WHITE PAPER

Why You Might (or Might Not) Need an Industrial Managed Ethernet Switch

Explore the reasons and applications where a managed switch should be used and when an unmanaged switch is sufficient.

By Jonathan Griffith
Product Manager, Industrial Communications & Power Supplies, AutomationDirect

AUTOMATIONDIRECT.com
The #1 Value in Automation.™

Many industrial engineers and IT staff understand the need for industrial grade networking equipment. AutomationDirect has provided resources on that **here**. What might not be as obvious is when to choose a managed Ethernet switch. The price differential between an unmanaged and managed switch is significant and can impact the overall system budget. In this white paper, we explore the reasons and applications where a managed switch should be used and when an unmanaged switch is sufficient.

Why might you need a Managed Switch?

1. Enhanced traffic filtering:

Although an unmanaged switch will filter out many packets from an end device, there are still many types of packets that an unmanaged switch cannot determine what to do with and must forward on to all devices on its 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 is a logical way to separate networks in ways that previously required physical separation. In many cases it is difficult to physically separate networks, but managed switches offer VLANs that simplify the setup and achieve the required separation for these situations.

- **Traffic Priority (QoS, Quality of Service):** Some traffic may be more important to a specific device than other traffic. Using the Quality of Service feature, the Stride managed switch can apply tags to a packet coming into the switch to give that packet a higher priority going to another switch. The last switch will then remove the tag before sending the packet to the device. It can also use the tags applied to the packets by the devices themselves if they support this.

2. 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. A Stride SE-series managed switch can also give you visibility in to the type of packets that are being sent across the switch by viewing the Network Statistics page in the configuration.

- **Port Monitoring:** 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 that port and use Ethernet sniffing software (such as Wireshark) to see the data being sent back and forth.

- **Network Statistics:** By looking at what kind of packets come in and out of the switch, you can determine what action needs to be taken to make your network more efficient. If you see a lot of Multicast traffic, utilize the IGMP Filtering feature (mentioned previously). If there are lots of broken packets, troubleshoot the wiring to determine where the problem lies using the virtual cable test in the switch.

3. Redundancy:

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 to prevent unnecessary down time. So why not just physically connect unmanaged 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.

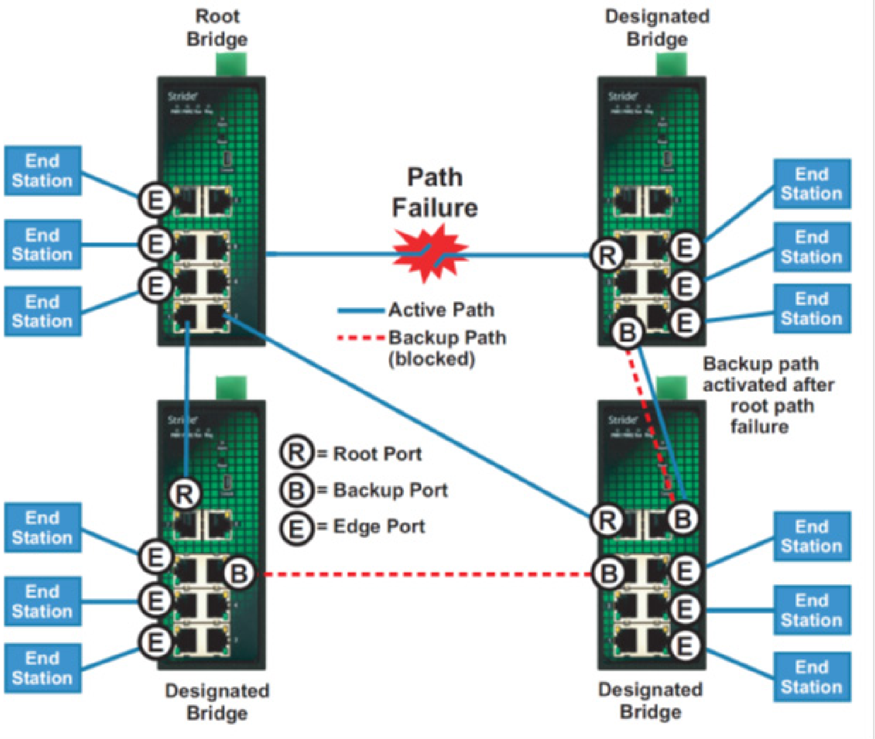
In an unmanaged Ethernet network there can be only one path between any two ports on the network. If there is more than one path from one unmanaged switch to another, a broadcast message (and in some cases other messages) sent by the network will be forwarded and will complete a loop once it returns on the second path. Since unmanaged 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 with unmanaged switches.

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 so that managed switches can communicate with each other to discover and prevent loops.

- **RSTP:** Rapid Spanning Tree Protocol is currently the preferred method to purposely create a ring that allows multiple, redundant paths on the network. This feature allows managed switches to intelligently decide one path when the network comes up and assign alternate paths if some part of the original path goes down. The manner in which it decides the original paths and the time in which it changes to alternate paths is much, much faster than when using 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 typically enabled by default.

- **AD- Ring:** In many control systems, the time it takes for the RSTP algorithm to change paths upon some network failure is too slow. The AD-Ring is proprietary to the Stride SE2-series managed switches, and performs the same function as the RSTP but it has the advantage of changing paths very quickly.

In the diagram below you can see the advantages of a managed switch network implementation. The root bridge is connected to three designated bridges and each designated bridge is connected to each other. This creates a redundant network which would bring down an unmanaged network. Using RSTP or another proprietary redundancy protocol, the switches temporarily block the backup paths so the loops do not interfere with the network. When the active path between the root bridge and a designated bridge is disconnected the associated backup path is activated so that no switch is removed from the network. In an unmanaged network, the path failure would have removed that switch from the network leaving all of the end stations on that switch unable to communicate.



4. Security:

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

Some security features protect access to switch management and provide a level of protection from the switch being accidentally or maliciously reconfigured. Other security features provide a level of protection for the traffic on your network as it moves across the switch.

- **Port Control:** In the "Port Settings" 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.

- **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.

- **Browser Security:** 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.

5. Better Network 'Awareness':

The ability to know when and what is wrong on your network is a powerful 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 TCP:** If you have a controlling device on the network that has Modbus TCP or UDP client capability, several diagnostic tags that can be read from the switch to indicate the health of the network and certain configuration tags may be written into the switch. Stride SE-series managed switches allow the ability to read switch parameters using Modbus TCP while Stride SE2-series managed switches allow full switch management capability using Modbus TCP.

- **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. SE2-series managed switches have full switch management capability using EtherNet/IP.

- **SNMP:** SNMP stands for Simple Network Management Protocol and is used for just that. There are many software tools out there that can query or receive 'traps' sent by the Stride managed switch to ascertain events or health of the switch. Traps are simply alert notifications sent by the switch to the SNMP manager.

- **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 managed switch keeps a table of the MAC IDs of devices that are communicating across it.

When to stick with an Unmanaged Switch

Unmanaged switches are the most commonly used for simple networks which don't require the additional managed features we've discussed above (redundancy, traffic filtering, or troubleshooting). They are most effective when connecting four to five switches together with low priority networking. They cost much less than managed switches, starting around $75 for a 5 port unmanaged industrial switch (SE2-SW5U). Most industrial Ethernet switches have five to sixteen ports in DIN rail mount models. Gigabit and fiber options are normally available and provide higher bandwidth or greater distance, respectively. In addition to greater distances, fiber provides noise immunity which is particularly important in electrically noisy industrial environments. So if your networking needs are simple and/or your budget is a concern, then sticking with an unmanaged Ethernet switch may be the way to go. The table below highlights some of the main differences between managed and unmanaged Ethernet switches.

Attribute	Unmanaged Switch	Managed Switch
Cost	Starting ~$75	Starting ~$429
Ease of Use	✓	✓
Network Speed	✓	✓
Fiber Compatible	✓	✓
Redundancy	--	✓
Network Management	--	✓
Industrial Protocol Management (Modbus TCP, EtherNet/IP)	--	✓
Enhanced Traffic Filtering	--	✓
Port Monitoring	--	✓

Table: Industrial Ethernet Switches - Unmanaged vs. Managed Comparison