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 C.

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

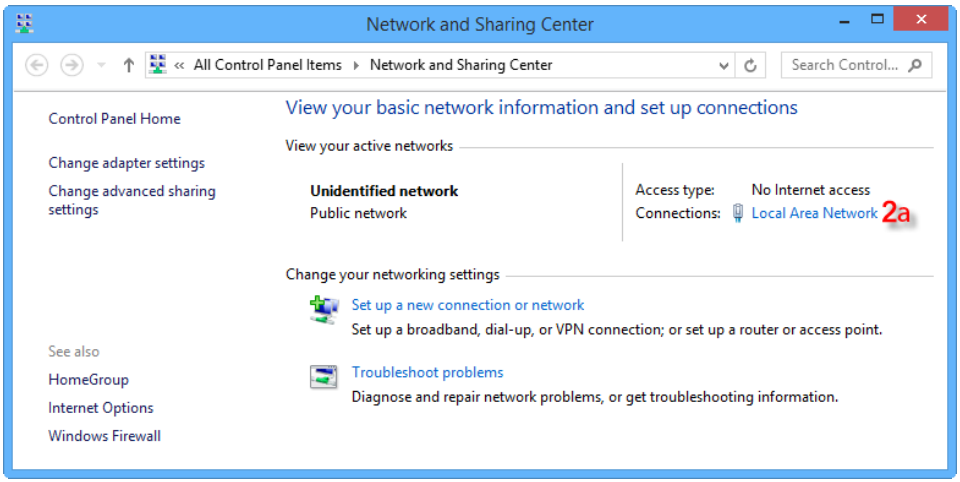
***NOTE**: All configuration changes except IP address and password must be committed to the switch by performing SAVE. If not committed by SAVE, changes will be lost on power cycle. Likewise, changes made by performing LOAD DEFAULTS must be committed to the switch by performing SAVE or else the switch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

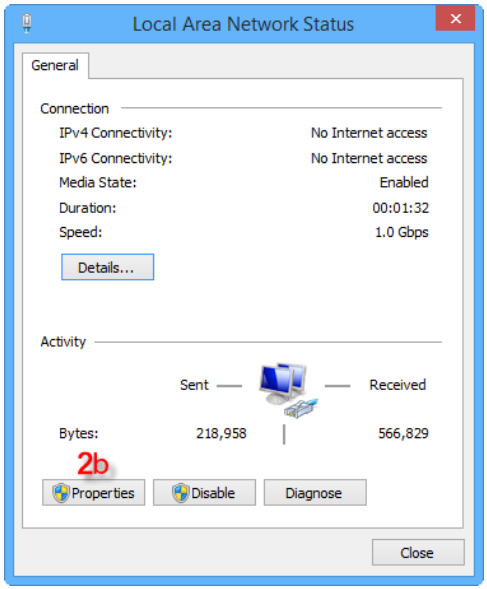
This example shows a switch connected directly to a PC running Windows 8.1.

1. Open Network and Sharing Center:



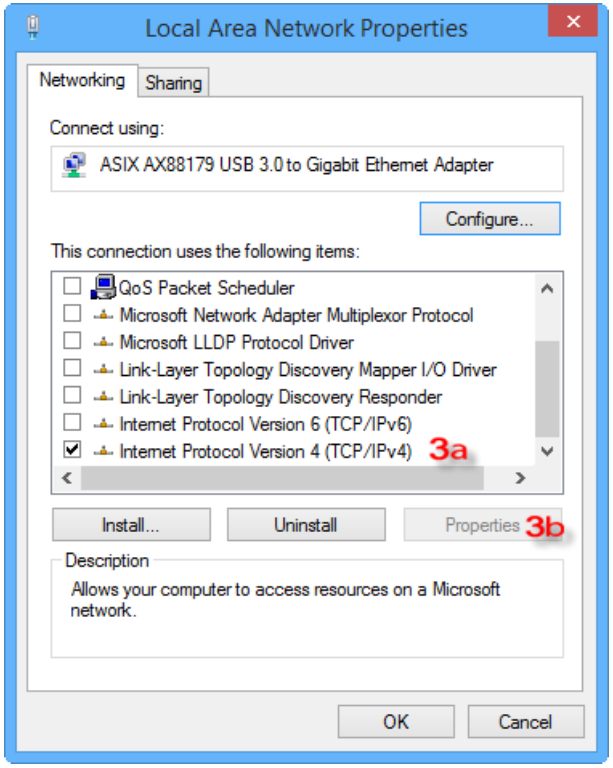
2a. Click on the name of the NIC connected to the switch to open the NIC status window.

2b. Click the Properties button:

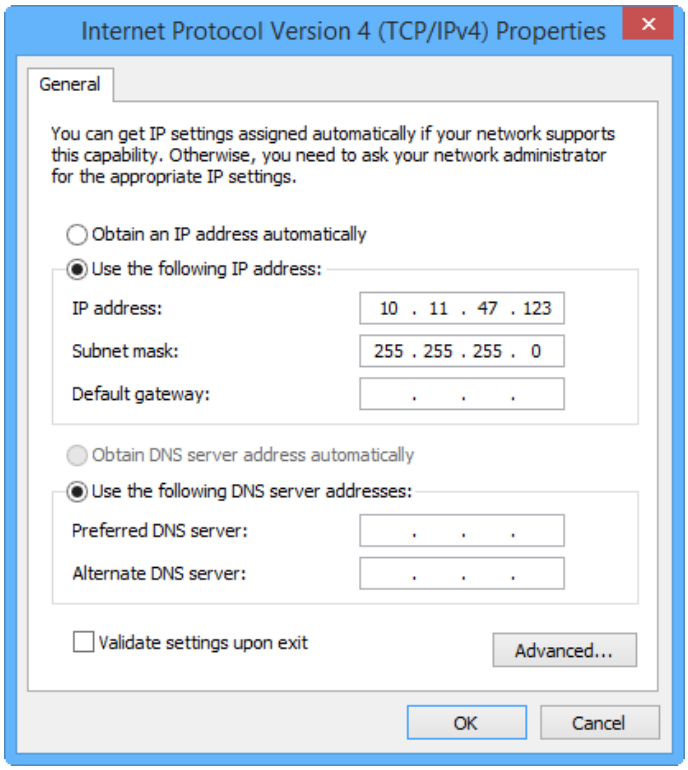


3a. Click to highlight Internet Protocol Version 4 (TCP/IPv4).

3b. Click the Properties button.



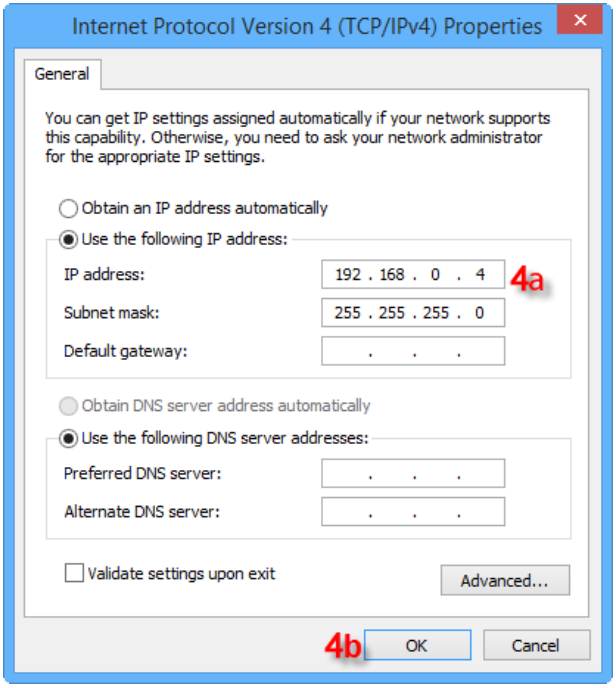
Write down (or screen capture) the existing settings so you can revert to them after we change the switch IP address. For our example, the PC starting IP address is 10.11.47.123, the subnet mask is 255.255.255.0 and there is no default gateway.



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.

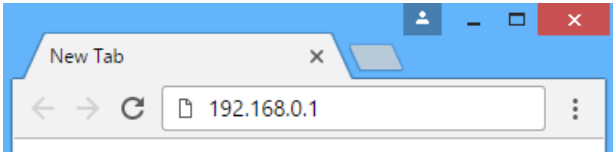
***NOTE 1**: Neither the Network Address nor the Broadcast Address for your subnet are valid host addresses. For our example where the Subnet Mask is 255.255.255.0 and the first three octets of the switch address are 192.168.0, neither the PC nor the switch may be assigned 192.168.0.0 or 192.168.0.255 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.



4c. Click CLOSE on the NIC Properties Window.

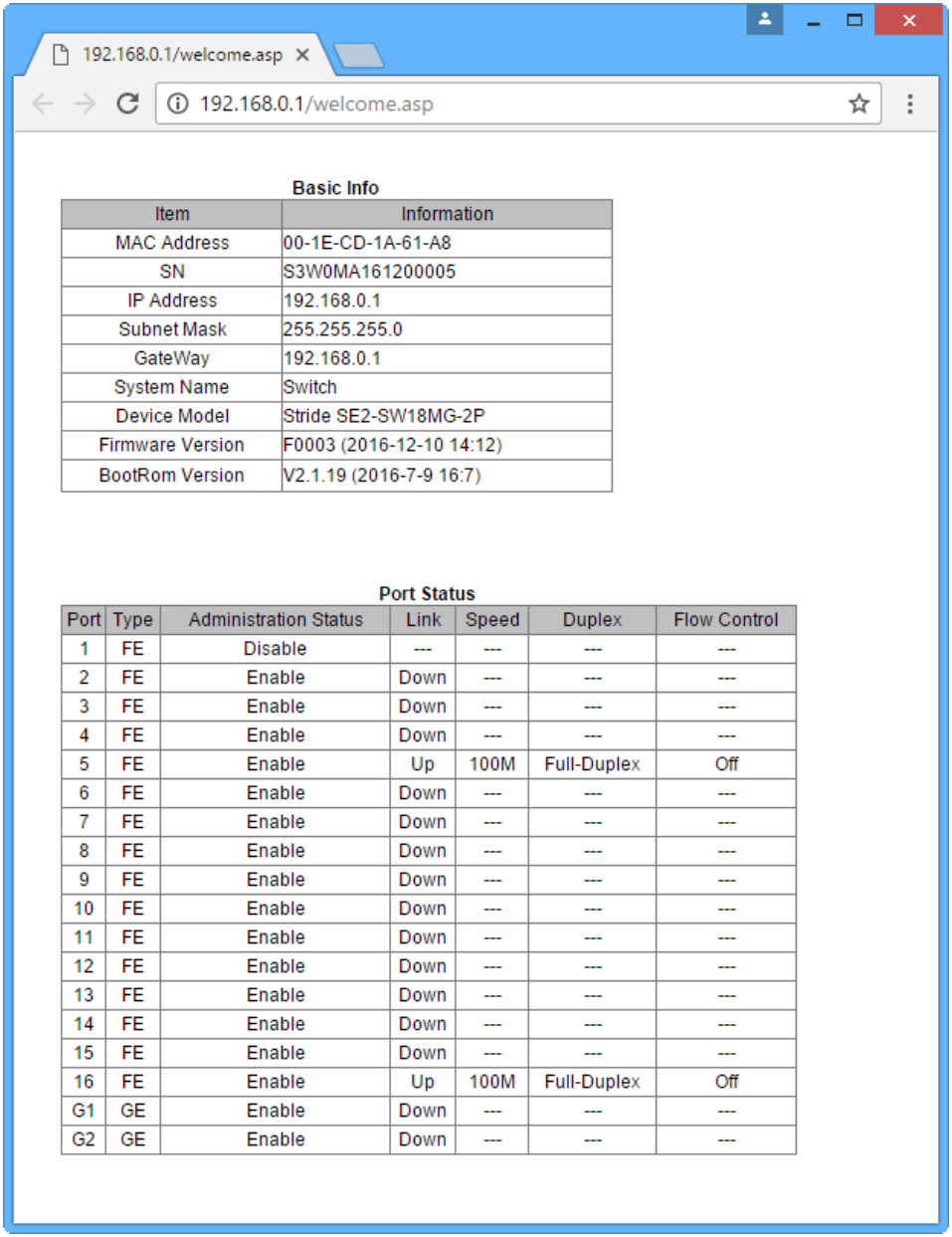
5. In your browser (we use Google Chrome for this example) type 192.168.0.1 (the switch's IP address) in the address field and Enter.



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

This screen will appear.



Basic Info

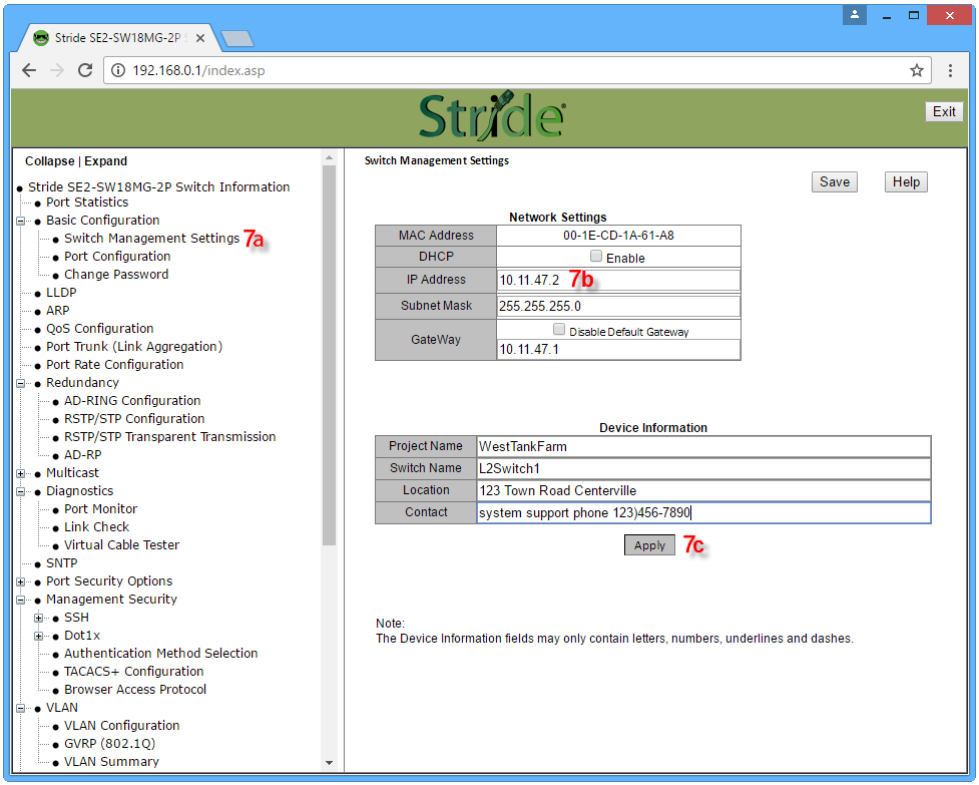
Item	Information
MAC Address	00-1E-CD-1A-61-A8
SN	S3W0MA161200005
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
GateWay	192.168.0.1
System Name	Switch
Device Model	Stride SE2-SW18MG-2P
Firmware Version	F0003 (2016-12-10 14:12)
BootRom Version	V2.1.19 (2016-7-9 16:7)

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).



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.