Do I Need a Managed Switch?

As the trend to implement Ethernet on the factory floor and into control networks continues to grow, more and more is being said about managed switches. The simple question of "Do I need a managed switch?" can be given the simple answer of "Maybe - Maybe not." This article will provide a brief overview of the differences between managed and unmanaged switches and give some examples of situations where a managed switch should be a consideration.

Managed vs. Unmanaged Switches

Unmanaged switches have traditionally provided the backbone for basic network connectivity. Unmanaged switches are available with features such as redundant power inputs, extended operating temperature, reduced noise susceptibility, and other hardware features that can be crucial to industrial networks.

Many control networks have specific needs such as; deterministic or real time communications. Managed switches provide additional built-in protocols and software tools that can increase determinism, and provide optimized constant and consistent data flow. If a business network is down for ten minutes during which time users cannot get e-mail, it's merely an inconvenience. If certain industrial networks are down for ten minutes, the results could be costly or even catastrophic. Some applications such as motion control often demand response times of a few milliseconds or less. In order to achieve consistent communications times and deterministic communications it's often necessary to implement a managed network.

Managed Network Components

Managed switches allow us to take control of communications over an Ethernet network. There are three types of control: Bandwidth Control, Data Control, and Traffic Control. Depending upon the type and number of devices on a network, one, two or all of the above can be applied.

Bandwidth Control can be achieved by using the IGMP Snooping Protocol and tools such as Rate Limiting and Port Trunking. IGMP Snooping allows intelligent routing of Multicast traffic. There are three types of transmissions over an IP network - Broadcast, Unicast, and

Multicast. Broadcast traffic is data that is sent out to all devices on the network. Unicast messages are messages intended for one device, whereas multicast messages are packets sent to a predefined group of devices. Routers are aware of multicast messages being passed to and from the internet or separate networks making multicast messaging more efficient than Unicast messaging. However, LANs are not aware of multicast traffic unless the IGMP snooping protocol is implemented. Without IGMP snooping, these messages become broadcast messages which can decrease network performances, or possibly bring down the network altogether. Since Multicast messaging is more efficient, many popular industrial protocols such as Ethernet/IP use it for real time or near real time communications. Rate limiting insures that a malfunctioning or misconfigured device does not use more than a predetermined amount of bandwidth for sending or receiving which could degrade network performance. Port Trunking expands the bandwidth between managed switches by aggregating multiple ports.

Data control refers to guaranteeing that the most important data is delivered first, and not affected by other traffic on the network. Most managed switches offer Quality of Service (QoS), which provides the ability to prioritize network traffic. QoS increases determinism by insuring that high-priority traffic is passed through first. For example, frames to and from a motion controller would be processed before traffic to and from an e-mail server. Manufacturers with devices that use the Profinet protocol highly recommend the use of QoS with their products.

Traffic Control can be accomplished by implementing Virtual Local Area Networks (VLANs). VLAN configuration allows a switch to logically group devices and to isolate traffic between these groups even if all the devices share a common physical media. For example, if the switch was being used for both office communications and factory communications, two VLANs could be created to isolate the office traffic from the factory traffic. Some switches also allow devices to be located on multiple VLANs. This is sometimes called overlapping VLANs. If one device, a SCADA system for example, needs to communicate with both the office and the factory, then this device would exist in both the office VLAN and the factory VLAN. This would isolate traffic between the remaining office and factory devices, but allow the SCADA system to communicate on both networks.

Another important feature of a managed switch is Network Redundancy. Redundancy institutes a "back-up plan", and reduces or eliminates potential downtime. Managed switches can provide protocols such as the Rapid Spanning Tree Protocol (RSTP). RSTP allows for alternate cabling paths while preventing loop situations that can cause a network to stop functioning.

The above-mentioned features are just a sample of common tools and protocols found in most managed switches. There are other features that may be available depending upon the particular switch being used.

With or Without Managed Switches

Now, back to the question of "Do I need a managed switch?" There are only two disadvantage of using a managed switch. The first one is that they are physically larger. This can be a consideration when control panel real estate is limited. The second disadvantage is the price. Managed switches are generally two to three times the price of unmanaged switches.

So how can you tell which type of switch is the right one for your application? One method of defining the requirements of your network is to monitor it. A protocol analyzer can be employed to detect the types and amount of traffic by port or on an aggregated basis. Monitoring allows us to optimize performance by defining which of the above mentioned tools should be used and where. It also allows us to take a "snapshot" of the network for benchmark testing. A popular protocol analyzer is Wireshark which can be downloaded at no charge (www.wireshark.org). Most managed switches also provide built in traffic monitoring capabilities.

Another helpful source in defining your network's requirements is to ask the device manufacturer. There is no manufacturer who can specifically quantify how much traffic will be generated by their devices in every situation. They can, however, tell you what type of traffic will be used and make recommendations as to what protocols and features, if any, will increase network performance.

So what does this all tell us? It tells us, "*maybe* you need a managed switch". It seems absurd that in this high-tech world where networking is a precise science that someone might suggest good old fashioned trial and error when it comes to designing an industrial network. The truth is that you can listen to your hardware vendors, you can do all of the research you possibly can, you can perform calculations, and you can hire consultants, but until you actually have a real world functional test, the rest is meaningless. Consultants and manufacturers have the tendency to suggest a "safe" solution, and since the additional cost is not coming from their pocket, why not recommend managed switches? Most network hardware vendors will offer "consignment" terms, or a free trial period which will give you an opportunity to get live results as to whether a managed switch is truly necessary.

In conclusion, chances are an unmanaged switch will work just fine for a small or isolated control network. Managed switches offer several methods of communications control and should be considered for mixed networks where the control network shares a common infrastructure, as well as, high traffic networks, devices that use multicast messaging, mission critical data, and real-time communications. If you are not sure what the demands of your application actually are, I recommend monitoring and benchmark testing in your real world environment.

For further information on any of the above, or to discuss your own networking issues with our network engineering team, email us at info@msitec.com or call (866) 397-7388.

