The ABCs of EtherNet/IP Switches

EtherNet/IP end devices such as PLCs, remote I/Os and OIs can create high levels of multicast traffic. These high levels of multicast messages can inundate end devices which do not expect this level of traffic, causing these devices to operate abnormally. Since EtherNet/IP is a control network, it is sensitive to issues that may not be experienced by office-type networks. As a result, EtherNet/IP networks require specific switch features in order to function without failure. Contemporary Controls managed switches (the EISX_M, the EICP_M, and the EISB_M) provide all the following required and recommended features — and other features which can be employed to achieve optimum network performance.

EtherNet/IP Required Features:

- IGMP snooping (one switch/router requires IGMP query)
- Full-duplex switching
- Port mirroring

EtherNet/IP Recommended Features:

- IGMP query
- Auto-negotiated/manually configurable port settings
- VLAN
- SNMP
- Wire-speed switching

Full-Duplex Switching

Full-duplex switching eliminates collisions occurring on half-duplex networks. At the level of messaging produced by EtherNet/IP devices, it is imperative to eliminate potential collisions so that the deterministic qualities of EtherNet/IP can be retained.

IGMP Snooping

Since EtherNet/IP devices can create a high level of multicast traffic, it is important to limit which end devices receive this traffic. The reason is that a high level of multicast traffic can overwhelm an end device and make it operate improperly. A switch incorporating IGMP snooping can forward received multicasts to only those devices which requested this traffic. When a switch designed without this feature receives multicast messages, it floods these message to all ports and overwhelms the end devices. IGMP snooping restricts multicast messages to only end devices that have requested to receive this traffic and are designed to handle this level of traffic. This is important in EtherNet/IP networks.

When an EtherNet/IP device wants to consume produced data, it will transmit an IGMP join message. These join messages are received by all IGMP snooping switches. When this produced multicast data is transmitted, the switch will use the information it learned from the join messages to determine which ports will receive the produced multicast data. This will restrict the produced multicast data to only those ports and end devices that expect this traffic — allowing the end devices to operate normally.

For IGMP snooping to work properly, one or more switches or routers in the network must provide IGMP query support. The IGMP querier will periodically ask each end device in the network which multicasts they wish to receive, refreshing the IGMP snooping multicast/port associations. If no switch or router is present that supports IGMP query, the IGMP snooping switches will eventually forget all the multicast/port associations learned and all received multicasts will be flooded to all end devices. This can cause end devices to operate abnormally. Essentially, the IGMP snooping process will fail without the support of an IGMP querier. All Contemporary Controls managed switches can act as IGMP queriers.

Port Mirroring

Many network problems are diagnosed and solved by capturing all network traffic between end devices. To capture all traffic between end devices on a switched network, the switch must support *port mirroring*. Port mirroring copies all traffic from one or multiple ports to one mirror port. This mirror port can be connected to a computer running a protocol analyzer or to a network capture tool. Without port mirroring, it would be very difficult to troubleshoot problems on the EtherNet/IP network.

IGMP Query Support

This feature is required on one switch or router in the EtherNet/IP network. *IGMP query* also supports multiple IGMP queriers. The IGMP querier with the lowest IP address will act as the network querier. If this device fails, the device with the next lowest IP address will take over. As IGMP query is critical to IGMP snooping, it is recommended that multiple switches in the EtherNet/IP network have this ability.

VLAN

A VLAN (Virtual LAN) can be used to isolate groups of devices, keeping all traffic of one group from reaching another. This is viewed as one more method to keep multicast traffic produced by EtherNet/IP devices from overwhelming end devices. In addition, as EtherNet/IP is a control network, it cannot survive network issues commonly experienced by IT networks. Most IT networks will not notice large losses in bandwidth for a short time due to broadcast storms, STP loops, improperly operating equipment, etc. A VLAN can be used to connect the IT network to the EtherNet/IP network but isolate it from IT network issues. The common VLAN disadvantage is that once VLANs are used, end devices in different VLANs are 100% isolated from each other. A router must be employed if an end device in one VLAN group needs to communicate with devices in another VLAN group. One solution to this problem is a feature called *overlapped VLANs*. These VLANs allow an end device to exist in multiple VLANs. Contemporary Controls managed switches support overlapped VLANs.

Auto-negotiated/Manually Configurable Port Settings

Usually, switches and end devices auto-negotiate the best communication settings when talking together. This includes the data rate (10 Mbps or 100 Mbps) and duplex (half- or full-). For example, if a switch is connected to an end device which supports 10 Mbps or 100 Mbps and half- or full-duplex communications, the two devices will auto-negotiate a communication setting of 100 Mbps full-duplex. However, not all end devices fully support auto-negotiation. If an end device has been configured to use a specific data rate or duplex, it may not support auto-negotiation and this may confuse the switch as it tries to auto-negotiate communication settings. The switch and the end device may end up using different communication settings. If one side employs half-duplex, and the other side uses full-duplex, this will create many collisions and a large loss in bandwidth. If one side chooses 10 Mbps and the other uses 100 Mbps, there will be no communications between these two devices. Manually configurable port settings on the switch permit the user to control data rate and duplex which can help when auto-negotiation problems occur.

Wire-speed switching indicates the ability of the switch to handle 100% loading on each port without dropping messages. Although most switches have this capability, one should ask their switch supplier if these products are designed with wire-speed switching. Due to the high level of traffic from EtherNet/IP devices, it is important that all switches support this feature.

SNMP

SNMP (Simple Network Management Protocol) provides the ability to view the network statistics as seen by the switch. Network statistics can include the link status of each port, the number of messages received/transmitted on each port, the number of errors on each port and much more. Because SNMP is a standard supported by most managed switches, a single application can be can be used to view the network statistics from all switches, even if these switches are from different manufacturers. Also, there are many SNMP to OPC servers available which can share this data with OI and HMI systems.

For more information on the Contemporary Controls EtherNet/IP managed switches which support all of the EtherNet/IP required and recommended features, see *www.ccontrols.com/EIP.htm*.

REFERENCES

EtherNet/IP, Switches and Multicast Frames (Rockwell Automation Application Note)

http://domino.automation.rockwell.com/applications/kb/RAKB.nsf/0/84379FB8AFD936FC85256CEF005586D0