WHEN TO USE MANAGED SWITCHES IN AN INDUSTRIAL NETWORK

Managed vs. Unmanaged Ethernet Switches
The use of Ethernet on factory floors and in industrial applications to create, access and remotely monitor data is rapidly growing. As Ethernet reaches the factory floor, choosing the right infrastructure—including the right switch for the right application—is imperative to maximize the performance of an entire system. At the highest level, this decision begins with the selection of managed vs. unmanaged Ethernet switches.

Unmanaged Switches
Unmanaged switches allow Ethernet devices to communicate with one another by providing a connection to the network. Unmanaged switches are plug and play devices, meaning you only have to plug them in for them to work. Simple installation and operation come with a significant opportunity cost. The fixed configuration of unmanaged Ethernet switches limits the functionality of a network to that of the Ethernet devices connected.

Managed Switches
Managed switches offer all of the functionality of an unmanaged switch out of the box, but they also offer a suite of other features that make it possible to manage and troubleshoot your network remotely and securely. These switches allow engineers to reach optimal network performance in a reliable and repeatable fashion.

Simple Network Management Protocol
Managed switches use a protocol called Simple Network Management Protocol (SNMP) to relay network configuration data to network engineers and allow them to set configuration parameters remotely. This allows network management and optimization functions to be performed from a central or remote location. Some software programs improve on the benefits of SNMP to make network management and visualization easier and more straightforward, which reduces troubleshooting time and increases uptime.

Network Management Software Example

Source: Hirshmann, A Belden Brand

Prioritization of Data
Managed Ethernet switches have a number of tools that are capable of setting and recognizing differing priorities in the Ethernet data being handled. Critical and time-sensitive data, such as control system devices or voice over IP (VOIP) network traffic, can be given higher network priority through either quality of service (QoS) designation or virtual local area network (VLAN) segmentation. These tools deliver important messages to reduce control network latency or make VOIP calls smooth and clear. There are more advanced timing technologies available such as IEEE 1588 that allow more deterministic transfer of data.
WHEN TO USE MANAGED SWITCHES IN AN INDUSTRIAL NETWORK

Multicast Traffic Support
Managed Ethernet switches allow users to manage the routing of multicast packets, a capability that can drastically improve network performance by reducing unnecessary traffic. Managed Ethernet switches do so by using a feature called Internet Group Management Protocol (IGMP) that makes sure multicast traffic reaches its intended destination(s) while not flooding that traffic onto the rest of the network. Unmanaged switches do not support IGMP and treat multicast traffic in the same fashion as Ethernet broadcast traffic, forwarding to all ports. This can overwhelm a network when uncontrolled and lead to devastating broadcast storms. The management of multicast Ethernet traffic is a particularly important feature on industrial networks as a prevalent industrial Ethernet protocol, the Allen-Bradley® EtherNet/IP™ protocol, relies heavily on multicast traffic. By extension, many industrial Ethernet devices rely on multicast traffic and can be overcome by mishandling it.

Redundancy
When selecting an Ethernet switch for the factory floor it is important to remember that industrial sites are particularly harsh and uptime is extremely important in these critical systems. If a link or device fails on the network, it is imperative that the remainder of the network remains functional. Managed Ethernet switches have many options for redundancy, allowing for maximum network functionality even in the worst conditions. The two most common redundant configurations are Rapid Spanning Tree Protocol (RSTP) and ring topologies. RSTP is extremely flexible and is fairly simple to implement, while still allowing the network to repair itself if a network connection point fails. If quicker recovery time is needed, then ring style topographies can be implemented and allow for recovery times in a sub-30 ms window. Finally, parallel network options exist that allow for seamless redundancy (0 ms) for the most critical of applications.

Topology of Parallel Redundancy Protocol

Conclusion
All of the features of managed switches do come at additional costs, so it is important to know when to select a hardened managed switch or when an unmanaged switch can be used. Unmanaged switches are mostly used to connect edge devices on network spurs, or on a small stand-alone network with only a few components. Managed switches should be used on any network backbone switch so that segments of network traffic can be monitored and controlled. Additionally, any device that would be considered critical to your network should be connected via a managed switch so its health can be monitored and secured and so redundancy can be implemented to increase uptime and reliability. Finally, switches being implemented in an Ethernet IP network should be managed, because Ethernet IP extensively uses multicast traffic that can overwhelm networks if it is not managed properly.

For more information, contact your local Anixter representative at 1.800.ANIXTER or visit anixter.com.