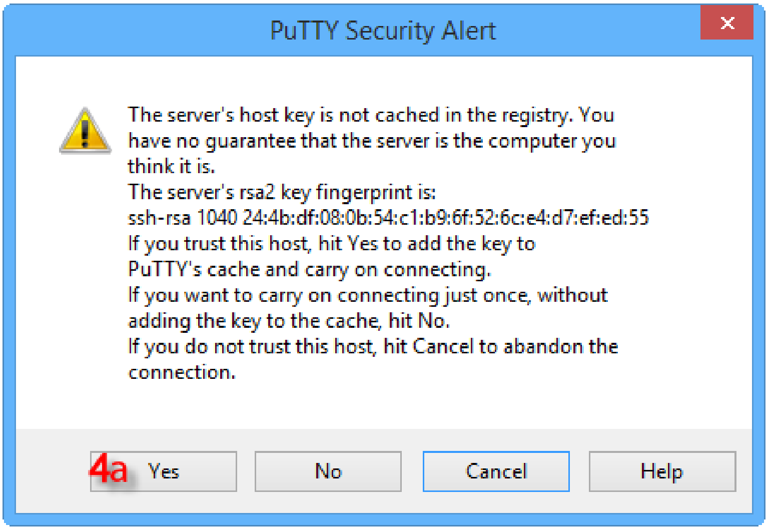
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

4. Click <Open> button and the following warning message appears.

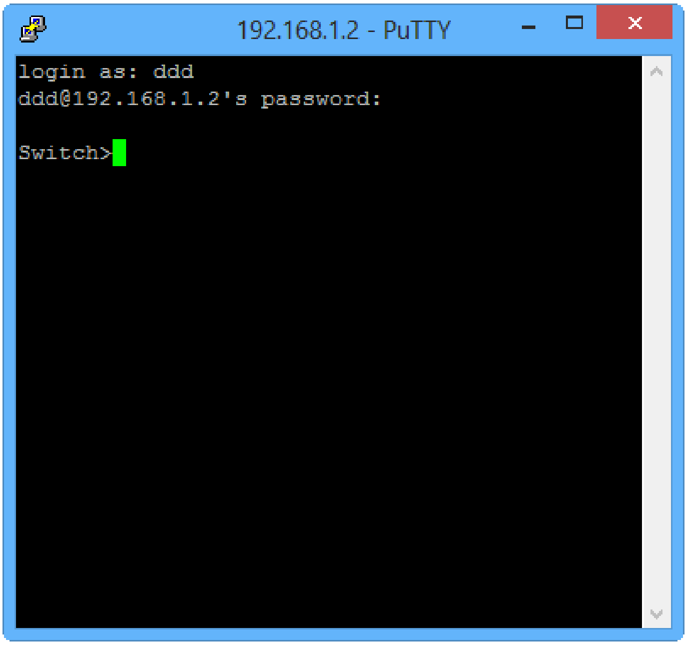
a.)Click "Yes".



PuTTY Security Alert

The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1040 24:4b:df:08:0b:54:c1:b9:6f:52:6c:e4:d7:ef:ed:55
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

5. Input the user name "ddd" and the password "444" to enter the switch configuration interface, as shown below.



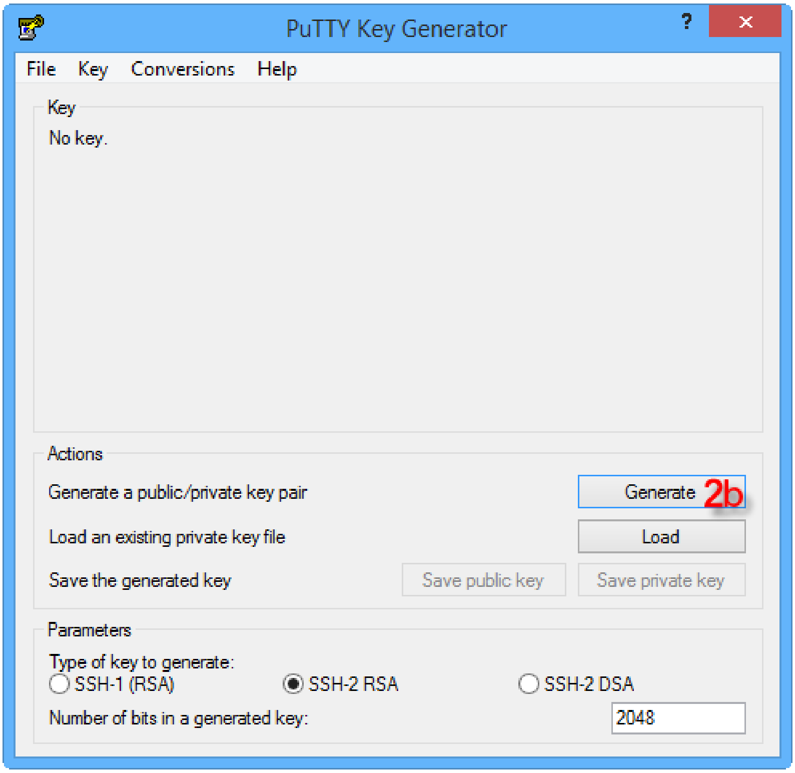
192.168.1.2 - PuTTY

```
login as: ddd
ddd@192.168.1.2's password:

Switch>
```

SSH user with authentication type "Public Key"

1. On the SSH Server configuration page:
   - Disable SSH.
   - Click the Set SSH Server button to create a new Key Value.
   - Enable SSH.
   - Click Apply
2. On the device that will access switch management:
   a. Run PuTTYGen.exe
   b. Click <Generate> button to generate the client key pair:



PuTTY Key Generator

File Key Conversions Help

Key

No key.

Actions

Generate a public/private key pair — Generate 2b

Load an existing private key file — Load

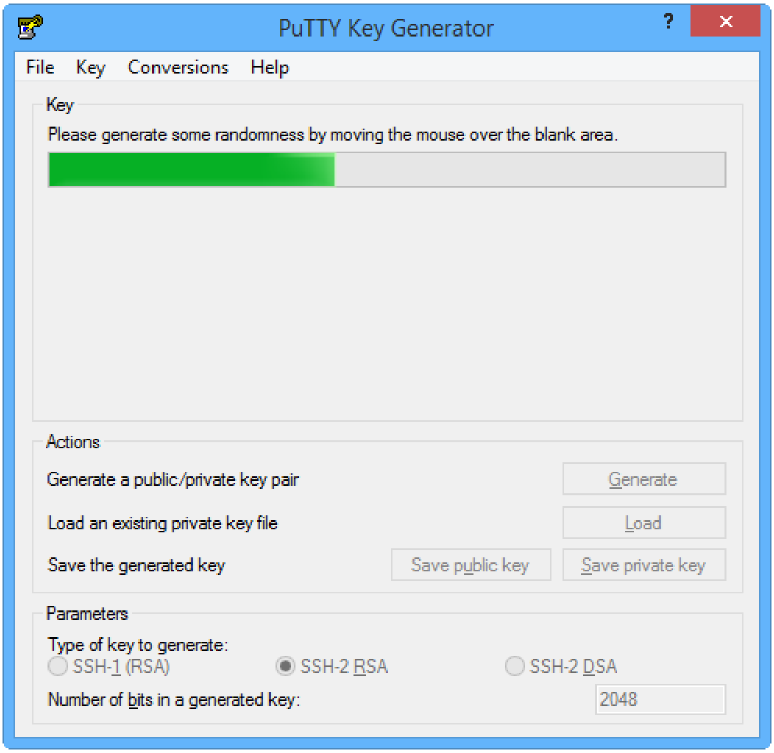
Save the generated key — Save public key — Save private key

Parameters

Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048



Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

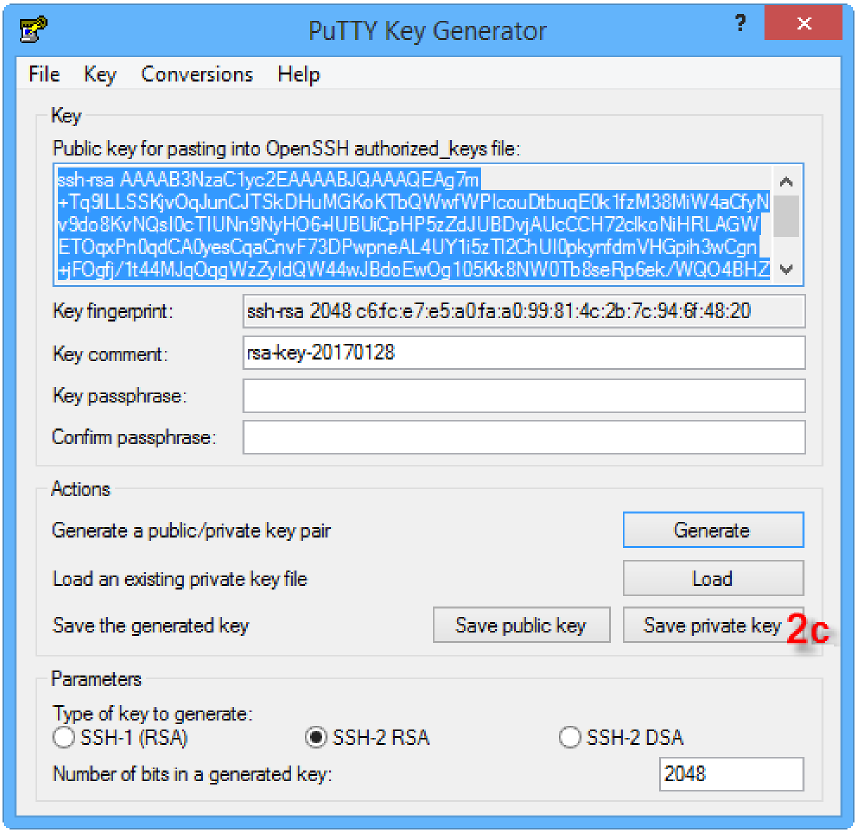
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

c. Click <Save private key> to save the private key,

d. Copy the public key to the switch SSH Key Configuration page in the Key Value box. Enter Key Name 111.

NOTE: *Typically, PuTTYgen requires random mouse movement while the key is being generated*



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAg7m
+Tq9lLLSSKjvOqJunCJTSkDHuMGKoKTbQWwfWPlcouDtbuqE0k1fzM38MiW4aCfyN
v9do8KvNQsI0cTIUNn9NyHO6+lUBUiCpHP5zZdJUBDvjAUcCCH72clkoNiHRLAGW
ETOqxPn0qdCA0yesCqaCnvF73DPwpneAL4UY1i5zTl2ChUI0pkynfdmVHGpih3wCgn
+jFOgfj/1t44MJqOqgWzZyldQW44wJBdoEwOg105Kk8NW0Tb8seRp6ek/WQO4BHZ
```

Key fingerprint: ssh-rsa 2048 c6:fc:e7:e5:a0:fa:a0:99:81:4c:2b:7c:94:6f:48:20

Key comment: rsa-key-20170128

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair — Generate

Load an existing private key file — Load

Save the generated key — Save public key — Save private key

Parameters

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

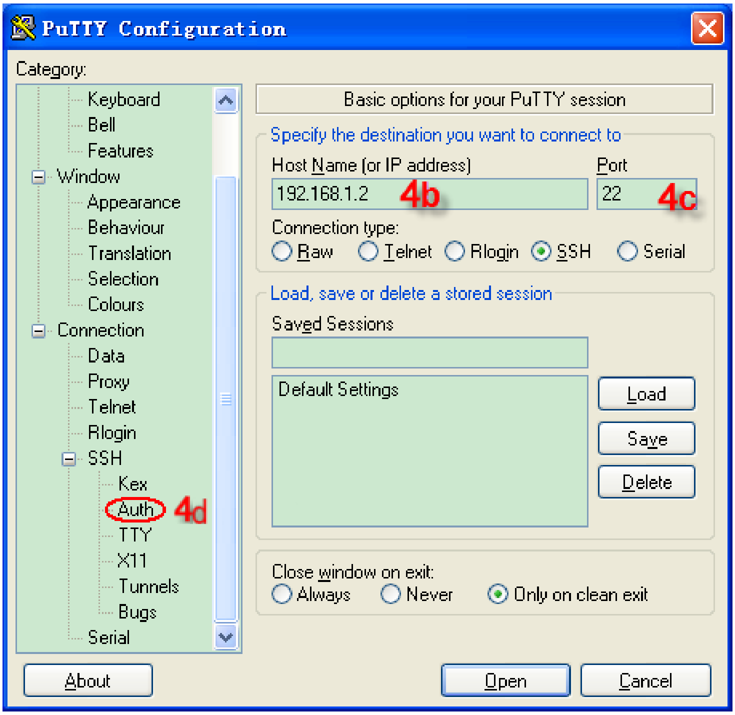
3. On the switch SSH User Manager page:

a. Enter the SSH user name aaa.

b. Select authentication type “Public Key”.

c. Select key name 111.

4. Establish the connection with the SSH server.
   a. Open the terminal application, PuTTY.exe in our example.
   b. Enter the switch management IP address in the Host Name field, 192.168.0.1 is the default, we're using 192.168.1.2 in our example.
   c. Enter port 22 and select SSH connection type.
   d. Click the Auth option in the navigation tree on the left of the PuTTY window.


PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.1.2

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

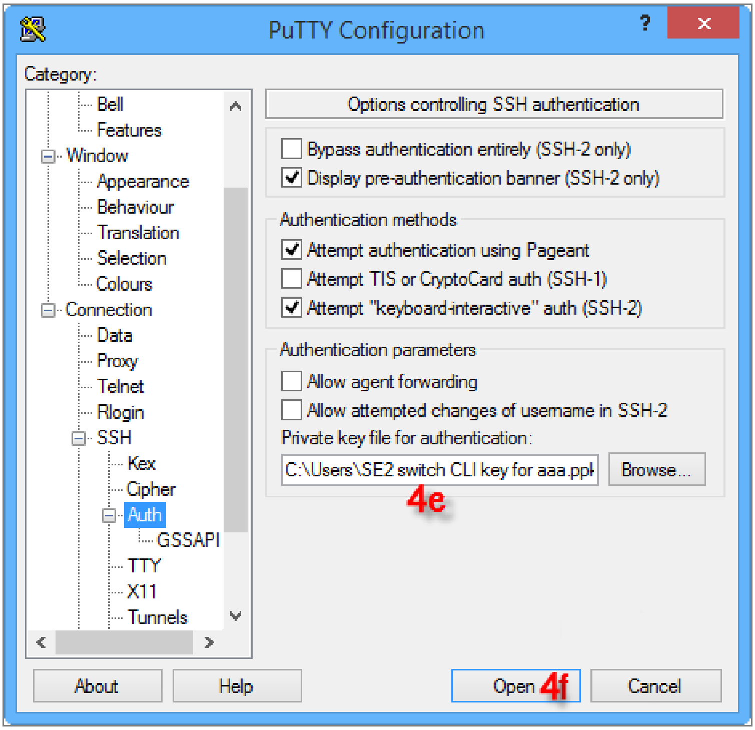
Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

e. Browse to the private file saved in the step 2c.

f. Click <Open> button;



Options controlling SSH authentication

☐ Bypass authentication entirely (SSH-2 only)

☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

☐ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

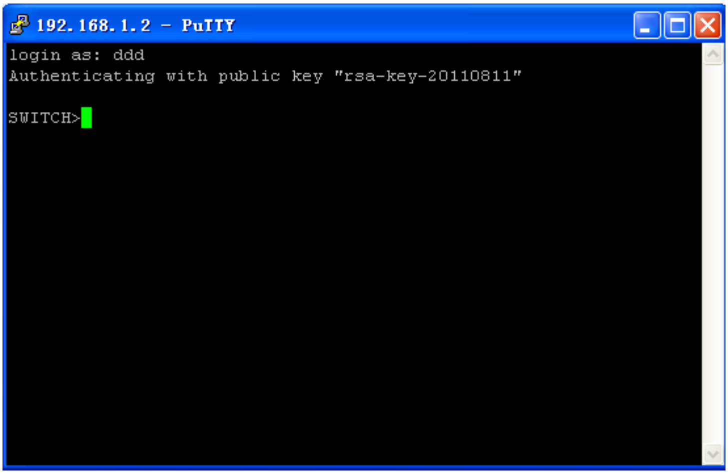
Authentication parameters

☐ Allow agent forwarding

☐ Allow attempted changes of username in SSH-2

Private key file for authentication: C:\Users\SE2 switch CLI key for aaa.ppk

g. Input the user name to enter the switch configuration interface



```
login as: ddd
Authenticating with public key "rsa-key-20110811"

SWITCH>
```

RMON Statistics

RMON (Remote Network Monitoring) allows network management devices to actively monitor and manage network devices. Network management devices may use RMON to read statistical information from the switch, for example, traffic information per port. The switch may use RMON to send alarms to the network management device, for example, traffic exceeding a configured threshold. The switch can automatically record alarm events in an RMON log, or send a Trap message to the management device.

RMON Group

The **Stride** SE2 series switches support statistics group, history group, event group and alarm group of public MIB. Each group supports max 32 entries.

⚠ **CAUTION: If a sampled value of an alarm variable exceeds the threshold multiple times in the same direction, only the first time can trigger an alarm event. That is, in order to capture multiple occasions of a rising condition, an alarm event must be configured for the falling condition to reset the alarm.**

Syslog

The system log file, Syslog, records the switch system information and operation information for troubleshooting. It includes a System log and Running log. Syslog is enabled by default and Runlog is disabled by default.

System log contains:

- Task suspension log
- Reboot caused by task suspension
- Reboot caused by pressing <Reset> button on switch front panel
- Reboot caused by Reboot command
- Reboot caused by clicking <Reboot> button on Web interface
- System reboot

Running log contains:

- Port state change
- Power state change
- Reboot caused by Reboot command
- Reboot caused by clicking <Reboot> button on Web interface

Max 1024 logs are supported. When the number exceeds 1024, a new entry will overwrite the oldest entry.

Save in Flash – when enabled, the logs can be viewed on the switch management interface.

Send to Server – when enabled, switch logs can be uploaded to server in real time.

Remote-server IP – Configure the IP address of server to upload logs

SNMP

SNMP (Simple Network Management Protocol) allows the network administrator to check device information, modify device parameters, monitor device status and locate network faults.

Implementation

SNMP protocol adopts manager/agent mode, so SNMP network contains NMS and Agent.

- NMS (Network Management Station) is a workstation running the SNMP-supported client network management software, playing a core role in SNMP network management.
- Agent is a program in the managed device, the SE2 switch in our case. It is responsible for receiving, processing requests from NMS. When an alarm happens, Agent will automatically inform the NMS.

NMS manages the SNMP network, while Agent is managed by SNMP network. The management information exchange between NMS and Agent is through SNMP protocol. SNMP provides 5 basic operations:

- Get-Request
- Get-Response
- Get-Next-Request
- Set-Request
- Trap

Explanation

SNMP Agent in **Stride** SE2 series switches, supports SNMPv2 and SNMPv3 versions. SNMPv2 is compatible with SNMPv1.

SNMPv1 adopts Community Name Authentication. The community name works as a password and is used to restrict SNMP NMS accessing SNMP Agent. If the community name of the SNMP message cannot pass device authentication, this message will be dropped.

SNMPv2 also adopts Community Name Authentication. It not only is compatible with SNMPv1, but also expands the functions of SNMPv1.

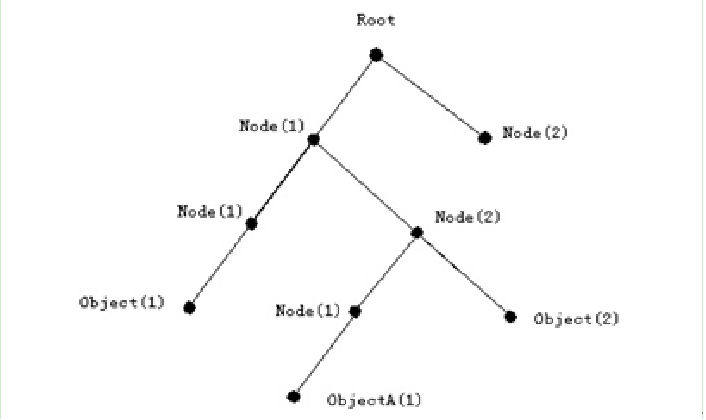
NMS and Agent must support the same SNMP version. Agent can be configured with multiple versions at the same time, and use different versions to communicate with different Network Management Station.

MIB Introduction

Any managed resource can be viewed as an object called a managed object.

An MIB (Management Information Base) is a collection of all managed objects. It defines the hierarchical relationships between managed objects and defines a series of attributes of objects, such as object name, access rights, data types, and so on. Each Agent has its own MIB. NMS can read or write objects in the MIB according to its rights.

MIB defines a tree structure and each tree node is a managed object. Each tree node contains an OID (Object Identifier) that can indicate the node position in the MIB tree structure. As this figure shows, the OID of the managed object A is 1.2.1.1.



SNMPv3

Introduction

SNMPv3 provides a USM (User-Based Security Model) authentication mechanism. User can configure authentication and encryption functions. Authentication is used to verify the legitimacy of the message sender to avoid access by unauthorized users. Messages between NMS and Agent are encrypted. The combination of authentication and encryption improves the communication security between SNMP NMS and SNMP Agent.

Implementation

SNMPv3 has four configuration tables each of which can configure 16 entries. These tables codetermine whether the specified users based on context group can access MIB information.

User table is used to create users. Each user can use different security policies to realize user authentication, encryption and other security functions.

Access table can access MIB node information by matching group name, context name, and by setting security model, security level.

Group table is a collection of multiple users. Access rights are subject to a user group, the access rights of a group are applicable for all users in the group.

Context tables are readable character strings to identify users. It has nothing to do with the specific security model.

Modbus TCP

Industrial applications may be able to more easily and more effectively use Modbus TCP or EtherNet/IP to manage the network, rather than SNMP or RMON. Modbus addresses defined in the SE2 series managed switches may be accessed to read the conditions of the switch, similar to RMON and SNMP. The switch may generate alerts written to the Modbus master. The master may also write to the switch to change some configuration settings.

The Modbus TCP server listening port is 502.

Client devices may read status of Modbus registers as follows:

Item	Description	Protocol Address	Modbus Address
1	Device information	0x0000–0x0fff	400001–404096
2	Port Information	0x1000–0x2fff	404097–412288
3	Alarm Information	0x3000–0x3fff	412289–416384
4	AD–RING Information	0x4000–0x4fff	416385–420480
5	AD–RP Information	0x5000–0x5fff	420481–424576
6	RSTP Information	0x6000–0x6fff	424577–428672

Refer to Appendix E for details on the Modbus TCP switch management features.

EtherNet/IP

Industrial applications may be able to more easily and more effectively use Modbus TCP or EtherNet/IP to manage the network, rather than SNMP or RMON. EtherNet/IP addresses defined in the SE2 series managed switches may be accessed to read the conditions of the switch, similar to RMON and SNMP. The switch may generate alerts written to the EtherNet/IP master.

The master may also write to the switch to change the status. These addresses are detailed in Appendix D.

The SE2 managed switches support EtherNet/IP in the following ways:

Class 1 Implicit I/O Messaging Server/Adapter

Class 3 Explicit Messaging Server/Adapter

Unconnected Explicit Messaging Server/Adapter

Refer to Appendix D for details on the EtherNet/IP switch management feature.

Firmware Update

Occasionally a new firmware version will become available to add features and/or fix bugs. The firmware .bin file may be accessed from a folder on the connected PC or from an FTP server on the network.

When the firmware is in a folder on the connected PC, you may simply Browse to that folder, highlight the new firmware .bin file and Click the Update button.

When the firmware is available from an FTP or TFTP server, carefully enter the full file name including the .bin extension.

Take care to avoid interrupting power to the switch and the source device during the firmware update process.

When the firmware update completes successfully, reboot the switch and check the switch Basic Information page to ensure the new version is reflected in the basic information table.

Configuration Upload and Download

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 LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.

It is always helpful to backup the work of configuring a switch in the event you must replace the switch, or in case the configuration is unintentionally changed.

The configuration file may be saved to the connected PC or to an FTP/TFTP server.

A saved configuration file may be written into the switch from a connected PC or from a FTP/TFTP server on the network. After a configuration file is written into the switch, SAVE must be performed to commit the configuration to the switch.

Load Default

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 LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.*

Besides the software Load Default feature, the **Stride** SE2 series switches may Load Default by pressing the RESET button on the face of the switch for longer than 5 seconds until all LEDs start to flash. When the button performs the Load Default, the previous configuration will not be accessible afterward.

Reboot

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 LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch will revert to the last committed changes on power cycle.*

If changes have been made to the configuration or a software Load Default was performed unintentionally, the switch can revert to the previous configuration by performing Reboot.

Besides the software Reboot feature, the SE2 series switches have a Reboot button on the face of the switch. Reboot can be performed by pressing the Default button on the face of the switch for 1 to 5 seconds. If held for more than 5 seconds, it will reset configuration back to default.

APPENDIX A

DEFAULT SETTINGS

In this Appendix...

Default Settings

Stride SE2 Series Managed Switch Default Settings		
Configuration Parameter		Default Settings
Main Settings		
System Settings	User Name	admin
	Password	admin
	DHCP	Disabled
	IP Address	192.168.0.1
	Subnet Mask	255.255.255.0
	Gateway	192.168.0.1
	Project Name	PRJNAME
	Switch Name	Switch
	Location	Switch Location
	Contact	Contact Info
Port Settings	Port Admin	Enabled (all ports)
	Auto Speed and Duplex	Enabled (all ports)
	Flow Control	Off
	Jumbo Frame	Enabled
Redundancy Settings		
RSTP	Redundancy	RSTP enabled (all ports)
	Spanning Tree Priority	32768
	Hello Time	2
	Max Age Time	20
	Forward Delay Time	15
	Message Age Increment	Default = Increments by the greater of (Max Age Time / 16) or one
	Port Priority	128
	Path Cost	Auto (all ports)
Proprietary Redundancy Protocols	RTSP Transparent	Disabled (all ports)
	AD-Ring	No Domain ID assigned No ports assigned as AD-Ring ports
	AD-Ring+	Disabled
	AD-RP	No Domain ID assigned No ports assigned as AD-RP Ring ports

Stride SE2 Series Managed Switch Default Settings (cont’d)		
Configuration Parameter		Default Settings
Traffic Filtering Settings		
Multicast Filtering	IGMP	Enabled (all ports)
	IGMP Auto Query	Enabled (all ports)
QoS	QoS	802.1P (all ports)
	Egress Type	SP (Strict Priority) (all ports)
VLAN	VLAN	All ports and switch management participate in VLAN1
	GVRP	Disabled
	MAC Aging Time	300 sec
Switch Management Settings		
	ARP Aging Time	20 min
	Port Trunk (Link Aggregation) Mode	HASH No port selected for Link Aggregation
	SSH	Disabled
	Dot1x	Disabled
	TACACS+	Disabled
	Browser Access Protocol	HTTP
	DHCP Server	Disabled
	DHCP Snooping	Disabled
Network Management Settings		
Network Monitoring	LLDP	Disabled
	Syslog	Enabled
	RunLog	Disabled
	Save in Flash	Disabled
	Send to Server	Disabled
	Remote Server IP Address	0.0.0.0
	SNMP	Disabled
	SNMP Trap	Enabled
	SNMP Trap Port ID	162
	EtherNet/IP	Disabled
	Modbus TCP	Disabled
	Link Check	No ports enabled
	RMON	None Configured
	Network Time Protocol SNTP	Disabled

Stride SE2 Series Managed Switch Default Settings (cont'd)		
Configuration Parameter		Default Settings
Network Management Settings (continued)		
Network Security	Port Security	No ports enabled
Network Troubleshooting Settings	Port Monitor	No ports monitored
	Alarm	No alarms enabled
	Port CRC Project	No ports enabled
	Loop Detect	No ports enabled

Appendix B

Console Port Access & CLI Commands

In this Appendix...

Console Port Access:

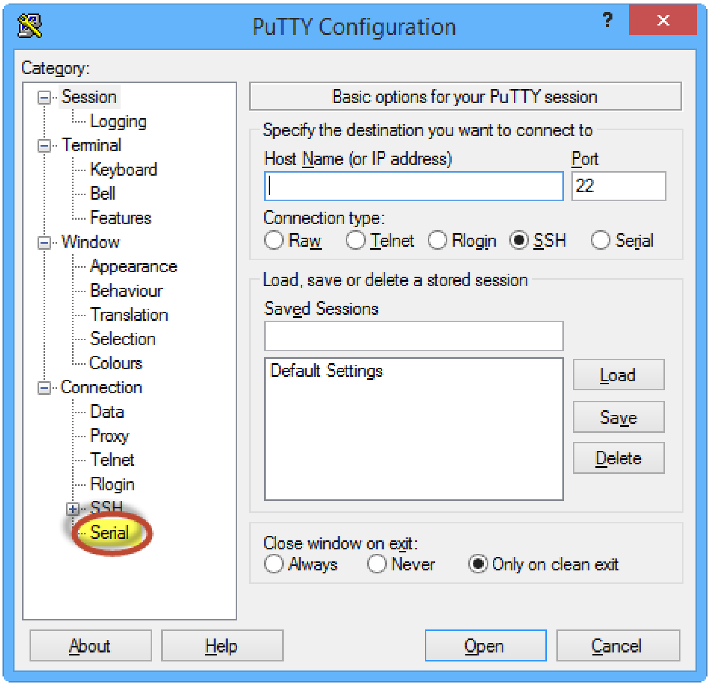
Serial Access

There are a variety of ways to access a switch.

- Web browser via Ethernet connection at a switch port,
- Command Prompt via Ethernet connection at a switch port,
- Telnet via USB connection

This manual details switch management by the web browser. The USB console port offers alternative access to the switch management and this appendix details how to connect through the USB port. The user can access a switch by its USB Console port and PuTTY or Windows Hyper Terminal or other software that supports serial port connection. The following example shows how to use the Console port and PuTTY to access the switch.

1. Install the mini USB serial port driver "Mini USB_driver.exe". The driver may be downloaded from the AutomationDirect downloads page.
2. Use a mini USB cable to connect the PC USB and the switch Console port
3. Open PuTTY on your PC. Click the Serial option at the bottom of the Navigation Tree on the left.



PuTTY Configuration

Category:

Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address):

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

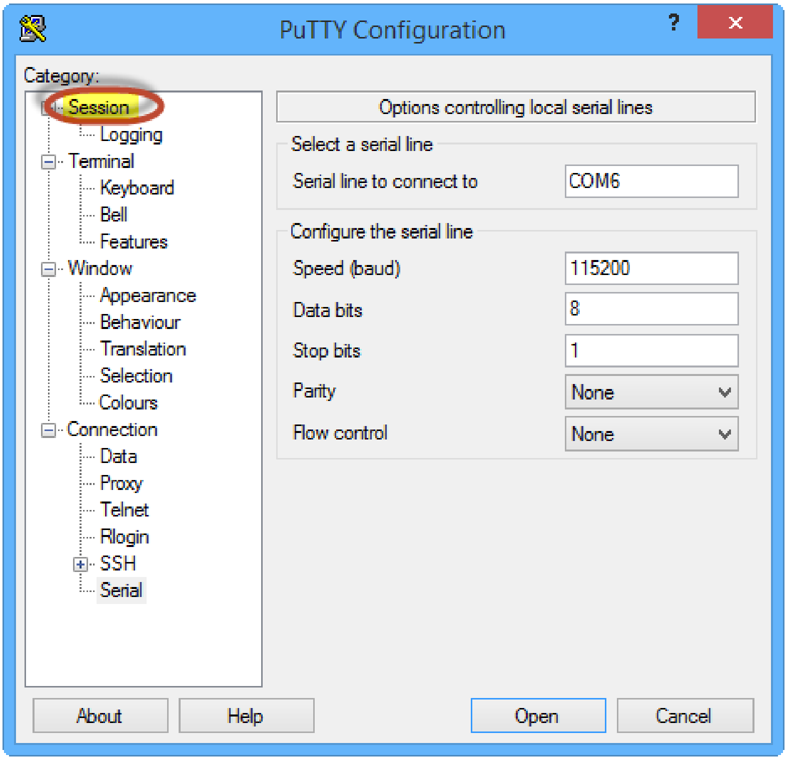
Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

4. For the Serial Line, enter the COM port assigned to your switch. The COM port number is shown in Windows Device Manager under "Ports (Com & LPT)'. The settings for the serial line are:

   - Baud - 115200
   - Data bits - 8
   - Stop bits - 1
   - Parity - None
   - Flow control - None

   Then Click the Session selection at the top of the Navigation tree on the left.



PuTTY Configuration

Category:

Options controlling local serial lines

Select a serial line

Serial line to connect to: COM6

Configure the serial line

Speed (baud): 115200

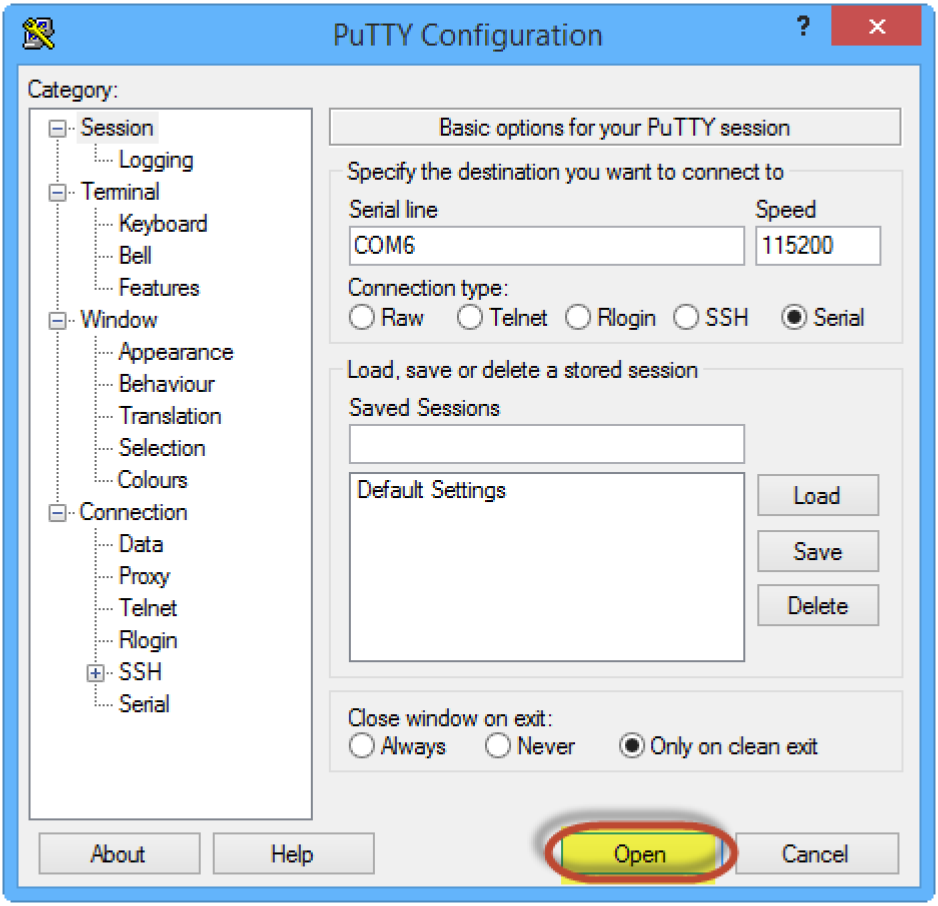
Data bits: 8

Stop bits: 1

Parity: None

Flow control: None

5. Click on the Serial radio button in the top pane, and verify the Serial line COM port number and Speed are correct. Then click the Open button at the bottom of the window.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM6

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

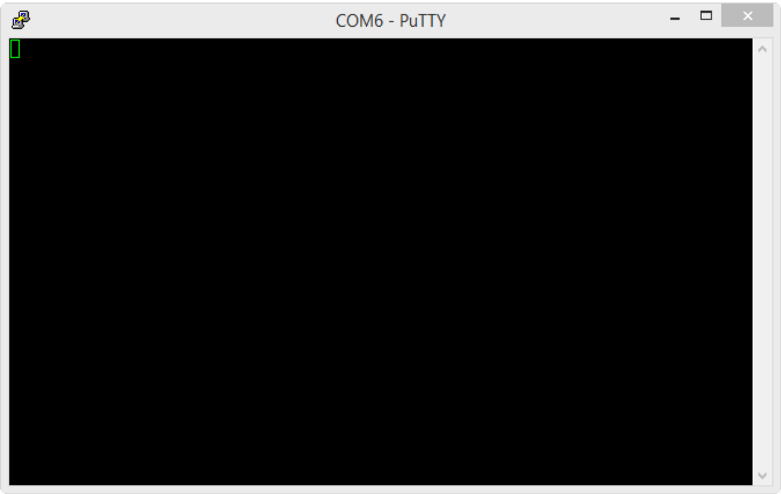
Load, save or delete a stored session

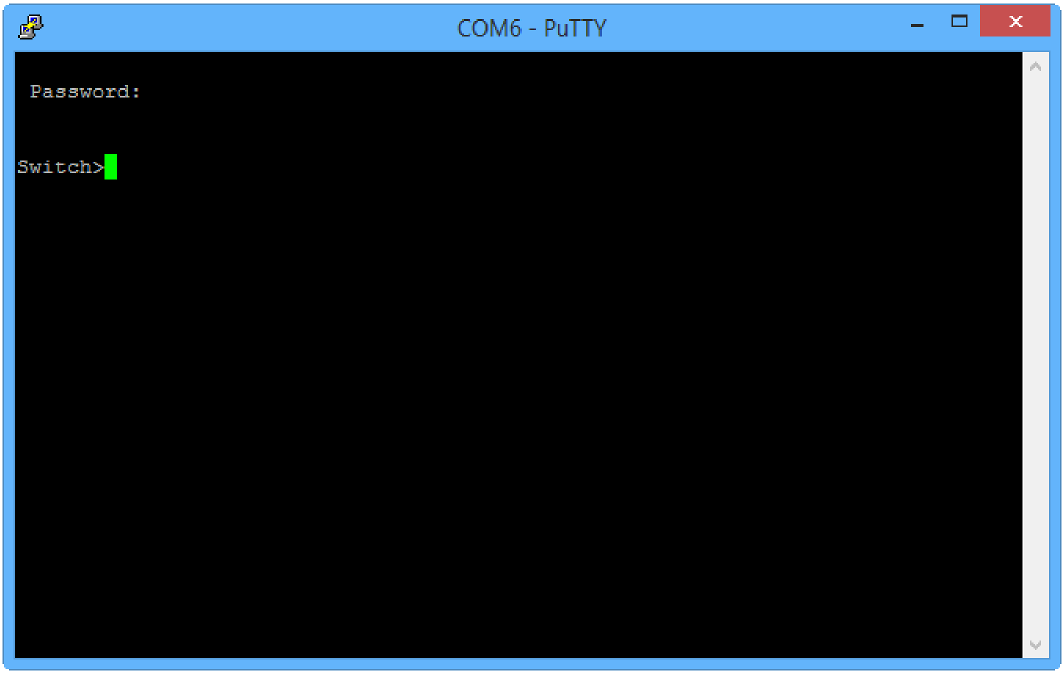
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

6. Hit Enter on your keyboard to move to the Password request. Then carefully enter the password, admin is the default.





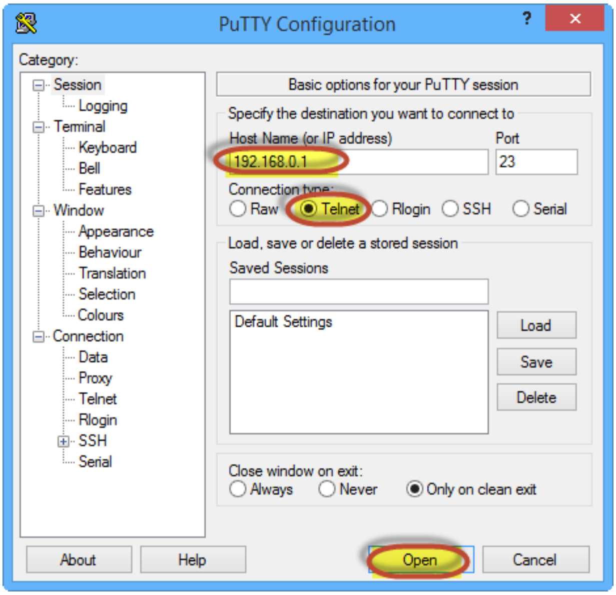
```
 Password:

Switch>
```

Telnet Access

For a switch connected to the PC by an Ethernet cable, and the switch's IP Address is known, PuTTY or another terminal emulator application may be used to access switch management.

1. Open PuTTY and Select the Telnet Radio button, then enter the switch IP address and Click Open.



Specify the destination you want to connect to

Host Name (or IP address): 192.168.0.1 Port: 23

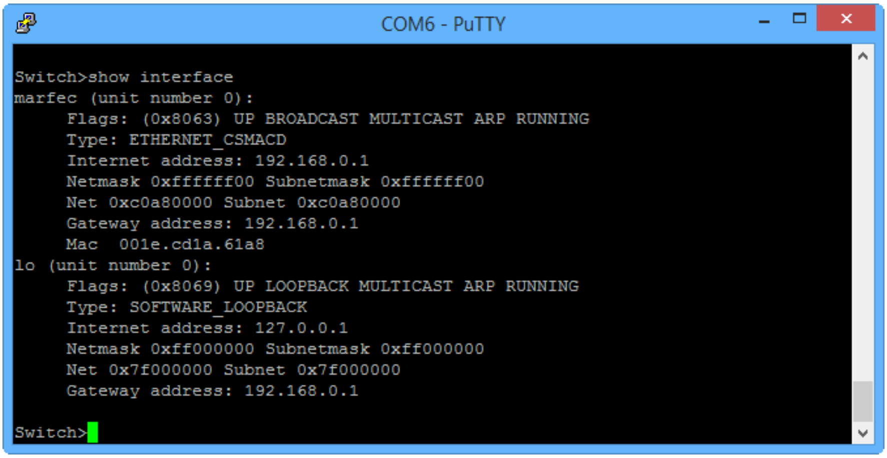
Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

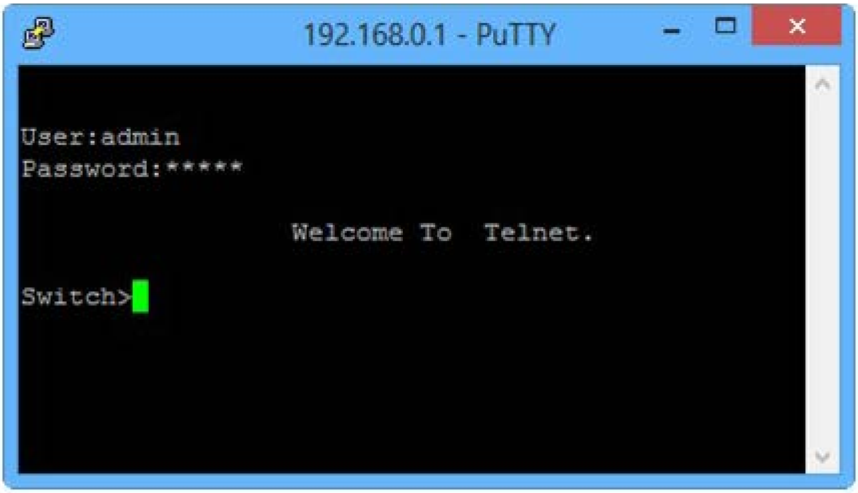
NOTE: *The switch default IP address is 192.168.0.1. If the IP address is unknown, you must use the Serial Access to connect to the switch, login and enter the "show interface" command.*



```
Switch>show interface
marfec (unit number 0):
     Flags: (0x8063) UP BROADCAST MULTICAST ARP RUNNING
     Type: ETHERNET_CSMACD
     Internet address: 192.168.0.1
     Netmask 0xffffff00 Subnetmask 0xffffff00
     Net 0xc0a80000 Subnet 0xc0a80000
     Gateway address: 192.168.0.1
     Mac  001e.cd1a.61a8
lo (unit number 0):
     Flags: (0x8069) UP LOOPBACK MULTICAST ARP RUNNING
     Type: SOFTWARE_LOOPBACK
     Internet address: 127.0.0.1
     Netmask 0xff000000 Subnetmask 0xff000000
     Net 0x7f000000 Subnet 0x7f000000
     Gateway address: 192.168.0.1

Switch>
```

2. Carefully enter the user name, admin, and the password, admin.



```
User:admin
Password:*****

                    Welcome To  Telnet.

Switch>
```

View Types

When logging into CLI (Command Line Interface) by Console port or Telnet, a user can navigate to different views as shown below.

View Switching			
View Prompt	**View Type**	**View Function**	**Command for View Switching**
SWITCH>	User View	• Show currently used commands • Show IP address • Show software version	Input "enable" to enter the management view
SWITCH #	Management View	• Show switch configuration information • Upload/download configuration file • Upload/download log record • Restore default configuration • Save current configuration • Software update • Reboot switch	• Input "configure terminal" to switch from the management view to the configuration view; • Input "exit" to return to the user view
SWITCH (config) #	Configuration View	Configure all switch functional modules	Input "exit" or "end" to return to the management view

When a switch is configured by command line, "?" can be used to get command help. In the help information, there are different parameter descriptions, for example, <1, 255> means a number range; <H.H.H.H> means an IP address; <H:H:H:H:H:H> means a MAC address; word<1,31> means a string range. In addition, ***INSERT DOWN ARROW SYMBOL*** and ***INSERT UP ARROW SYMBOL*** can be used to scroll through the last used 10 commands.

CLI Commands

Introduction

The command-line interface (CLI) largely behaves as a text-based Cisco-type CLI.

When logged in to the switch CLI, entering the question mark character will return the list of available commands.

Type a command followed by a space and the question mark character to see the list of expected arguments for that command.

From the exec mode prompt (Switch#) type configure terminal to access commands to change the configuration of the switch and its interfaces. In configuration mode, remember to commit changes to save them to the switch configuration file.

Exit moves back thru the modes of access in the CLI

CLI Commands

Global Commands

The following global commands are available anywhere in the CLI:

Command	Effect
commit	Commit the set of changes to the switch and cause the changes to take operational effect
defaults	Restore factory defaults
quit	CLI is exited. Uncommitted changes are discarded without prompting.
reset	Reset the Switch.
help	Print a help message.
prompt	Enable/disable the prompt (usage: “prompt enabled” or “prompt disabled”)

When restoring factory defaults, network settings may be maintained by adding a “savenw” option. In other words:

```
defaults
```

restores all values, but

```
defaults savenw
```

restores all defaults except the current settings for DHCP, IP address, etc…

Appendix C

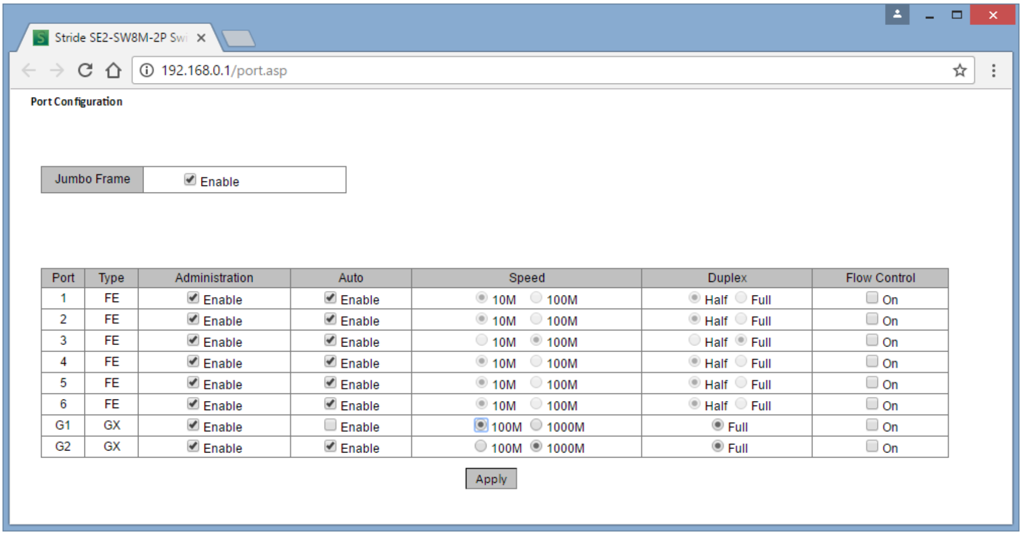
Troubleshooting

In this Appendix...

Troubleshooting Fiber Connections

1. If you are using a 100Mbps SFP in a Stride switch, you must manually change the port speed on the Port Configuration page of the Switch Setup interface. Note that if matching100Mbps SFPs are installed and connected by a proper mode-type patch cable but the Port Configuration has not been changed from the default 1000Mbps (Gigabit speed), the Port Status and RSTP Port Status pages will not indicate the port speed mismatch. That is, the browser interface will not alert the user to this speed mismatch.

- Verify the type of SFP. In the configuration shown below, port G1 is a 100Mbps SFP.
- Verify the port number.
- Verify the Port Speed Setting on the Basic Configuration - Port Configuration page.



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
G1	GX	☑ Enable	□ Enable	● 100M ○ 1000M	● Full	□ On
G2	GX	☑ Enable	☑ Enable	○ 100M ● 1000M	● Full	□ On

2. Make sure that the speeds of both ends of a link match: a 100Mbps SFP on one switch must connect to a 100Mbps connection on the other switch or end device. Fiber ports do not negotiate speed.

3. Ensure that the cable type you are using matches the transceiver type. That is, Multimode cable requires Multimode transceivers, and Single-mode cable requires Single-mode transceivers.

4. Additionally, it is important that 62.5um is used with 62.5um and 50um used with 50um. If the fiber cores are not aligned correctly significant attenuation will occur.

5. Make sure that all of your connectors are clean. Even a little bit of dust, dirt or grease on a connector face can significantly degrade a fiber signal. This includes the main fiber optic link as well as any patch cables that you may be using. When cleaning, it is important to use lint free swabs or wipes, preferably of a clean room quality. These can be used dry or wet (with 99% isopropyl alcohol solutions).

- Make certain that you are not cleaning an active fiber, as the laser can cause permanent damage to your eyes should you look into the end face.
- Additionally, it is not necessary to scrub the end face, rather to just gently wipe it clean and then double-check the link. If additional cleaning is required simply repeat this process.

6. Make sure that all connectors are plugged completely into their proper ports. Again, if end faces are not lined up correctly with transceivers and/or mated fiber ends, the system may fail due to excess attenuation.

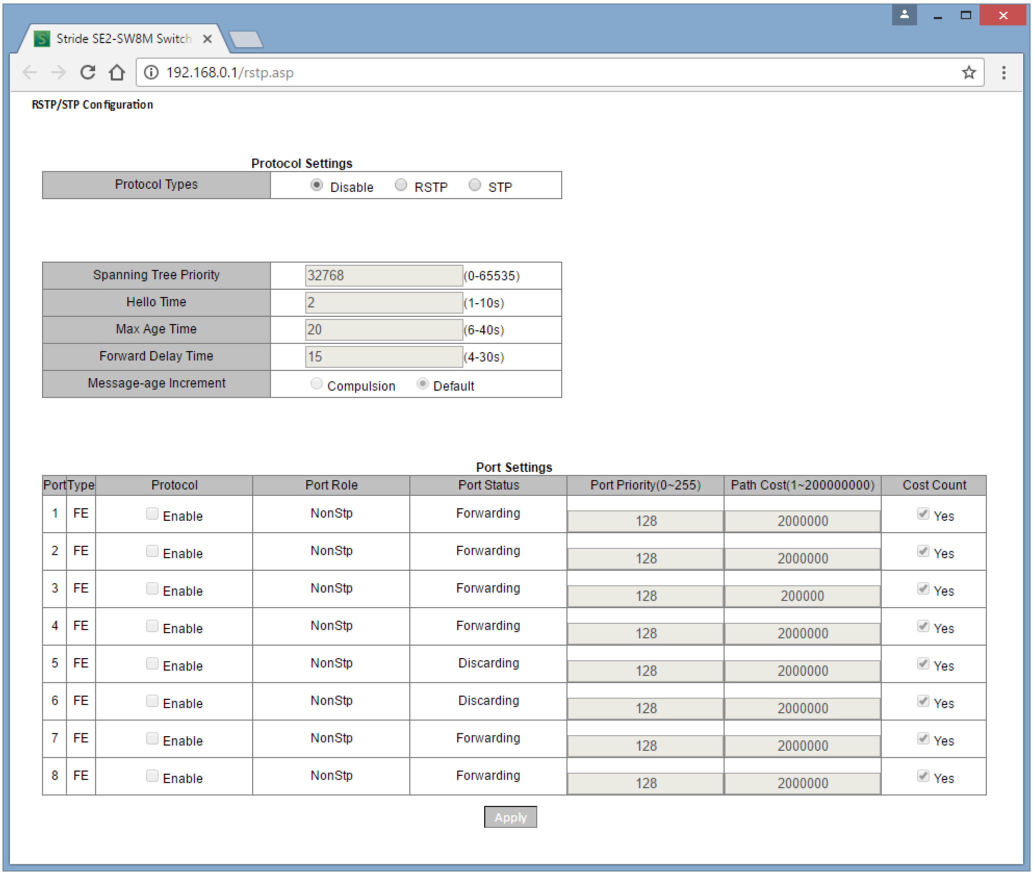
7. Make sure that the transmit cable at the near end is the receive cable at the far end. There needs to be a crossover for a fiber link to work correctly. Be sure to factor in all patch cord that may be used.

NOTE: *The physical connectors on the ends of a fiber cable do NOT need to match: a link may use an LC connector on one end and an SC connector on the other.*

Troubleshooting AD-Ring

1. Typically a switch will be protected by either AD-Ring or RSTP. If AD-Ring is configured on a switch, disable RSTP.

- On the Redundancy – RSTP/STP Configuration page, set Protocol Types to “Disable.



RSTP/STP Configuration

Protocol Settings

Protocol Types	● Disable ○ RSTP ○ STP

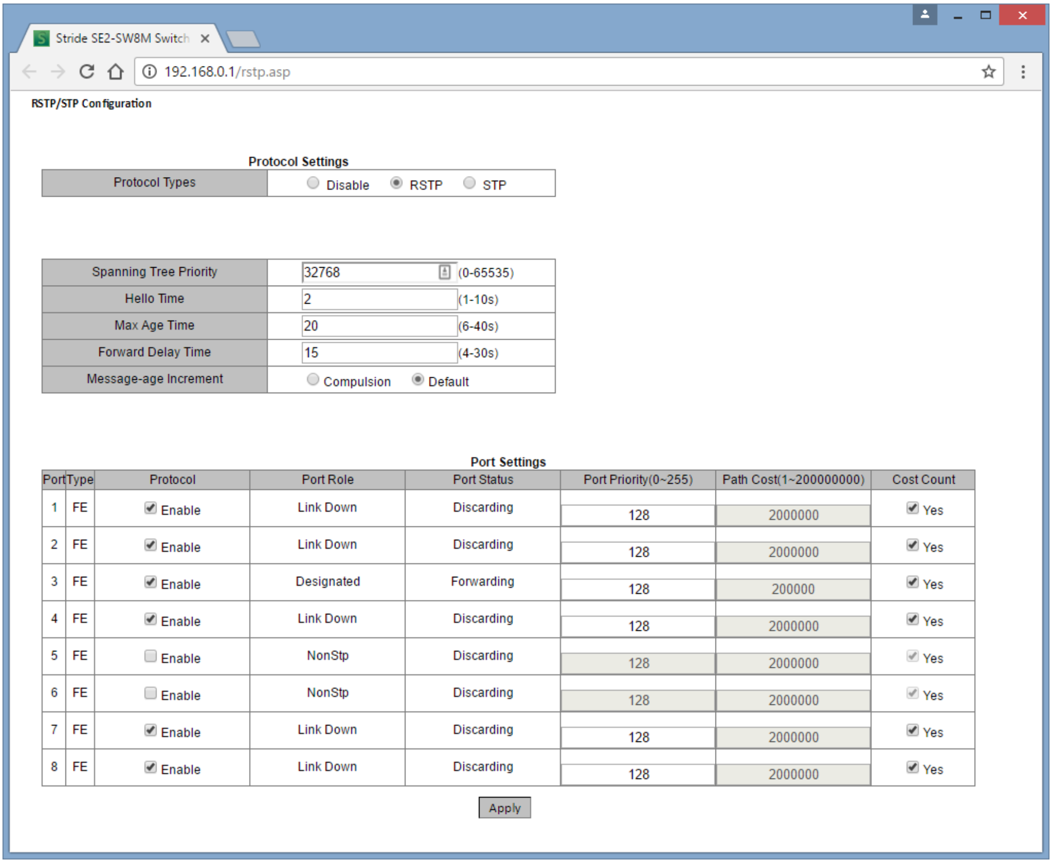
Spanning Tree Priority	32768	(0-65535)
Hello Time	2	(1-10s)
Max Age Time	20	(6-40s)
Forward Delay Time	15	(4-30s)
Message-age Increment	○ Compulsion ● Default	

Port Settings

Port	Type	Protocol	Port Role	Port Status	Port Priority(0~255)	Path Cost(1~200000000)	Cost Count
1	FE	☐ Enable	NonStp	Forwarding	128	2000000	☑ Yes
2	FE	☐ Enable	NonStp	Forwarding	128	2000000	☑ Yes
3	FE	☐ Enable	NonStp	Forwarding	128	200000	☑ Yes
4	FE	☐ Enable	NonStp	Forwarding	128	2000000	☑ Yes
5	FE	☐ Enable	NonStp	Discarding	128	2000000	☑ Yes
6	FE	☐ Enable	NonStp	Discarding	128	2000000	☑ Yes
7	FE	☐ Enable	NonStp	Forwarding	128	2000000	☑ Yes
8	FE	☐ Enable	NonStp	Forwarding	128	2000000	☑ Yes

2. It is possible for AD-Ring and RSTP to coexist on a switch. If a switch participates in both an AD-Ring and a spanning tree, exclude the AD-Ring ports from Spanning tree:

- On the Redundancy – RSTP/STP Configuration page, check the boxes to exclude the Real-Time Ring ports from Spanning Tree. Ports 5 & 6 are excluded because they are part of AD-Ring AD-1-1.



RSTP/STP Configuration

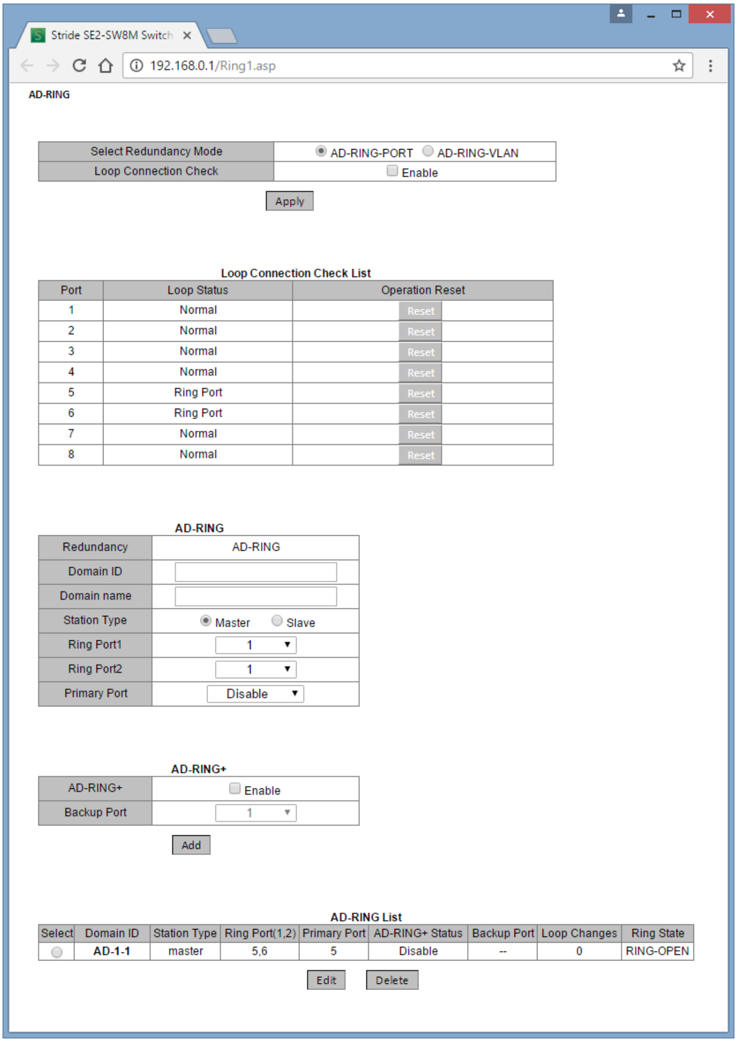
Protocol Settings

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	Designated	Forwarding	128	200000	☑ Yes
4	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
5	FE	□ Enable	NonStp	Discarding	128	2000000	☑ Yes
6	FE	□ Enable	NonStp	Discarding	128	2000000	☑ Yes
7	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes
8	FE	☑ Enable	Link Down	Discarding	128	2000000	☑ Yes



AD-RING

Select Redundancy Mode	● AD-RING-PORT ○ AD-RING-VLAN
Loop Connection Check	□ Enable

Loop Connection Check List

Port	Loop Status	Operation Reset
1	Normal	Reset
2	Normal	Reset
3	Normal	Reset
4	Normal	Reset
5	Ring Port	Reset
6	Ring Port	Reset
7	Normal	Reset
8	Normal	Reset

AD-RING

Redundancy	AD-RING
Domain ID	
Domain name	
Station Type	● Master ○ Slave
Ring Port1	1
Ring Port2	1
Primary Port	Disable

AD-RING+

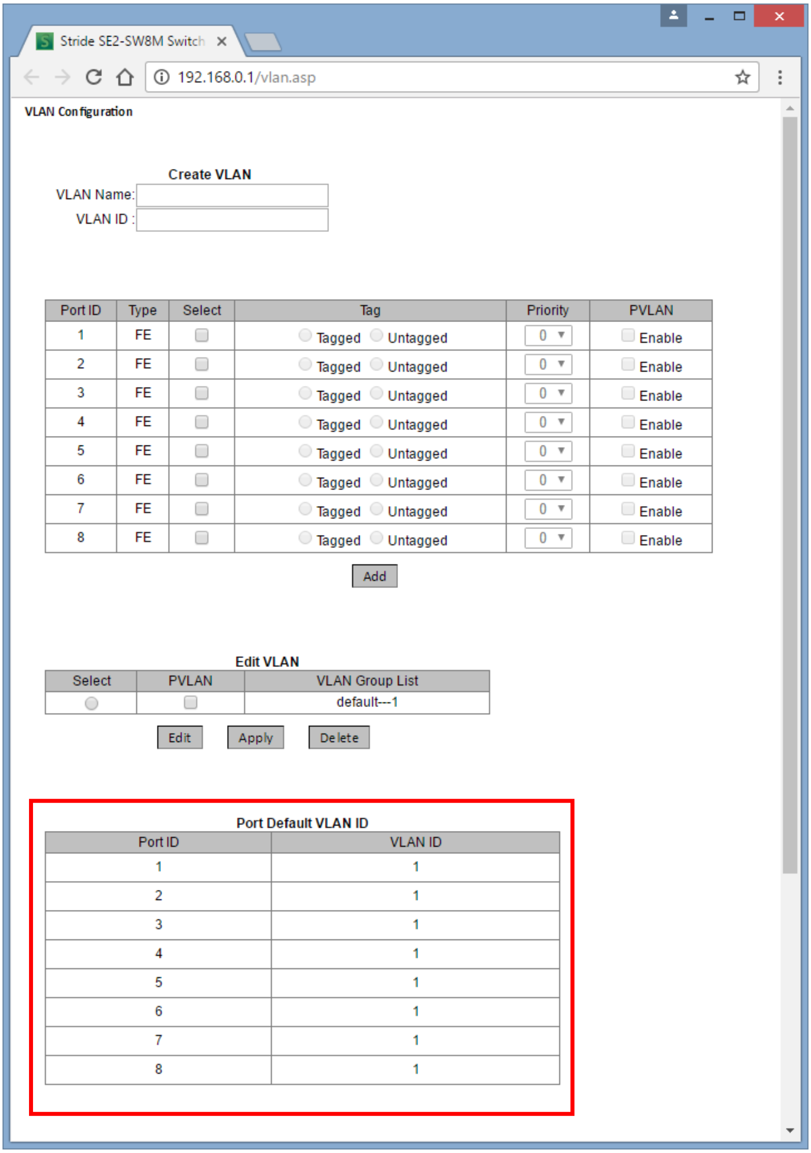
AD-RING+	□ Enable
Backup Port	1

AD-RING List

Select	Domain ID	Station Type	Ring Port(1,2)	Primary Port	AD-RING+ Status	Backup Port	Loop Changes	Ring State
○	AD-1-1	master	5,6	5	Disable	--	0	RING-OPEN

Troubleshooting VLANs

The most common VLAN is the Tag-based **VLAN**. The port that is used to access the browser based switch management must participate in **VLAN**1. All ports participate in VLAN1 by default.



VLAN Configuration

Create VLAN

VLAN Name:

VLAN ID :

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

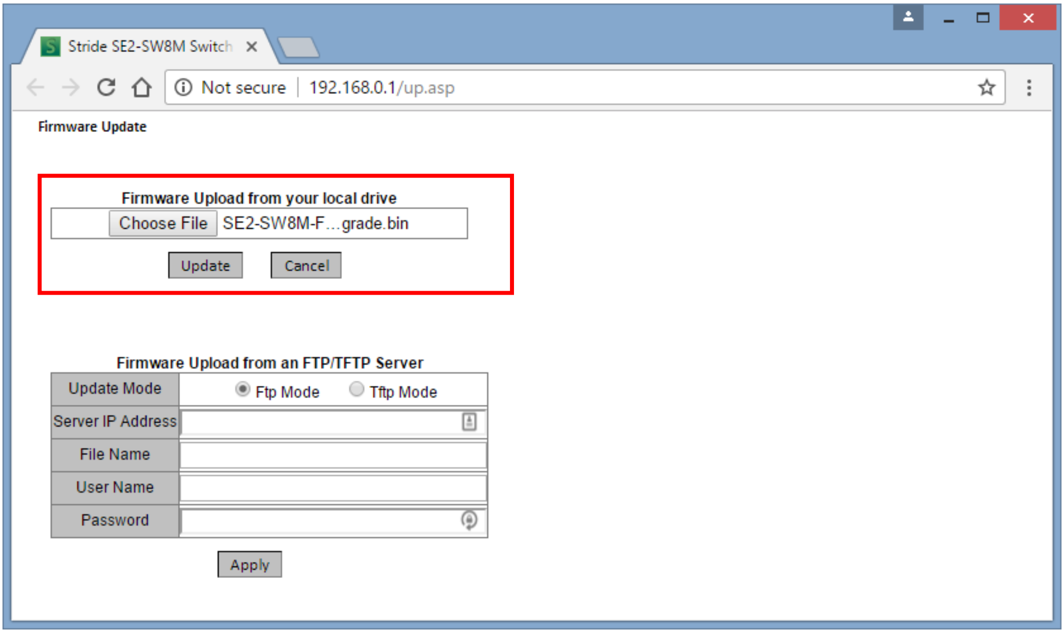
Select	PVLAN	VLAN Group List
○	□	default---1

Port Default VLAN ID

Port ID	VLAN ID
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	1

Installing Switch Firmware

Switch firmware is written from the browser or CLI. SE2 series switches do not maintain multiple versions of firmware.



Firmware Update

Firmware Upload from your local drive

Choose File SE2-SW8M-F...grade.bin

Update Cancel

Firmware Upload from an FTP/TFTP Server

Update Mode	● Ftp Mode ○ Tftp Mode
Server IP Address	
File Name	
User Name	
Password	

Apply

Appendix D

EtherNet/IP

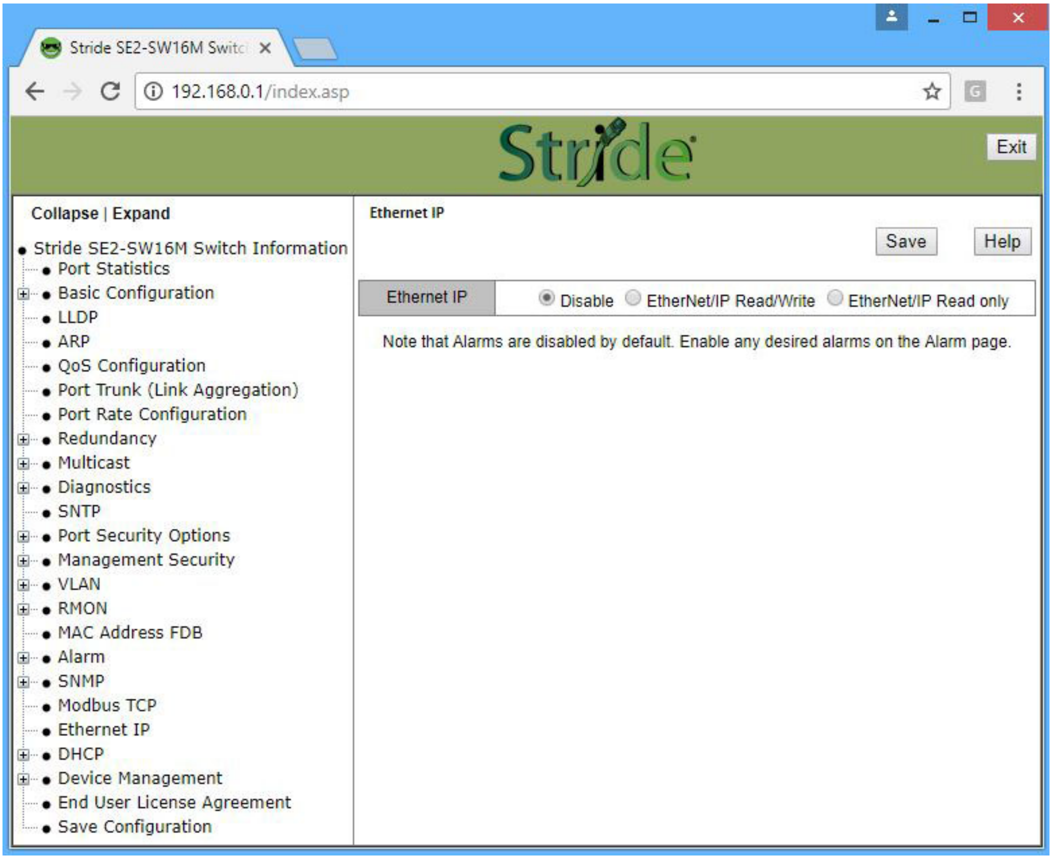
In this Appendix...

EtherNet/IP Switch Management

The **Stride** SE2 managed switch supports EtherNet/IP (Ethernet Industrial Protocol) in the following ways:

- Class 1 Implicit (I/O) Messaging Server/Adapter
- Class 3 Explicit Messaging Server/Adapter
- Unconnected Explicit Messaging Server/Adapter

The EtherNet/IP server is disabled by default in the Managed Switch.



Ethernet IP

Ethernet IP ● Disable ○ EtherNet/IP Read/Write ○ EtherNet/IP Read only

Note that Alarms are disabled by default. Enable any desired alarms on the Alarm page.

NOTE: *The configuration must be saved (selection is available on left hand side at the bottom) or it will be lost upon the next power cycle.*

Implicit (I/O) Messaging

The **Stride** SE2 managed switch supports both Unicast and Multicast Implicit (I/O) Messaging. The required parameters are shown below:

Assembly Instance		
Connection Points		Size
Input	101 (0x65)	156 bytes
Output	102 (0x66)	20 bytes
Config	0	0

The Configuration is not required in the path. If it is included, use 0 for the Attribute and 0 size.

The Run/Idle (4 byte) header is required and is not included in the Output size specified above.

Input Data is defined as the data that is 'Produced' by the **Stride** managed switch and is read (Consumed) by the EtherNet/IP Master/Scanner device.

Input Data			
Byte Offset Number	**Size (in Bytes)**	**Name**	**Details**
		Input Data	

0	2	Port Status: Ports 1–8	2 bits per port
			Diabled = 00
			Up = 01
			Down = 10
			For example, Port 1 is the most significant bit and Port 8 is the least significant bit.

2	2	Port Status: Ports 9–16	
4	2	Port Status: Ports 17–24	
6	2	Port Status: Ports 25–32	
8	2	Port Status: Ports 33–40	
10	2	Port Status: Ports 41–48	
12	2	Port Status: Ports 49–56	
14	2	Port Status: Ports 57–64	

16	1	Alarm Status of Port 1	Diabled = 0x00
			Normal = 0x01
			Alarm = 0x02

17	1	Alarm Status of Port 2	
18	1	Alarm Status of Port 3	
19–79	1	Alarm Status of Port 4–64	
80	1	AD-Ring Alarm Status Ring 1	

81	1	AD-RP Ring Alarm Status Ring 1	Diabled = 0x00
			Normal = 0x01
			Alarm = 0x02
			None = 0x03

82-143	2	AD-Ring Alarm and AD-RP Ring Alarm Status for Rings 2-32	Same format as previous 2 bytes but for Rings 2-32

144	2	IP Address Conflict Alarm Status	Diabled = 0x00
			Normal = 0x01
			Alarm - 0x02

145	1	MAC Address Conflict Alarm	

146	1	Power Alarm Status	Diabled = 0x00
			Normal = 0x01
			Power 1 Alarm = 0x02
			Power 2 Alarm = 0x03

147	9	Reserved	

Output Data is defined as the data that is ‘Produced’ or written from the EtherNet/IP Master/Scanner device and is received (Consumed) by the **Stride** managed switch.

Output Data			
Byte Offset Number	Size (in Bytes)	Name	Details
Output Data			
	4	Run/Idle Header	Bits 4-31: Reserved Bits 2-3: ROO (Ready for Ownership of Outputs) Bit 1:COO (Claim Output Ownership) Bit 0: Run/Idle (Run = 1, Idle = 0) This header is typically sent by the Operating System
0	2	Port Enable: Ports 1–8	2 bits per port: Enable = 01 Disable = 10 No change = 00 No change = 11
2	2	Port Enable: Ports 9–16	
4	2	Port Enable: Ports 17–24	
6	2	Port Enable: Ports 25–32	
8	2	Port Enable: Ports 33–40	
10	2	Port Enable: Ports 41–48	
12	2	Port Enable: Ports 49–56	
14	2	Port Enable: Ports 57–64	
16	2	Reserved	
18	2	Reserved	

Explicit Messaging

Explicit messaging allows for much more information to be accessed in the managed switch but does require more configuration.

There are 2 different services that the managed switch supports:

Set Single Attribute Service	
Service	16 (0x10): Set Single Attribute
Class	4
Instance	104 (0x68)
Attribute	3
Size	22 bytes

Get Single Attribute Service	
Service	14 (0x0e): Get Single Attribute
Class	4
Instance	103 (0x67)
Attribute	3
Size	260 bytes

The first two bytes of the data sent in the “Set Single Attribute Service” determine the meaning of the remaining 20 bytes of the write block and also what type of data is sent in the response to the “Get Single Attribute Service”.

The first two bytes of the data sent in the "Set Single Attribute Service" can be either of the following:

- Byte 0 = 01 Byte 1 = 00: Determines that the rest of the sent data is the same format as the I/O Messaging Output data. The data sent in the response to the "Get Single Attribute Service" will be the same as the I/O Messaging Input data.
- Byte 0 = 00 Byte 1 = 00: Allows access to many other pieces of data in the managed switch. These bytes should be followed by pointer values explained in the table below.

Address Matrix

	00	01	02	03	04	05	····>	N
00	Port Status and alarm (Same as I/O Messaging)	–	–	–	–	–	–	–
01 (Device Info)	–	Mfg Name	Device Type	Mfg Address	Contact Phone Number	Other Info	–	–
02 (Port Info)	–	Port 1	Port 2	Port 3	Port 4	Port 5	····>	Port N
03 (AD-Ring Info)	Ring Mode	Ring 1	Ring 2	Ring 3	Ring 4	Ring 5	····>	Ring N
04 (AD-RP Ring Info)	Ring Mode	Ring 1	Ring 2	Ring 3	Ring 4	Ring 5	····>	Ring N
05 (RSTP Ring Info)	Root Bridge Status	Ring 1	Ring 2	Ring 3	Ring 4	Ring 5	····>	Ring N

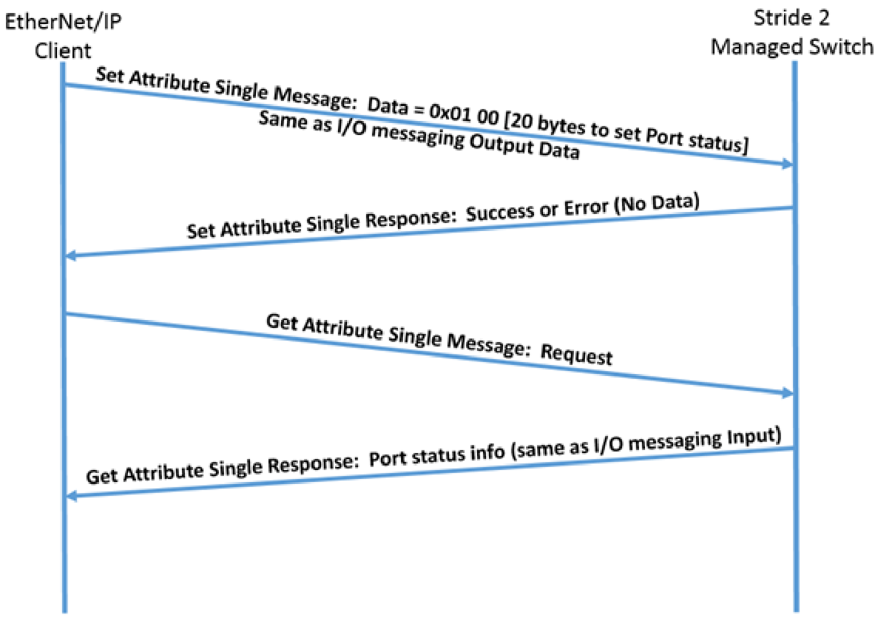
When Byte 0 = 00 and Byte 1 = 00, Byte 2 should be the value in the Row such as 01 for Device Info or 02 for Port Info and Byte 3 should be the value in the Column header to choose the specific piece of data from the Info type.

For example:

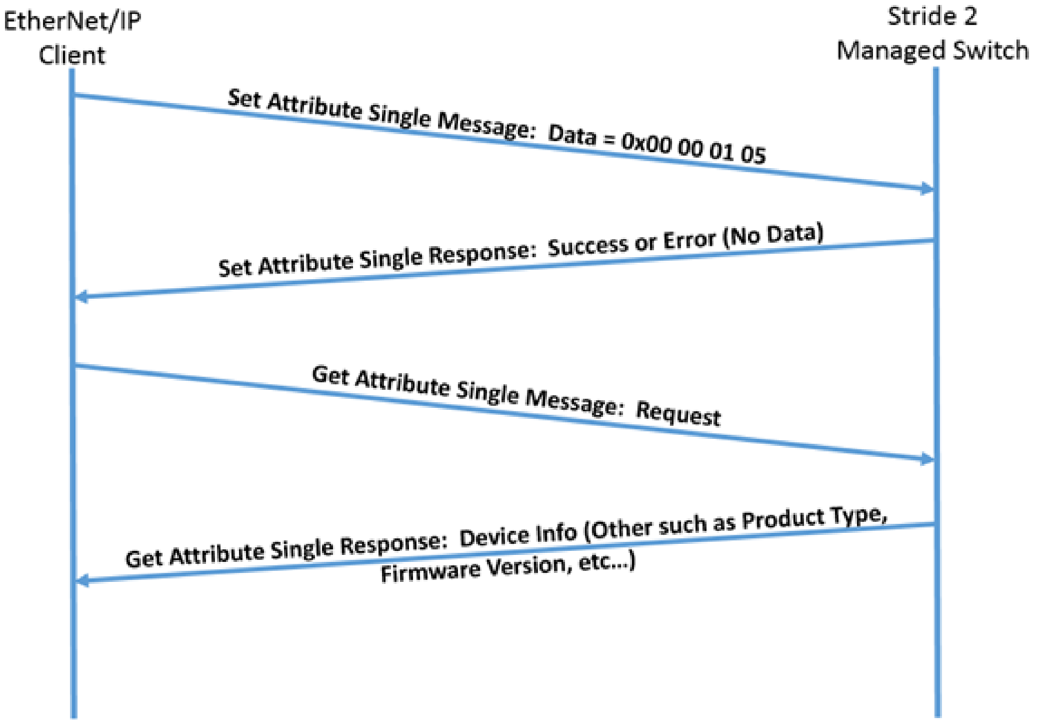
- To retrieve the Manufacturer Address, Bytes 0 – 3 should contain the following (in respective order) = 00 00 01 03
- To retrieve the Information for RSTP Ring 4, Bytes 0 – 3 should contain the following = 00 00 05 04

NOTE: *The first four bytes of "Set Attribute Single Service" message determine the response of the "Get Attribute Single Service" message. The "Set Attribute Single Service" response is always the same and does not contain the information in the switch.*

To Enable/Disable Ports and retrieve Port status (same as I/O Messaging):


EtherNet/IP
Client
Stride 2
Managed Switch
Set Attribute Single Message: Data = 0x01 00 [20 bytes to set Port status]
Same as I/O messaging Output Data
Set Attribute Single Response: Success or Error (No Data)
Get Attribute Single Message: Request
Get Attribute Single Response: Port status info (same as I/O messaging Input)

To retrieve extended data: Example: Device Info (Other):


EtherNet/IP Client
Stride 2 Managed Switch
Set Attribute Single Message: Data = 0x00 00 01 05
Set Attribute Single Response: Success or Error (No Data)
Get Attribute Single Message: Request
Get Attribute Single Response: Device Info (Other such as Product Type, Firmware Version, etc...)

The tables on the following pages detail the format of the data returned by the various information areas outlined in the table above.

Device Information				
Byte Offset Number	Size (in Bytes)	Data Type	Name	Details
Device Information: Manufacturer Name (Set Attribute Single = 0x00 00 01 01)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	258	ASCII	Mfg Name	Example: “A” = 0x41 “u” = 0x75 “t” = 0x74 “o” = 0x6f “m” = 0x6d “a” = 0x61 “t” = 0x74 etc.......
Device Information: Device Type (Set Attribute Single = 0x00 00 01 02)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	258	ASCII	Model Number	Example: “S” = 0x53 “E” = 0x45 etc.....
Device Information: Manufacturer Address (Set Attribute Single = 0x00 00 01 03)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	258	ASCII	Location	Example: “3” = 0x33 “5” = 0x35 etc.....
Device Information: Contact Phone Number (Set Attribute Single = 0x00 00 01 04)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	258	ASCII	Contact Phone Number	Example: “1” = 0x31 “(” = 0x28 etc.....

Device Information (cont'd)				
Byte Offset Number	Size (in Bytes)	Data Type	Name	Details
Device Information: Other Info (Set Attribute Single = 0x00 00 01 05)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	40	ASCII	Model Number	Example: "S"= 0x53 "t" = 0x74 "r" = 0x72 "i" = 0x69 "d" = 0x64 "e" = 0x65 "S" = 0x53 "E" = 0x45 "2" = 0x32 etc.....
42	30	ASCII	Serial Number	ASCII formatted as shown in "Model Number" ex. above
72	22	ASCII	Bootrom Version	
94	18	ASCII	Current Firmware Version	
112	4	INT32	Switch Management Interface IP Address	192.168.0.1 (0xc0a80001)
116	2	INT16	Device MAC Address Number	
118	6	INT16	Device Full MAC Address	00-1E-CD-00-00-01 Word 0 HI byte = 0x00 Word 0 LO byte = 0x1e Word 1 HI byte = 0xcd Word 1 LO byte = 0x00 Word 2 HI byte = 0x00 Word 2 HI byte = 0x00
124	1	INT	Power 1 Status	Power Off = 0x00 Power On - 0x01
125	1	INT	Power 2 Status	Power Off = 0x00 Power On - 0x01 None = -x-2
126	2	INT16	CPU occupancy rate (long term)	
128	2	INT16	CPU occupancy rate (short term)	
130	4	INT32	Total Memory (bytes)	
134	4	INT32	Free memory (bytes)	
138	4	INT32	Device running time (minutes)	

Port Information				
Byte Offset Number	Size (in bytes)	Data Type	Name	Details
Port Information (Set Attribute Single = 0x00 00 02 01 - Number of ports on switch)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	64	ASCII	Port Description	"FE" or "GE"

66	1	INT	Port Status	Up/Down/Disable
				Disable = 0x00
				Up = 0x01
				Down = 0x02

67	1	INT	Port Rate	10/100/1000/10000M 10M = 0x00 100M = 0x01 1000M = 0x02 10000M = 0x03

68	1	INT	Port Duplex	Half/Full
				Half = 0x00
				Full = 0x01

69	1	INT	Port Flow Control Status	On/Off
				Off = 0x00
				On = 0x01

70	8	INT64	Port Received Packets	
78	8	INT64	Port Received Bytes	
86	8	INT64	Port Sent Packets	
94	8	INT64	Port Sent Bytes	
102	8	INT64	Port Received Unicast Packets	
110	8	INT64	Port Received Multicast Packets	
118	8	INT64	Port Received Broadcast Packets	
126	8	INT64	Port Sent Unicast Packets	
134	8	INT64	Port Sent Multicast Packets	
142	8	INT64	Port Sent Broadcast Packets	
150	8	INT64	Port Received Pause Frames	
158	8	INT64	Port Sent Pause Frames	
166	8	INT64	Port received CRC Error Packets	

AD-RING Information				
Byte Offset Number	**Size (in bytes)**	**Data Type**	**Name**	**Details**
AD-RING Information: Ring Mode (Set Attribute Single = 0x00 00 03 00)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff

2	2	INT16	Ring Working Mode	Port/VLAN
				Port = 0x0000
				VLAN = 0x0001

AD-RING Information: Ring Info (Set Attribute Single = 0x00 00 03 01-20 (32))				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	2	INT16	Ring ID	

4	2	INT16	Station Role	Master/Normal
				Master = 0x0000
				Normal = 0x0001

6	2	INT16	Ring Enable Status	Enable/Disable
				Disable = 0x0000
				Enable = 0x0001

8	2	INT16	Ring Status	Open/Close/Alarm
				Open = 0x000
				Close = 0x001
				Alarm = 0x0002

10	2	INT16	Port 1 Status of the Ring	Down/Forward/Block
				Down = 0x000
				Forward = 0x0001
				Block = 0x002

12	2	INT16	Port 2 Status of the Ring	Down/Forward/Block
				Down = 0x000
				Forward = 0x0001
				Block = 0x002

14	2	INT16	Ring Switching Times	

16	2	INT16	AD-RING+ Status	Disable = 0x000
				Enable = 0x0001

18	2	INT16	Backup Port Status	None = oxooo
				Forward = 0x0001
				Block = 0x0002

20	4	INT32	Backup Port 1 Status: IP	192.168.0.1 (0xc0 1e cd 00 00 01)
24	6	INT16	Backup Port 1 Status: MAC	00-1e-cd-00-00-01 (0x00 1e cd 00 00 01)

AD-RING Information (cont’d)				
Byte Offset Number	**Size (in bytes)**	**Data Type**	**Name**	**Details**

30	2	INT16	Backup Port 1 Status	None = 0x000
				Forward = 0x0001
				Block = 0x0002

32	4	INT32	Backup Port 2 Status: IP	192.168.0.0 (0x00 1e cd 00 00 01)
36	6	INT16	Backup Port Status: MAC	00-1e-cd-00-00-01 (0x00 1e cd 00 00 01)

42	2	INT16	Backup Port 2 Status	None = 0x000
				Forward = 0x0001
				Block = 0x0002

44	8	INT16	Ring Port 1 Info	
52	8	INT16	Ring Port 2 Info	
60	8	INT16	Backup Port	
68	2	INT16	Main Port	0 = disable, non-zero = port number
70	32	INT16	VLAN List	

AD-RP RING Information

Byte Offset Number	Size (in bytes)	Data Type	Name	Details
AD-RP RING Information: Ring Mode (Set Attribute Single = 0x00 00 04 00)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff

2	2	INT16	Ring Working Mode	Port or VLAN
				Port = 0x0000
				VLAN = 0x0001

AD-RP RING Information: Ring Info (Set Attribute Single = 0x00 00 04 01-20 (32))				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff
2	2	INT16	Ring ID	

4	2	INT16	Station Role	Init = 0x0000
				Root = 0x0001
				B-Root = 0x0002
				Normal = 0x0003

6	2	INT16	Station Priority	

8	2	INT16	Ring Protocol Enable Status	Disable = 0x0000
				Enable = 0x0001

10	2	INT16	Ring Status	Init = 0x0000
				Open = 0x0001
				Close = 0x0002
				None = 0x0003

12	2	INT16	Ring Port 1 Link Status	Down = 0x0000
				Up = 0x0001

14	2	INT16	Ring Port 2 Link Status	
16	2	INT16	Backup Port Link Status	

18	2	INT16	Ring Port 1 Block Status	Forwarding = 0x0000
				Blocked = 0x0001
				Linkdown = 0x0002

20	2	INT16	Ring Port 2 Block Status	
24	8	INT16	Ring Port 1 Info	Ring Number
32	8	INT16	Ring Port 2 Info	
40	8	INT16	Backup Port	
48	2	INT16	Priority Port	None = 0x0000 Ring Port 1 = 0x0001 Ring Port 2 = 0x0002
50	2	INT16	CRC Threshold	

AD-RP RING Information (cont’d)				
Byte Offset Number	Size (in bytes)	Data Type	Name	Details
52	2	INT16	DHP Mode	Disable = 0x0000 Normal Node = 0x0001 Home Node = 0x0002
54	2	INT16	Home Port	None - 0x0000 Ring Port 1 = 0x0001 Ring Port 2 = 0x0002 Ring Port 1-2 = 0x0003
56	4	INT16	Boot IP	0 or the IP address. Ex: 192.168.0.1 (0xc0 a8 00 01)
60	2		Protocol VLAN	All 0xFF if none
62	32	INT16	Protected VLAN	16 VLAN, All 0xFF if none

RSTP Information				
Byte Offset Number	**Size (in bytes)**	**Data Type**	**Name**	**Details**
RSTP Information: Root Bridge Status (Set Attribute Single = 0x00 00 05 00)				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff

2	2	INT16	Protocol Enable Status	Disable = 0x0000
				Enable = 0x0001

4	8	INT16	Root Bridge ID	Combination of priority and MAC address Example: Priority = 0x8000 MAC = 00-1e-cd-00-00-01 Root Bridge ID = 0x8000001ecd000001
12	8	INT16	Bridge ID	Combination of priority and MAC address
20	2	INT16	Spanning Tree Priority	
22	2	INT16	Hello Time	
24	2	INT16	Max Age Time	
26	2	INT16	Forward Delay Time	

28	2	INT16	Message-age Increment	Compulsion = 0x0001
				Default = 0x0002

RSTP Information: Ring Info (Set Attribute Single = 0x00 00 05 01-20 (32))				
0	2	INT16	Query Status	Query Successful = 0x0000 Query Failure = 0xffff

2	2	INT16	Port Protocol Enable Status	Disable = 0x0000
				Enable = 0x0001

4	2	INT16	Port Priority	Init = 0x0000
6	4	INT32	Routing Cost	

10	2	INT16	Cost Automatic Calculation Status	Disable = 0x0000
				Enable = 0x0001

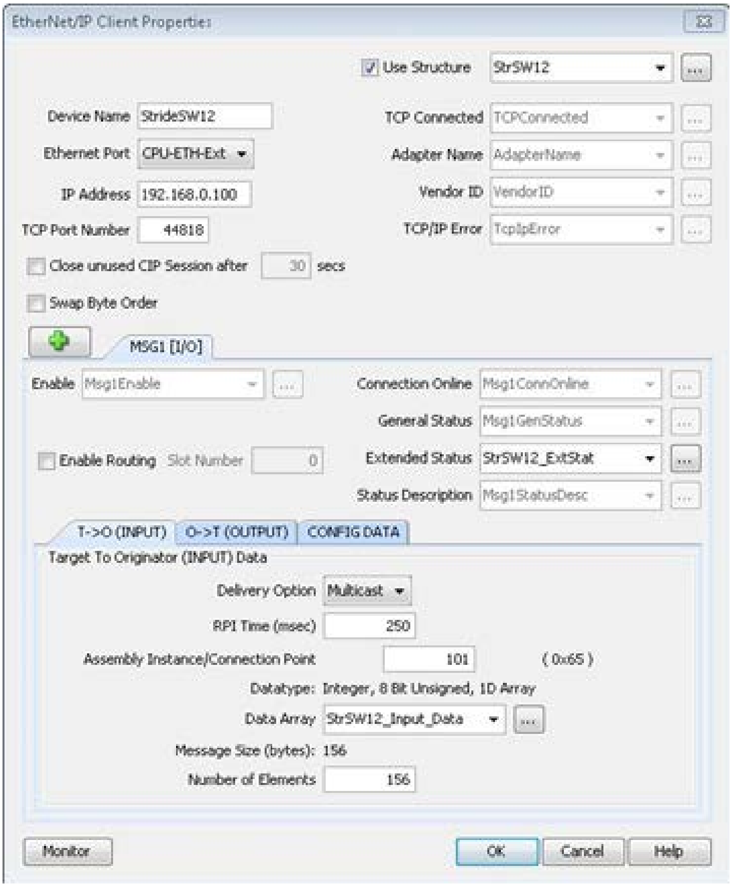
12	2	INT16	Port Role	Designated = 0x0000
				Root = 0x0001
				Alternate = 0x0002
				Backup = 0x0003
				Edge = 0x0004
				RSTP disable = 0x0005
				Linkdown - 0x0006

14	2	INT16	Port Status	Forwarding = 0x0001
				Blocked = 0x0002

Examples

Productivity 2000 I/O Messaging

Input Data



EtherNet/IP Client Properties

☑ Use Structure: StrSW12

Device Name: StrideSW12

Ethernet Port: CPU-ETH-Ext

IP Address: 192.168.0.100

TCP Port Number: 44818

☐ Close unused CIP Session after 30 secs

☐ Swap Byte Order

TCP Connected: TCPConnected

Adapter Name: AdapterName

Vendor ID: VendorID

TCP/IP Error: TcpIpError

MSG1 [I/O]

Enable: Msg1Enable

Connection Online: Msg1ConnOnline

General Status: Msg1GenStatus

☐ Enable Routing   Slot Number: 0

Extended Status: StrSW12_ExtStat

Status Description: Msg1StatusDesc

T->O (INPUT) | O->T (OUTPUT) | CONFIG DATA

Target To Originator (INPUT) Data

Delivery Option: Multicast

RPI Time (msec): 250

Assembly Instance/Connection Point: 101 (0x65)

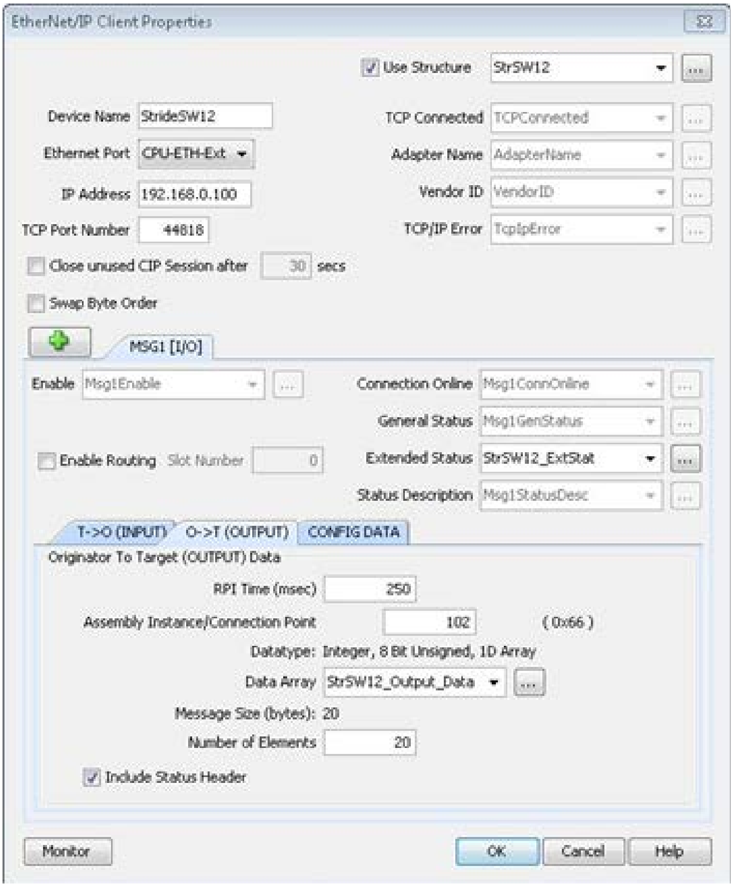
Datatype: Integer, 8 Bit Unsigned, 1D Array

Data Array: StrSW12_Input_Data

Message Size (bytes): 156

Number of Elements: 156

Output Data



EtherNet/IP Client Properties

☑ Use Structure: StrSW12

Device Name: StrideSW12

Ethernet Port: CPU-ETH-Ext

IP Address: 192.168.0.100

TCP Port Number: 44818

TCP Connected: TCPConnected

Adapter Name: AdapterName

Vendor ID: VendorID

TCP/IP Error: TcpIpError

□ Close unused CIP Session after 30 secs

□ Swap Byte Order

MSG1 [I/O]

Enable: Msg1Enable

Connection Online: Msg1ConnOnline

General Status: Msg1GenStatus

□ Enable Routing Slot Number: 0

Extended Status: StrSW12_ExtStat

Status Description: Msg1StatusDesc

T->O (INPUT) | O->T (OUTPUT) | CONFIG DATA

Originator To Target (OUTPUT) Data

RPI Time (msec): 250

Assembly Instance/Connection Point: 102 (0x66)

Datatype: Integer, 8 Bit Unsigned, 1D Array

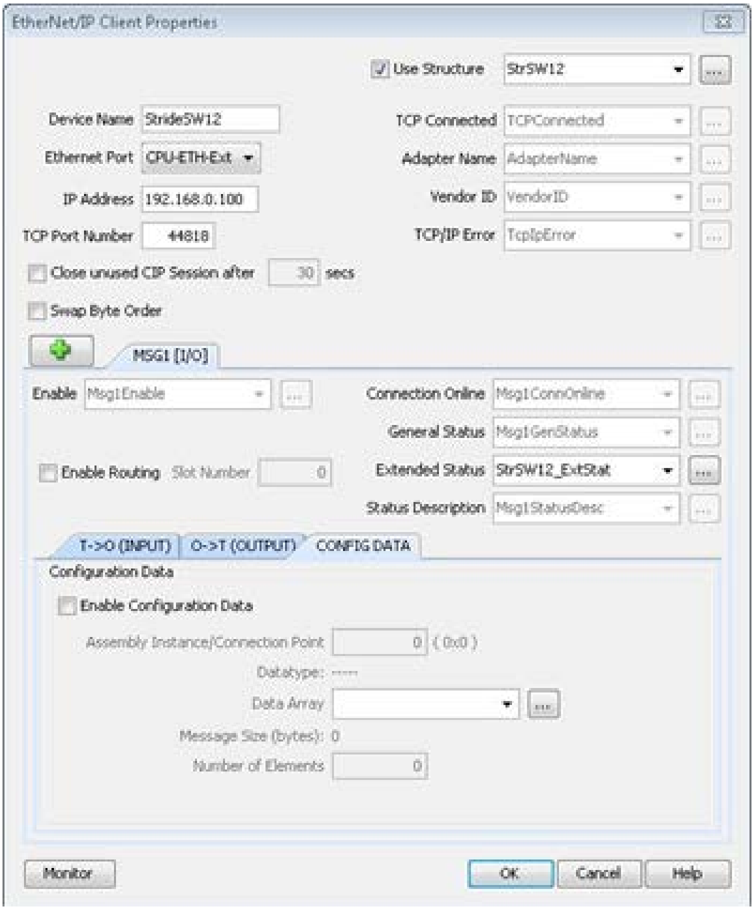
Data Array: StrSW12_Output_Data

Message Size (bytes): 20

Number of Elements: 20

☑ Include Status Header

Configuration Data (None)



EtherNet/IP Client Properties

☑ Use Structure: StrSW12

Device Name: StrideSW12

Ethernet Port: CPU-ETH-Ext

IP Address: 192.168.0.100

TCP Port Number: 44818

☐ Close unused CIP Session after 30 secs

☐ Swap Byte Order

TCP Connected: TCPConnected

Adapter Name: AdapterName

Vendor ID: VendorID

TCP/IP Error: TcpIpError

MSG1 [I/O]

Enable: Msg1Enable

☐ Enable Routing Slot Number: 0

Connection Online: Msg1ConnOnline

General Status: Msg1GenStatus

Extended Status: StrSW12_ExtStat

Status Description: Msg1StatusDesc

T->O (INPUT) | O->T (OUTPUT) | CONFIG DATA

Configuration Data

☐ Enable Configuration Data

Assembly Instance/Connection Point: 0 (0x0)

Datatype: -----

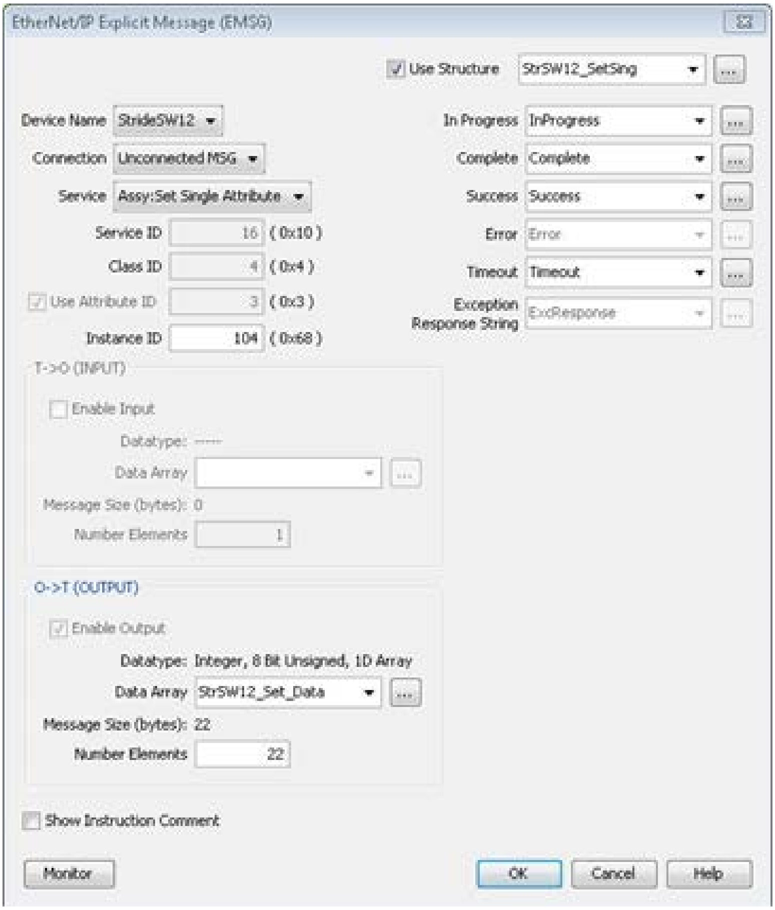
Data Array:

Message Size (bytes): 0

Number of Elements: 0

Productivity 2000 Explicit Messaging

Set Single Attribute Service



EtherNet/IP Explicit Message (EMSG)

☑ Use Structure: StrSW12_SetSing

Device Name: StrideSW12

Connection: Unconnected MSG

Service: Assy:Set Single Attribute

Service ID: 16 (0x10)

Class ID: 4 (0x4)

☑ Use Attribute ID: 3 (0x3)

Instance ID: 104 (0x68)

In Progress: InProgress

Complete: Complete

Success: Success

Error: Error

Timeout: Timeout

Exception Response String: ExcResponse

T->O (INPUT)

□ Enable Input

Datatype: -----

Data Array:

Message Size (bytes): 0

Number Elements: 1

O->T (OUTPUT)

☑ Enable Output

Datatype: Integer, 8 Bit Unsigned, 1D Array

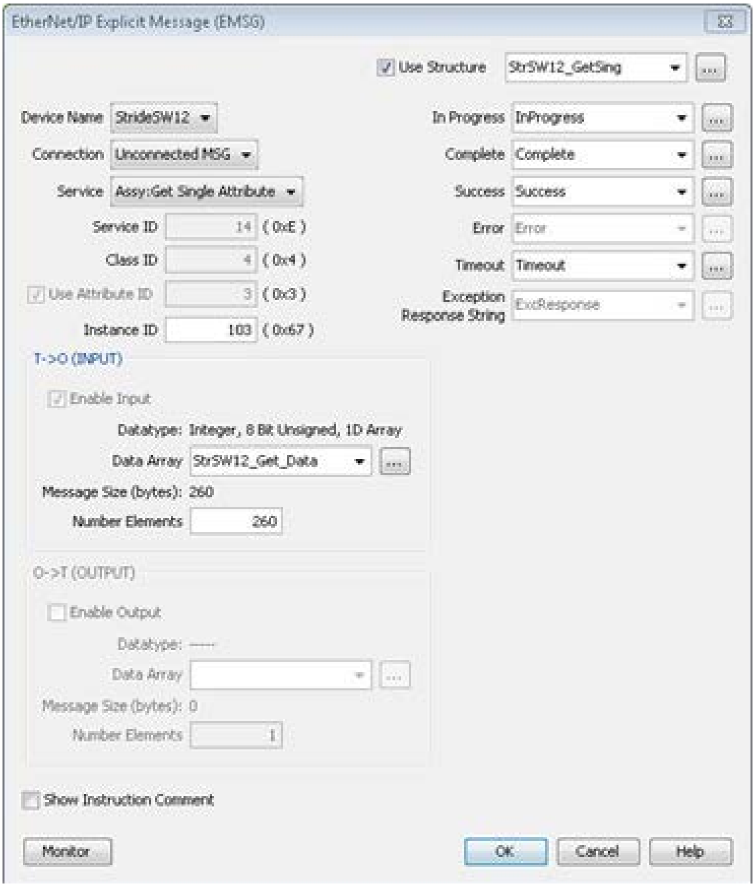
Data Array: StrSW12_Set_Data

Message Size (bytes): 22

Number Elements: 22

□ Show Instruction Comment

Get Single Attribute Service



EtherNet/IP Explicit Message (EMSG)

☑ Use Structure StrSW12_GetSing

Device Name StrideSW12

Connection Unconnected MSG

Service Assy:Get Single Attribute

Service ID 14 (0xE)

Class ID 4 (0x4)

☑ Use Attribute ID 3 (0x3)

Instance ID 103 (0x67)

In Progress InProgress

Complete Complete

Success Success

Error Error

Timeout Timeout

Exception Response String ExcResponse

T->O (INPUT)

☑ Enable Input

Datatype: Integer, 8 Bit Unsigned, 1D Array

Data Array StrSW12_Get_Data

Message Size (bytes): 260

Number Elements 260

O->T (OUTPUT)

□ Enable Output

Datatype: -----

Data Array

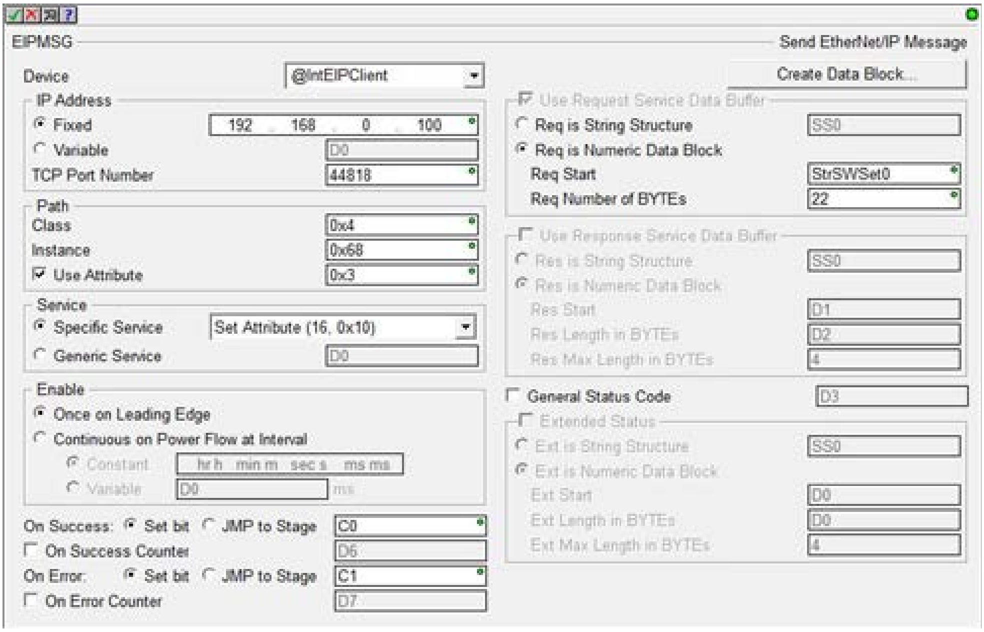
Message Size (bytes): 0

Number Elements 1

□ Show Instruction Comment

Do-more Explicit Messaging

Set Single Attribute Service



EIPMSG — Send EtherNet/IP Message

Device: @IntEIPClient

Create Data Block...

IP Address
● Fixed: 192 . 168 . 0 . 100
○ Variable: D0
TCP Port Number: 44818

Path
Class: 0x4
Instance: 0x68
☑ Use Attribute: 0x3

Service
● Specific Service: Set Attribute (16, 0x10)
○ Generic Service: D0

Enable
● Once on Leading Edge
○ Continuous on Power Flow at Interval
● Constant: hr h min m sec s ms ms
○ Variable: D0 ms

On Success: ● Set bit ○ JMP to Stage: C0
□ On Success Counter: D6
On Error: ● Set bit ○ JMP to Stage: C1
□ On Error Counter: D7

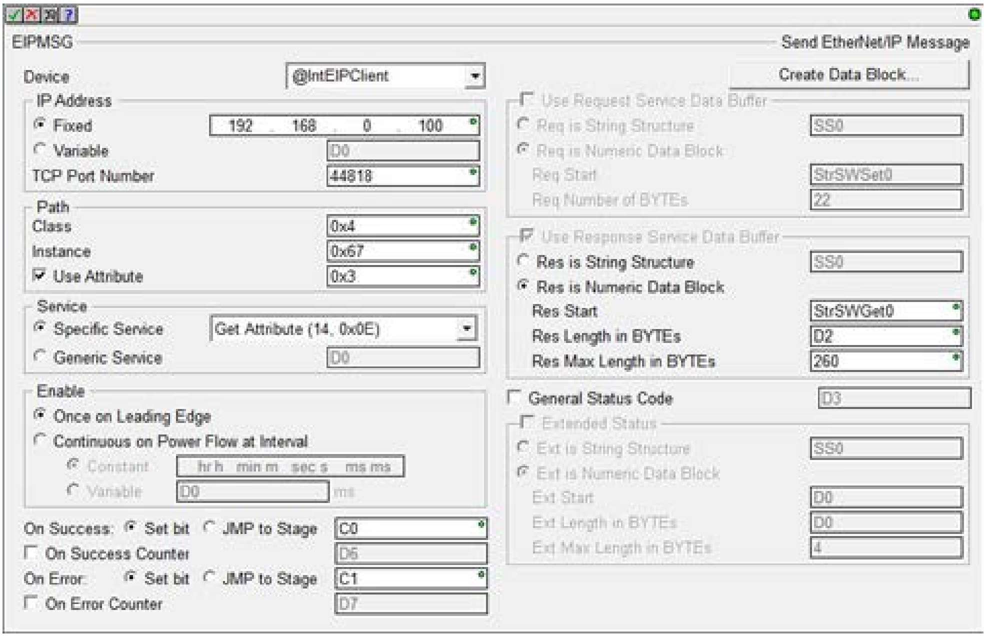
☑ Use Request Service Data Buffer
○ Req is String Structure: SS0
● Req is Numeric Data Block
Req Start: StrSWSet0
Req Number of BYTEs: 22

□ Use Response Service Data Buffer
○ Res is String Structure: SS0
● Res is Numeric Data Block
Res Start: D1
Res Length in BYTEs: D2
Res Max Length in BYTEs: 4

□ General Status Code: D3

□ Extended Status
○ Ext is String Structure: SS0
● Ext is Numeric Data Block
Ext Start: D0
Ext Length in BYTEs: D0
Ext Max Length in BYTEs: 4

Get Single Attribute Service



EIPMSG — Send EtherNet/IP Message

Create Data Block...

Device: @IntEIPClient

IP Address
- ● Fixed: 192 . 168 . 0 . 100
- ○ Variable: D0
- TCP Port Number: 44818

Path
- Class: 0x4
- Instance: 0x67
- ☑ Use Attribute: 0x3

Service
- ● Specific Service: Get Attribute (14, 0x0E)
- ○ Generic Service: D0

Enable
- ● Once on Leading Edge
- ○ Continuous on Power Flow at Interval
  - ● Constant: hr h min m sec s ms ms
  - ○ Variable: D0 ms

On Success: ● Set bit ○ JMP to Stage: C0

□ On Success Counter: D6

On Error: ● Set bit ○ JMP to Stage: C1

□ On Error Counter: D7

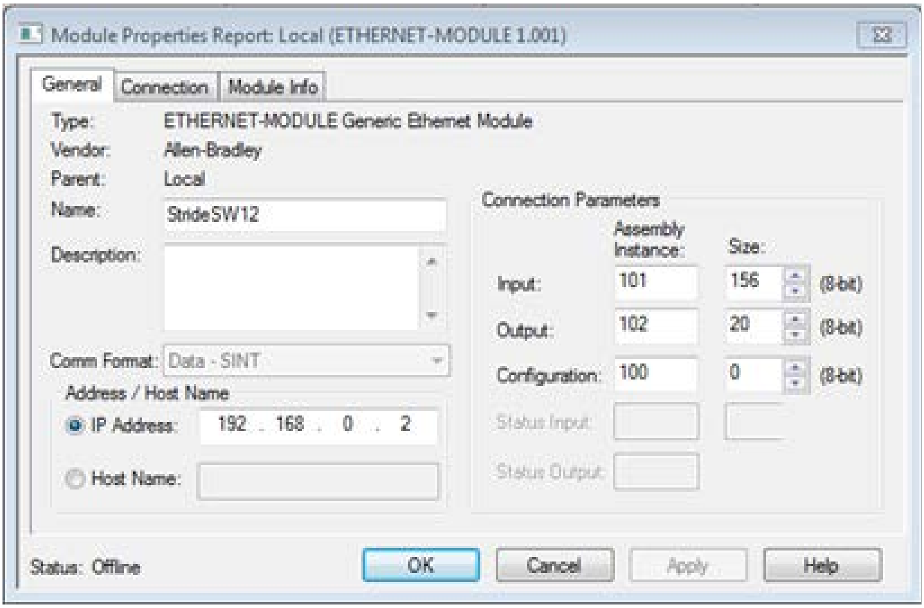
□ Use Request Service Data Buffer
- ○ Req is String Structure: SS0
- ● Req is Numeric Data Block
- Req Start: StrSWSet0
- Req Number of BYTEs: 22

☑ Use Response Service Data Buffer
- ○ Res is String Structure: SS0
- ● Res is Numeric Data Block
- Res Start: StrSWGet0
- Res Length in BYTEs: D2
- Res Max Length in BYTEs: 260

□ General Status Code: D3

□ Extended Status
- ○ Ext is String Structure: SS0
- ● Ext is Numeric Data Block
- Ext Start: D0
- Ext Length in BYTEs: D0
- Ext Max Length in BYTEs: 4

CompactLogix I/O Messaging



Module Properties Report: Local (ETHERNET-MODULE 1.001)

Type: ETHERNET-MODULE Generic Ethernet Module

Vendor: Allen-Bradley

Parent: Local

Name: Stride SW12

Description:

Comm Format: Data - SINT

Address / Host Name

● IP Address: 192 . 168 . 0 . 2

○ Host Name:

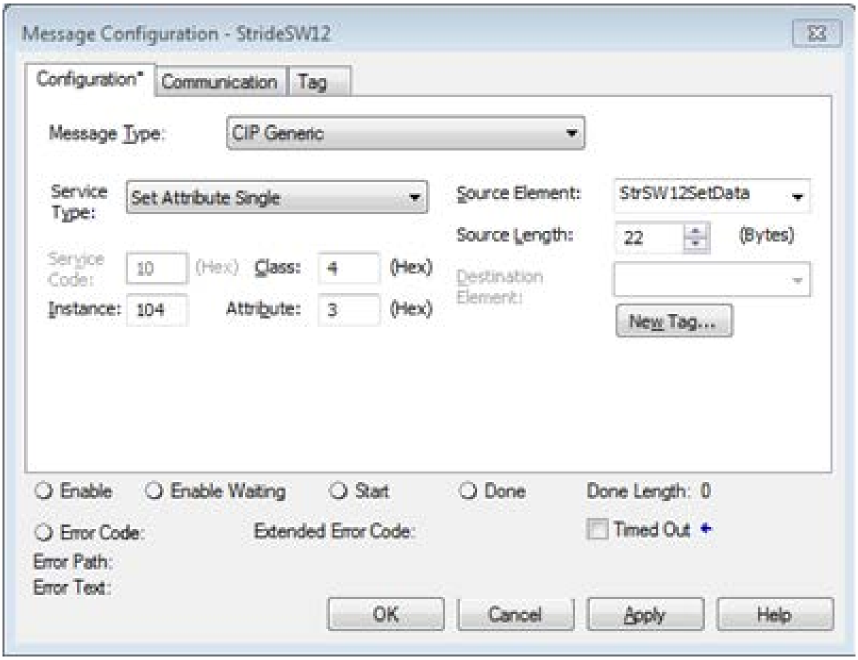
Connection Parameters

	Assembly Instance:	Size:	
Input:	101	156	(8-bit)
Output:	102	20	(8-bit)
Configuration:	100	0	(8-bit)
Status Input:			
Status Output:			

Status: Offline

CompactLogix Explicit Messaging

Set Single Attribute Service



Message Configuration - StrideSW12

Configuration* | Communication | Tag

Message Type: CIP Generic

Service Type: Set Attribute Single

Service Code: 10 (Hex)

Class: 4 (Hex)

Instance: 104

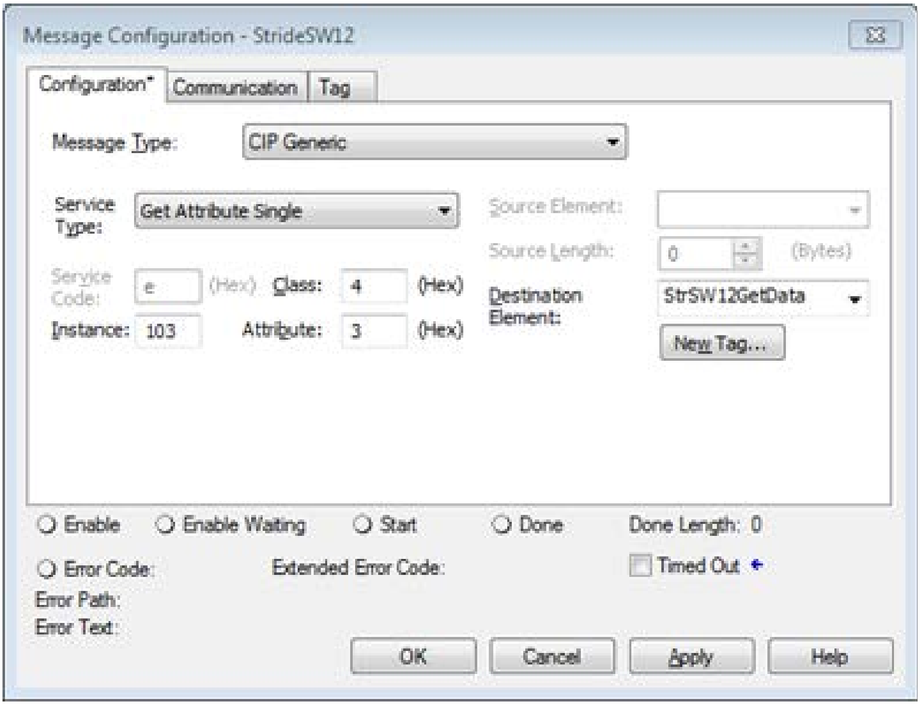
Attribute: 3 (Hex)

Source Element: StrSW12SetData

Source Length: 22 (Bytes)

Destination Element:

Get Single Attribute Service



Message Configuration - StrideSW12

Message Type: CIP Generic

Service Type: Get Attribute Single

Service Code: e (Hex)

Class: 4 (Hex)

Instance: 103

Attribute: 3 (Hex)

Source Element:

Source Length: 0 (Bytes)

Destination Element: StrSW12GetData

○ Enable ○ Enable Waiting ○ Start ○ Done Done Length: 0

○ Error Code: Extended Error Code: □ Timed Out

Error Path:

Error Text:

Modbus TCP

Appendix E

In this Appendix...

MODBUS TCP Definition

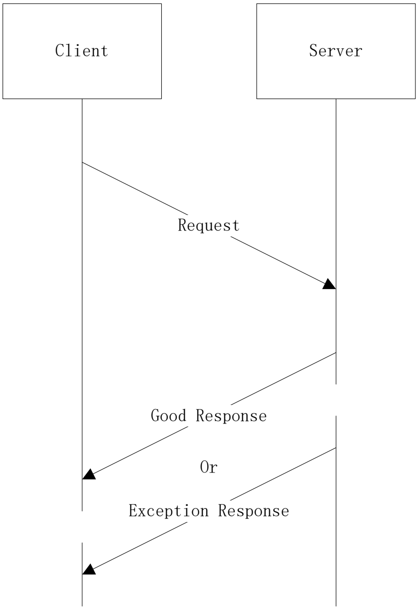
Port Definition

The MODBUS TCP server listening port is the standard value of 502.

Communication Process

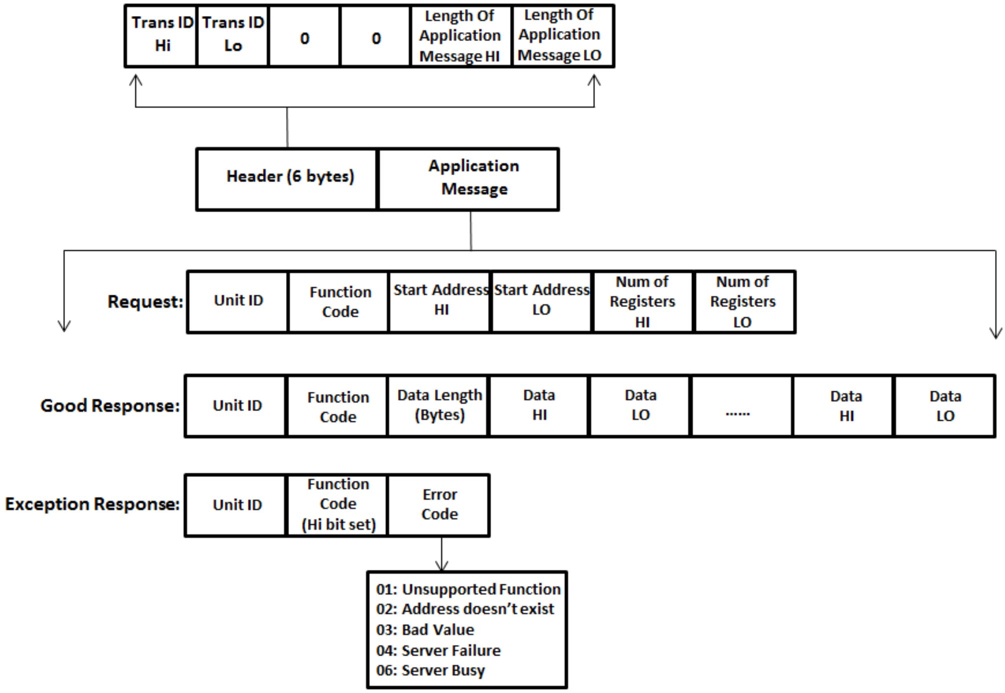
MODBUS information communication process is described below:

1. Client sends request to the switch;
2. The Switch (Server) receives the request and responds with a good response followed by the data requested or an exception response (high bit of Function Code set on) followed by the error code.



Information Frame Definition

MODBUS Frame definition is described below:



The Header is 6 bytes. Typically, the Transaction ID is incremented by 1 on every transaction by the Client device. The Server responds with the same value back.

The Unit ID is 1 byte.

The Function code is 1 byte and only Function Codes 3 and 4 are supported by the switch.

Maximum read size is 124 registers.

Function Code Definition

Function Code			
Item	**Function Code**	**Detail**	**Comments**
1	0x03	Holding Register	Read Register
2	0x04	Input Register	Read Register

Addresses are READ ONLY except where identified R/W in the tables that follow.

Example

Read the 4th register on server with Unit ID 01.

00 00 00 00 00 06 01 03 00 04 00 01– reads the value from 4th register address

00 00 00 00 00 05 01 03 02 00 05 – the response is 1 register (2 bytes) with a value of 5.

Read the value of the 4th and 5th register address from server with Unit ID 01.

00 00 00 00 00 06 01 03 00 04 00 02– Reads starting register 04 with a size of 2
00 00 00 00 00 07 01 03 04 00 05 00 04–The response to these 2 registers are 5 and 4.
00 00 00 00 00 03 01 83 0 – An example Exception Response. Unsupported Function Code error.

Switch MODBUS MAP

Addressing is described in 2 different ways

- Protocol Address
- Modbus Address

Protocol Addressing is more clear when writing the protocol itself or working with a Modbus master device that presents the data in a manner very closely tied to the protocol fields. As shown in the information of the previous section, the Modbus protocol request contains the Function code and the offset address from 0 in hexadecimal numbering.

Modbus Addressing makes more sense for devices that present the Modbus registers in a Modicon PLC style addressing where the high digit indicates the data type (4 for Holding Registers and 3 for Input Registers) followed by the offset from 1 in decimal numbering.

The tables below show only the Holding Register format (4xxxxx) for use with Function Code 3 but you could also substitute the upper 4 for 3 when doing Function Code 4 (reading Input Registers).

Register Address Allocation

Item	Description	Protocol Address	Modbus Address
1	Device Information	0x0000 – 0x0fff	400001 – 404096
2	Port Information	0x1000 – 0x2fff	404097 – 412288
3	Alarm Information	0x3000 – 0x3fff	412289 – 416384
4	AD-Ring Information	0x4000 – 0x4fff	416385 – 420480
5	AD-RP Ring Information	0x5000 – 0x5fff	420481 – 424576
6	RSTP Ring Information	0x6000 – 0x6fff	424577 – 428672

Addresses are READ ONLY except where identified R/W in the tables that follow.

Register Information

Device Information

Modbus Address	Protocol Address	Size	Data Type	Data Name	Register Sample
400001–400255	0x0000–0x00ff	255	ASCII	Manufacturer Name	Word 0 HI byte = ‘A Word 0 LO byte = ‘u Word 1 HI byte = ‘t’ Word 1 LO byte = ‘o’ Word 2 HI byte = ‘m’ Word 2 LO byte = ‘a’…
400257–400512	0x0100–0x01ff	255	ASCII	Device type	Industrial Ethernet Switch
400513–400768	0x0200–0x02ff	255	ASCII	Manufacturer address	3505 Hutchinson Road, Cumming, GA 30040
400769–401024	0x0300–0x03ff	255	ASCII	Contact phone number	
401025–401044	0x0400–0x0413	20	ASCII	Product type	
401057–401071	0x0420–0x042e	15	ASCII	Serial number	
401089–401099	0x0440–0x044a	11	ASCII	Bootrom version	
401121–401129	0x0460–0x0468	9	ASCI	FW version	
401153–401156	0x0480–0x0483	4	ASCII	Reserved for future use	
401281–401300	0x0500–0x0513	20	ASCII	Reserved for future use	
401537–401538	0x0600–0x0601	2	INT16	Switch management interface IP information	192.168.0.1 Word 0 HI byte = 192(0xC0) Word 0 LO byte = 168(0xA8) Word 1 HI byte = 0(0x00) Word 1 LO byte = 1(0x01)
401539–401541	0x0602–0x0604	3	INT16	Device MAC address	00–1E–CD–00–00–01 Word 0 HI byte = 0x00 Word 0 LO byte = 0x1E Word 1 HI byte = 0xCD Word 1 LO byte – 0x00 Word 2 HI byte = 0x00 Word 2 LO byte = 0x01
401542	0x0605	1	INT16	Reserved for future use	
401543	0x0606	1	INT16	Power 1 status	0x0000 = None 0x0001 = Power ON 0x0002 = Power OFF
401544	0x0607	1	INT16	Power 2 status	
401545	0x0608	1	INT16	CPU usage (long term)	
401546	0x0609	1	INT16	CPU usage (short term)	
401547–401548	0x060a–0x060b	2	INT32	Total memory (in bytes)	
401549–401550	0x060c–0c060d	2	INT32	Available memory (in bytes)	
401551–401552	0x060e–0x060f	2	INT32	Device operating time (minutes)	

Addresses are READ ONLY except where noted.

Information - Port 1 details

Modbus Address	Register Address	Offset from Beginning of Block	Size (in words)	Data Type	Data Name	Register Sample
404097–404128	0x1000	0	32	ASCII	Port 1 Port Type	Either “FE” (fast Ethernet) or “GE” (Gigabet Ethernet)
404129	0x1020	32	1	INT16	Port 1 Status READ/WRITE *	up/down/disable 0x0000 = disable 0x0001 = up 0x0002 = down
404130	0x1021	33	1	INT16	Port 1 Speed	10/100/1000/10000M 0x0000 = 10 0x0001 = 100 0x0002 = 1000 0x0003 = 10000
404131	0x1022	34	1	INT16	Port 1 Duplex	half/full 0x0000 = half 0x0001 = full
404132	0x1023	35	1	INT16	Port 1 Flow Control	on/off 0x0000 = off 0x0001 = on
404133–404136	0x1024	36	4	INT64	Port 1 Received Packets	–
404137–404140	0x1028	40	4	INT64	Port 1 Received Bytes	–
404141–404144	0x102C	44	4	INT64	Port 1 Sent Packets	–
404145–404148	0x1030	48	4	INT64	Port 1 Sent Bytes	–
404149–404152	0x1034	52	4	INT64	Port 1 Received Unicast Packets	–
404153–404156	0x1038	56	4	IINT64	Port 1 Received Multicast Packets	–
404157–404160	0x103C	60	4	INT64	Port 1 Received Broadcast Packets	–
404161–404164	0x1040	64	4	INT64	Port 1 Sent Unicast Packets	–
404165–404168	0x1044	68	4	INT64	Port 1 Sent Multicast Packets	–
404169–404172	0x1048	72	4	INT64	Port 1 Sent Broadcast Packets	–
404173–404176	0x104C	76	4	INT64	Port 1 Received Pause Frame	–
404177–404180	0x1050	80	4	INT64	Port 1 Sent Pause Frame	–
404181–404184	0x1054	84	4	INT64	Port 1 Received CRC Error Packets	–

Addresses are READ ONLY except Port Status.
*** Note that the only values to write to Port Status are:**
0x0000 to Disable the port,
0x0001 to Enable the port.

Addresses are READ ONLY except Port Status.
*** Note that the only values to write to Port Status are:**
0x0000 to Disable the port,
0x0001 to Enable the port.

Starting Modbus Address	Starting Protocol Address	Port Number
404255–404352	0x1080	Port 2 information. Use Starting Address from this table and add "Offset from Beginning of Block" from the Port Details table on the previous page to identify the address for each Port Information element.
404353	0x1100	3
404481	0x1180	4
404609	0x1200	5
404737	0x1280	6
404865	0x1300	7
404993	0x1380	8
405121	0x1400	9
405249	0x1480	10
405377	0x1500	11
405505	0x1580	12
405633	0x1600	13
405761	0x1680	14
405889	0x1700	15
406017	0x1780	16
406145	0x1800	17
406273	0x1880	18
406401	0x1900	19
406528	0x1980	20
406657	0x1a00	21
406785	0x1a80	22
406913	0x1b00	23
407041	0x1b80	24
407169	0x1c00	25
407297	0x1c80	26
407425	0x1d00	27
407553	0x1d80	28
407681	0x1e00	29
407809	0x1e80	30
407937	0x1f00	31
408065	0x1f80	32
|	|	|
V	V	V
412161	0xdf80	64

Port Status

Addresses are READ ONLY except where noted.
The value in the register is INT 16:
Port Disabled = 0x0000
Port activity normal = 0x0001
Port alarm condition = 0x0002

Protocol Address	Modbus Address	Port Number
0x3000	412289	1
0x3010	412305	2
0x3020	402321	3
0x3030	412337	4
0x3040	412353	5
0x3050	412369	6
0x3060	412385	7
0x3070	412401	8
0x380	412417	9
0x390	412433	10
0x30a0	412449	11
0x30b0	412465	12
0x30c0	412481	13
0x30d0	412497	14
0x30e0	412513	15
0x30f0	412529	16
0x3100	412545	17
0x3110	412561	18
0x3120	412577	19
0x3130	412593	20
0x3140	412609	21
0x3150	412625	22
0x3160	412641	23
0x3170	412657	24
0x3180	412673	25
0x3190	412689	26
0x31a0	412705	27
0x31b0	412721	28
0x31c0	412737	29
0x31d0	412753	30
0x31e0	412769	31
0x31f0	412785	32
|	|	|
V	V	V
0x33f0	413297	64

AD-Ring Status

Each ring status includes two words. The first word is the AD-Ring number status and the second word is the AD-RP Ring number status.

Addresses are READ ONLY except where noted.
The value in the register is INT 16:
Ring Disabled - 0x000
Ring activity Normal = 0x0001
Ring alarm condition = 0x0002

AD-RP is not configured = 0x0003
(Applies to second word, AD-RP ring status only)

Protocol Address	Modbus Address	Ring Number
0x3400	413313	AD-Ring 1
0x3401	413314	AD-RP Ring 1
0x3402–0x3403	413315–413316	2
0x3404–0x3405	413317–413318	3
0x3406–0x3407	413319–413320	4
0x3408–0x3409	413321–413322	5
0x340a–0x340b	413323–413324	6
0x340c–0x340d	413325–413326	7
0x340e–0x340f	413327–413328	8
0x3410–0x3411	413329–413330	9
0x3412–0x3413	413331–413332	10
0x3414–0x3415	413333–413334	11
0x3416–0x3417	413335–413336	12
0x3418–0x3419	413337–413338	13
0x341a–0x341b	413339–413340	14
0x341c–0x341d	413341–413342	15
0x341e–0x341f	413343–4133344	17
|	|	|
V	V	V
0x343e–0x343f	413375–413376	32

Alarm Information

Addresses are READ ONLY except where noted.

Protocol Address	Modbus Address	Alarm	Values

0x3501	413570	IP address conflict	Disabled = 0x0000
			Normal = 0x0001
			Alarm = 0x0002

0x3502	413571	MAC address conflict	Disabled = 0x0000
			Normal = 0x0001
			Alarm = 0x0002

0x3505	413574	Power Alarm	Disabled = 0x0000
			Normal = 0x0001
			Power 1 Alarm = 0x0002
			Power 2 Alarm = 0x0003

AD-Ring - Ring 1 details

Addresses are READ ONLY except where noted.

Protocol Address	Modbus Address	Offset from Beginning of Block	Size (in Words)	Data Type	Name	Details
0x4008	416393	8	1	INT16	AD-RING + STATUS	Down/Forward/Block Down = 0x0000 Forward = 0x0001 Block=0x0002
0x4009	416394	9	1	INT16	Backup Port Status	None = 0x0000 Forward = 0x0001 Block = 0x0002
0x400a – 0x400b	416395–416396	10	2	INT16	Backup Port Status: Backup Port 1 IP	Ex: 192.168.0.1 (0x00 1e cd 00 00 01)
0x400c – 0x400e	416397–416399	12	3	INT16	Backup Port Status: Backup Port 1 MAC	Ex: 00-1e-cd-00-00-01 (0x00 1e cd 00 00 01)
0x400f	416400	15	1	INT16	Backup Port Status: Backup Port 1 Status	None = 0x0000 Forward = 0x0001 Block = 0x0002
0x4010 – 0x4011	416401–416402	16	2	INT16	Backup Port Status: Backup Port 2 IP	Ex: 192.168.0.1 (0x00 1e cd 00 00 01)
0x4012 – 0x4014	416403–416405	18	3	INT16	Backup Port Status: Backup Port 2 MAC	Ex: 00-1e-cd-00-00-01 (0x00 1e cd 00 00 01)
0x4015	416406	21	1	INT16	Backup Port Status: Backup Port 2 Status	None = 0x0000 Forward = 0x0001 Block = 0x0002
0x4016 – 0x4019	416407–146410	22	4	ASCII	Ring Port 1 Status	Returns Port number in ASCII format
0x401a – 0x401d	416411–416414	26	4	ASCII	Ring Port 2 Status	
0x401e – 0x4021	416415–416418	30	4	ASCII	Backup Port	
0x4022	416419	34	1	INT16	Master Port	Returns 0 if port is disabled, Returns Port number if enabled
0x4023 – 0x4032	416420–416435	35	16	INT16	VLAN list	If VLAN is disabled, returns all 0xff, returns VLAN numbers if enabled

AD-Ring (cont'd)

Starting Protocol Address	Starting Modbus Address	Ring Number
0x4041	416450	Ring 2 information. Use Starting Address from this table and add "Offset from Beginning of Block" from the Ring Details table on the previous page to identify the address for each Ring Information element.
0x4081	416514	Ring 3
0x40c1	416578	Ring 4
0x4101	416642	Ring 5
0x4141	416706	Ring 6
0x4181	416770	Ring 7
0x41c1	416834	Ring 8
0x4201	416898	Ring 9
0x4241	416962	Ring 10
0x4281	417026	Ring 11
0x42c1	417090	Ring 12
0x4301	417154	Ring 13
0x4341	417218	Ring 14
0x4381	417282	Ring 15
0x43c1	417346	Ring 16
|	|	|
V	V	V
0x47c1	418370	Ring 32

AD-RP Ring - Ring 1 details

Addresses are READ ONLY except where noted.

Protocol Address	Modbus Address	Offset from Beginning of Block	Size (in Words)	Data Type	Name	Details
0x5000	420481	0	1	INT16	Ring Working Mode	Port/VLAN Port = 0x000 VLAN = 0x0001
0x5001	420482	1	1	INT16	Ring ID	–
0x5002	420483	2	1	INT16	Node Status	Init = 0x0000 Root = 0x0001 B-Root = 0x0002 Normal = 0x0003
0x5003	420484	3	1	INT16	Node Priority	–
0x5004	420485	4	1	INT16	Ring Protocol Enable Status	Enable/Disable Disable = 0x0000 Enable = 0x0001
0x5005	420486	5	1	INT16	Ring Status	Init = 0x0000 Open = 0x0001 Close = 0x0002 None = 0x0003
0x5006	420487	6	1	INT16	Ring Port 1 Blocking Status	Forwarding = 0x0000 Blocking = 0x0001
0x5007	420488	7	1	INT16	Ring Port 1 Link Status	Down = 0x0000 Up = 0x0001
0x5008	420489	8	1	INT16	Ring Port 2 Blocking Status	Forwarding = 0x0000 Blocking = 0x0001
0x5009	420490	9	1	INT16	Ring Port 2 Link Status	Down = 0x0000 Up = 0x0001
0x500a	420491	10	1	INT16	Backup Port Blocking Status	Forwarding = 0x0000 Blocking = 0x0001
0x500b	420492	11	1	INT16	Backup Port Link Status	Down = 0x0000 Up = 0x0001
0x500c - 0x500f	420493–420496	12	4	ASCII	Ring Port 1 Information	Returns Port number in ASCII format
0x5010 - 0x5013	420497–420500	16	4	ASCII	Ring Port 2 Information	
0x5014 - 0x5017	420501–420504	20	4	ASCII	Backup Port	
0x5018	420505	24	1	INT16	Port Priority	None = 0x0000 Ring Port 1 = 0x0001 Ring Port 2 = 0x0002
0x5019	420506	25	1	INT16	CRC Gap	–
0x501a	420507	26	1	INT16	DHP Mode	None = 0x0000 Normal mode = 0x0001 Home node = 0x0002
0x501b	420508	27	1	INT16	Home Port	None = 0x0000 Ring Port 1 = 0x0001 Ring Port 2 = 0x0002 Ring Port 1-2 = 0x0003
0x501c - 0x501d	420509–420510	28	2	INT32	Root IP	Returns 0 if switch is Root, otherwise returns IP in 32 bit format
0x501e	420511	30	1	INT16	Reserved for future use	Reserved
0x501f - 0x502e	420512–420527	31	16	INT16	Protected VLAN	If VLAN isn't enabled, returns 0xff. Otherwise returns VLAN numbers.

AD-RP Ring (cont'd)

Starting Protocol Address	Starting Modbus Address	Ring Number
0x5041	420546	Ring 2 information. Use Starting Address from this table and add “Offset from Beginning of Block” from the Ring Details table on the previous page to identify the address for each Ring Information element.
0x5081	420610	Ring 3
0x50c1	420674	Ring 4
0x5101	420738	Ring 5
0x5141	420802	Ring 6
0x5181	420866	Ring 7
0x51c1	420930	Ring 8
0x5201	420994	Ring 9
0x5241	421058	Ring 10
0x5281	421122	Ring 11
0x52c1	421186	Ring 12
0x5301	421250	Ring 13
0x5341	421314	Ring 14
0x5381	421378	Ring 15
0x53c1	421442	Ring 16
|	|	|
V	V	V
0x57c1	422466	Ring 32

RSTP Settings

Addresses are READ ONLY except where noted.

Protocol Address	Modbus Address	Offset from Beginning of Block	Size (in Words)	Data Type	Name	Details
0x6000	424577	N/A	1	INT16	RSTP Ring Enable Status	Disable= 0x000 Enable= 0x0001
0x6001–0x6004	424578–424581	N/A	4	INT16	Root ID	Priority combined with MAC Ex: Priority = 0x8000 MAC = 00-1e-cd-00-00-01 Result = 0x800000ecd000001
0x6005–0x6008	424582–424585	N/A	4	INT16	Bridge ID	
0x6009	424586	N/A	1	INT16	Spanning-tree Priority	–
0x600a	424587	N/A	1	INT16	Hello Time	–
0x600b	424588	N/A	1	INT16	Max Age Time	–
0x600c	424589	N/A	1	INT16	Forward Delay Time	–
0x600d	424590	N/A	1	INT16	Message-age Increment	Compulsion = 0x0000 Default = 0x0001

RSTP - Port 1 details

Addresses are READ ONLY except where noted.

Protocol Address	Modbus Address	Offset from Beginning of Block	Size (in Words)	Data Type	Name	Details
0x600e	424591	0	1	INT16	Port Enable Status	Disable= 0x000 Enable= 0x0001
0x600f	424592	1	1	INT16	Port Priority	–
0x6010–0x6011	424593–424594	2	2	INT32	Path Cost	–
0x6012	424595	4	1	INT16	Automatic Cost Status	Disable= 0x000 Enable= 0x0001
0x6013	424596	5	1	INT16	Ring Port Pole	Disabled Port = 0x000 Alternate Port = 0x0001 Backup Port = 0x0002 Root Port = 0x0003 Designated Port = 0x0004 Master Port = 0x0005 Non Stp Port = 0x0006
0x6014	424597	6	1	INT16	Ring Port Status	Forwarding = 0x0001 Blocked = 0x0002

RSTP Settings (cont'd)

Starting Protocol Address	Starting Modbus Address	Ring Number
0x6016	424599	Port 2 information. Use Starting Address from this table and add "Offset from Beginning of Block" from the Port Details table on the previous page to identify the address for each Port Information element.
0x601e	424607	Port 3
0x6026	424615	Port 4
0x602e	424623	Port 5
0x6036	424631	Port 6
0x603e	424639	Port 7
0x6046	424647	Port 8
0x604e	424655	Port 9
0x6056	424663	Port 10
0x605e	424671	Port 11
0x6066	424679	Port 12
0x606e	424687	Port 13
0x6076	424695	Port 14
0x607e	424703	Port 15
0x6086	424711	Port 16
0x608e	424719	Port 17
0x6096	424727	Port 18
0x609e	424735	Port 19
0x60a6	424743	Port 20
0x60ae	424751	Port 21
0x60b6	424759	Port 22
0x60be	424767	Port 23
0x60c6	424775	Port 24
0x60ce	424783	Port 25
0x60d6	424791	Port 26
0x60de	424799	Port 27
0x60e6	424807	Port 28
0x60ee	424815	Port 29
0x60f6	424823	Port 30
0x60fe	424831	Port 31
0x6106	424839	Port 32
|	|	|
V	V	V
0x6206	425095	Port 64

Security Considerations for Control Systems Networks

Appendix F

In this Appendix...

Security Considerations for Control Systems Networks

Manufacturers are realizing that to stay competitive, their Automation and Control Systems need to be more integrated within their plant. The systems often need to be integrated with upstream Enterprise Data Systems, and even further integrated to allow information to be accessible across multiple plants, or even through the Internet. This convergence of the IT world with the Automation World creates challenges in maintaining secure systems and protecting your investments in processes, personnel, data and intellectual property.

While Automation Networks and Systems have built-in password protection schemes, this is only one very small step in securing your systems. Automation Control System Networks need to incorporate data protection and security measures that are at least as robust as a typical business computer system. We recommend that users of PLCs, HMI products and SCADA systems perform your own network security analysis to determine the proper level of security required for you application. However, the Department of Homeland Security's National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has provided direction related to network security and safety under an approach described as "Defense in Depth", which is published at https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

This comprehensive security strategy involves physical protection methods, as well as process and policy methods. This approach creates multiple layers and levels of security for industrial automation systems. Such safeguards include the location of control system networks behind firewalls, their isolation from business networks, the use of intrusion detection systems, and the use of secure methods for remote access such as Virtual Private Networks (VPNs). Further, users should minimize network exposure for all control system devices and such control systems and these systems should not directly face the internet. Following these procedures should significantly reduce your risks both from external sources as well as internal sources, and provide a more secure system.

It is the user's responsibility to protect such systems, just as you would protect your computer and business systems. AutomationDirect recommends using one or more of these resources in putting together a secure system:

- ICS-CERT's Control Systems recommended practices at the following web address:
  https://ics-cert.us-cert.gov/Recommended-Practices
- Special Publication 800-82 of the National Institute of Standards and Technology – Guide to Industrial Control Systems (ICS) Security
  https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
- ISA99, Industrial Automation and Control Systems Security
  http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821
  (please note this is a summary and these standards have to be purchased from ISA)

The above set of resources provides a comprehensive approach to securing a control system network and reducing risk and exposure from security breaches. Given the nature of any system that accesses the internet, it is incumbent upon each user to assess the needs and requirements of Security Considerations for Control Systems Networks their application, and take steps to mitigate the particular security risks inherent in their control system.

Automation Direct®