

Ethernet is Moving out of the Office into Harsh Industrial Environments.

Ethernet is an ideal medium to transport large volumes of data, at speed, across great distances. Previously, multiple networks carrying specific protocols were installed side by side to carry out unique tasks. This inevitably led to project costs increasing as additional fiber optic or copper cables were installed to deal with the increasing volume of data. Using Ethernet a single fiber optic cable can carry multiple protocols. Furthermore, manufacturers are exporting their legacy protocols onto Ethernet, designing new IP based communication protocols and providing embedded Web-Pages within devices that offer real-time information using simple tools like Internet Explorer and Netscape Navigator.

Unfortunately, although network hardware has dramatically increased in speed and technology over the past decade the poor perception of Ethernet has remained; namely as being difficult to fault-find and critically being a non-deterministic network. A key development that overcame some of these issues was the advent of the Ethernet Switch.

Early Ethernet networks were based on a hub or repeater. These units have no intelligence and therefore are unable to identify any information contained within the Header frame of an Ethernet packet. This means that it is not capable of determining which port to send the frame to. Therefore, every frame is sent to every port. A network of repeaters and hubs is called a 'Shared Ethernet' or 'Collision Domain'. Various devices will all compete with each other before sending data using 'Carrier Sense Multiple Access / Collision Detect' (CSMA/CD) protocol. This means that only one system is allowed to proceed with a transmission of a frame within a Collision Domain at any one time. This is a major disadvantage when using Hubs and Repeaters within a network.

A switch, like a hub, has to forward and receive packets from one network or device to another. The switch could forward all packets, but if this was the case it would have similar behavior to a hub. It would be more intelligent if the switch only forwarded packets which needed to travel from one network or device to another. To do this, the switch must learn which devices or networks are connected to each port. In simplistic terms; it needs to learn the destination and source ports of each and every packet received on each individual Switch port. Once learnt, any identically addressed packet will be automatically be forwarded. With today's enhanced processing power the introduction of a Switch has significantly increase network bandwidth.

Industrial Ethernet – What Are The Differences?

Industrial rated Switches are intended to be installed in both harsh climatic environments and noisy electrical installations. Such Switches are an excellent example of true industrial design principles – very high operating temperatures (down to -40°C), very low power consumption, dual input power supplies and wide DC operating voltages. In Roadside and tunnel applications distances between cabinets with a suitable power supply can be challenging. Naturally, fiber optic cable is the preferred solution. Using single mode fiber, runs of up to 52 miles (85 km) are possible. Even using standard CAT5e copper cable the Industrial Switch supports the long cable specification and distances of up to 607 ft (185 m) are viable.

However, the domain of Ethernet has always been controlled by the IT department who normally configured office networks with an iron fist and dictated to the organisation how the network would be designed. Complex network recovery protocols like spanning tree, and SNMP to help with fault finding and system analysis were often employed to enhance network resilience. If a network failure occurred the IT department would casually look at repairing the equipment; there was no real rush as it was an office network.

However, with industrial Ethernet you need very fast repair time and with an IT department not readily available on the roadside, maintenance personnel need to be made aware of the fault, find the error and repair it - quickly. To aid this, unique network recovery features are employed to significantly enhance network recovery times.

When an IT department requires a level of redundancy a common method is to employ the spanning tree protocol. However, spanning tree can be complex to program and critically can take over 30 seconds to detect and recover from the fault – far to long for critical applications!

Industrial Switches incorporate propriety protocols that enable up to 200 Switches to be placed into a redundant ring. A single Switch, configured as the network focal point will monitor, detect and recover from a fiber or copper link failure within approximately 30mS – for the majority of applications a seamless process. The configuration process of the network focal point is simple as it must be remembered that as the switches are to be installed on the roadside the first to be called to rectify a fault will more than likely be Maintenance personnel.

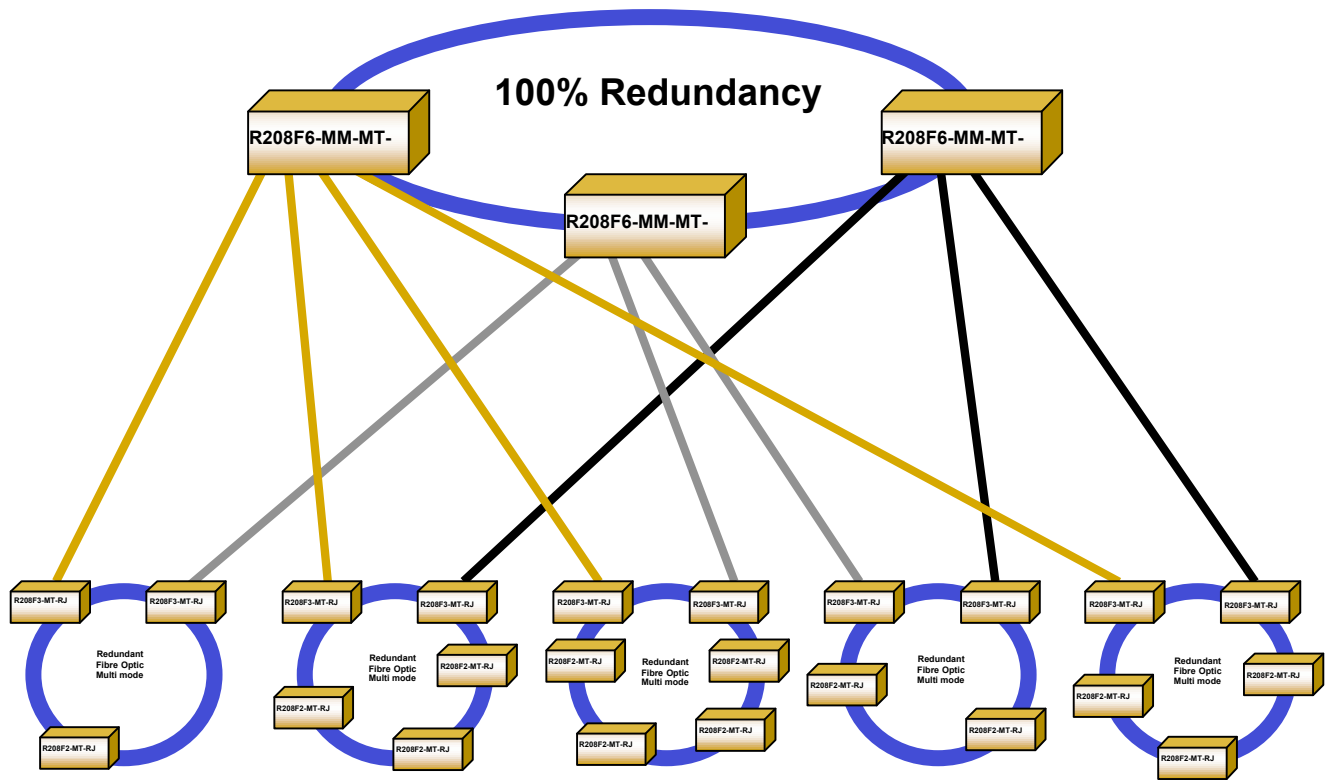


It is likely that these people will not be fully trained on Ethernet and the protocols that are in operation, nor will they fully understand the principles of SNMP etc. However, with a fault contact, fault LED's and graphical interface implemented with SNMP they have a multi-level approach to fault finding:

The fault contact is hard-wired to an alarm on a control panel or as an input to a DCS. If a link failure occurs (between two switches or an Ethernet Device) or a network failure occurs the fault contact on the Switches will be energized. The Maintenance Engineer can easily locate the fault.

In addition if the fault is due to a bandwidth deficiency, the IT Manager can pro-actively monitor specific ports and prevent such problems occurring using SNMP (Simple Network Management Protocol). SNMP is an ideal tool for monitoring a network. Firstly, a PC configured as an SNMP client can poll Switches to gain information on overall network loading, individual port status and running temperature information. Secondly, Switches can be configured to issue 'traps' to the client PC when a particular event occurs. The main benefit of using SNMP is that all of the unique Switch or total network information can be graphically represented on SCADA.

With the increased use of Ethernet in the field to pass critical data the greater the reliability in network infrastructure. Where multiple rings are configured in a system it is also critical that the links between the rings are also duplicated to provide enhanced redundancy. This can be achieved using Multi-ring Redundancy



Ethernet in Tunnels

In a tunnel application, the use of Ethernet can simplify and enhance the communications process. It is slowly becoming common-place to pass data controlling ventilation, lighting and traffic signage over Ethernet. If video surveillance is also required then why not pass images over the same network? A common fallacy of placing video over Ethernet is the perception that the large volume of data required and the way in which data is transmitted will swamp an Ethernet network.



The I/O cabinet also includes an Ethernet Switch. This is located in the cabinet below the red signal light

Video over IP

If the Ethernet Switch supports multicast filtering and IGMP (Internet Group Management Protocol) network traffic can be significantly reduced with no effect the total network performance. Multicasting allows one device on the network to send data to multiple IP devices that have identified themselves as interested in receiving the originating devices content. Multicasting was originally used for such applications such as updating the address books of mobile computers and sending out company newsletters to a distribution list. Recently, multicast has been used in applications where "broadcasting" of high-bandwidth programs like streaming media (video) to an audience that has "tuned in" by setting up a multicast group membership has become commonplace. Where IGMP is also present on a Switch it further enhances the network by allowing devices to exhibit their intent in joining and leaving multicast groups. If video codec's support multicast it allows high quality video to be passed over Ethernet with significantly reduced network utilisation. Whereas before the video would be passed to all devices on the network regardless of their interest in the image, today an Ethernet Switch supporting IGMP / multicast filtering will only allow devices that have a requested interest in video will receive the data.

Prioritising Network Data

Within a tunnel application the priority of the control data over video data is emphasised if an incident occurred in the tunnel; would the control of tunnel ventilation shafts, emergency fume extraction and lighting have a higher priority over tunnel closure of traffic diversion signage? The Industrial Switches incorporate packet prioritisation that enables users to place data into eight different levels of priority. Therefore, tunnel closure control could have a higher priority than that of fume extract with all control data having total priority over video images. Where the ability of packet prioritisation really comes into fruition is with head of line blocking prevention. If a network port becomes particularly congested un-prioritised data would be placed into the port buffer. However, if a high priority message is received at the port this packet would jump the queue. Therefore, network determinism is further enhanced.

Conclusion

Ethernet now is the perfect medium for use in roadside and tunnel applications. A fast, reliable Ethernet network enables multiple control protocols along with Video images to be passed over great distances. Furthermore, panel heating and UPS specification can be downsized due to the wide operating temperature and low power consumption. However, with all the control data and video images being passed over a single network the consequences of a fiber failure could be catastrophic. However, with a near seamless redundant ring recovery process of 30mS the option of using industrial Ethernet in such harsh environments seems highly viable.

For additional information on the R208W Ethernet Switch, and other Fiber Optic Converters for serial data interfaces and bus systems contact Weed Instrument at:

Toll Free: 800-880-9333 (U.S. only)
Phone: (512)434.2850
Fax: (512)434.2851
Email: fibersales@weedinstrument.com