Utilization of Modern Switching Technology in EtherNet/IP™ Networks

Anatoly Moldovansky
Rockwell Automation
1 Allen-Bradley Drive
Cleveland, Ohio 44124 USA
amoldovansky@ra.rockwell.com

Abstract

EtherNet/IP networks are widely used in industrial environments and time-critical applications. In this paper, we characterize traffic generated in a typical EtherNet/IP network and compare it with office network traffic. We provide recommendations regarding features of network switching and routing devices, which, when properly utilized, will help to achieve required performance of EtherNet/IP sub-nets and allow for their successful integration into a plant network. We also provide a list of issues that have been uncovered during these studies.

1. Introduction

Ethernet™ networks have been successfully used on the factory floor for the past 15 years, mainly in non time-critical applications. Evolution of the Ethernet[1] technology from a 10Mbps, half-duplex, bus/tree topology into a 100Mbps and 1Gbps, full duplex, switch/router based hierarchical star topology has created an opportunity for utilizing Ethernet in industrial networks supporting time-critical applications.

Ethernet/Industrial Protocol (EtherNet/IP) is a communication system suitable for use in industrial environments and time-critical applications [1]. It utilizes standard Ethernet and TCP/IP technologies and an open Application layer protocol called Control and Information Protocol (CIP). CIP is also used in ControlNet™ and DeviceNet™ networks. In EtherNet/IP networks, exchange of time-critical data is based on the producer/consumer model where a transmitting device (host or end-node) produces data on the network and many receiving devices can consume the data simultaneously. Implementation of the producer/consumer data exchange is based on the IP (Internet Protocol) multicast service mapped over the Ethernet multicast service.

EtherNet/IP supported functions include:

- Time-Critical data exchange
- Human-Machine Interface (HMI)
- Device configuration and programming
- Remote access to web pages embedded in EtherNet/IP devices
- Device and network diagnostics

2. EtherNet/IP Traffic Profile

In order to identify features of the EtherNet/IP network infrastructure helping to provide required performance and connectivity, it is necessary to characterize its traffic. Within the scope of this paper, EtherNet/IP network infrastructure is defined as a hierarchical interconnection of Layer 2 and Layer 3 Ethernet switches.

Traffic generated during programming, configuration, and diagnostics of EtherNet/IP devices as well as during exchange of non time-critical is normally low-rate traffic that, obviously, has insignificant impact on network performance. Although it contains all three major types, broadcast, unicast, and multicast, this traffic does not require engagement of any special features in the EtherNet/IP network infrastructure.

Broadcast and multicast traffic typically consists of IP packets supporting ARP, BOOTP, DHCP, DNS, SNMP, IGMP and other protocols of this type. Unicast traffic consists of TCP/IP packets.

Traffic generated during time-critical data exchange consists, predominately, of UDP/IP unicast and multicast packets.

Examples include:

- Input/Output (I/O) data and status produced by a remote I/O device for consumption by one or more programmable controllers
- Data produced by a programmable controller for consumption by one or more programmable controllers

[1] More accurately, IEEE Std 802.1™ and IEEE Std 802.3™ technologies.

While EtherNet/IP supports change-of-state reporting, in a typical control system data exchange is predominately cyclic. The time-critical traffic is normally generated at rate of tens of thousands of packets per second, depending on number and type of Ethernet/IP devices and the application. Some EtherNet/IP devices are, for example, capable of generating up to 5,000 packets per seconds. Normally, this traffic is evenly divided between UDP/IP unicast and multicast packets. Packet length is typically less than 100 bytes.

While handling of the UDP/IP unicast traffic does not require engagement of any special features in the EtherNet/IP network infrastructure, handling of the UDP/IP, or IP, multicast traffic does require such engagement.

As it has been already mentioned, IP multicast traffic generated in an EtherNet/IP network is a high-rate, short-packet traffic generated on a continuous basis. For this reason, EtherNet/IP networks differ considerably from typical office networks, where IP multicast traffic is generated sporadically and with much lower packet rates. A growing exception to this traffic profile may be in the area of multimedia audio and video conferencing applications.

An Ethernet Layer 2 switch normally retransmits each received IP multicast, broadcast or unknown unicast packet to all ports. In the example shown in Figure 1, IP multicast traffic produced by remote I/O device I/O$_{11}$ for consumption by Controller 1 will be sent to all devices connected to the switch.

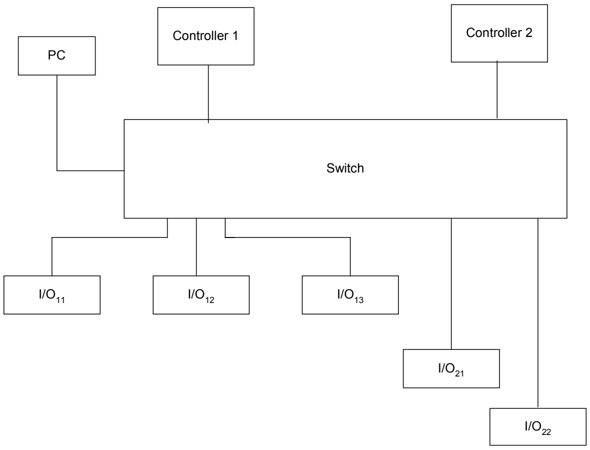

Figure1. Isolated network configured as a single VLAN

Utilization of device resources for filtering this unwanted high-rate traffic can significantly impact device and, consequently, control system performance.

When an EtherNet/IP sub-net is connected to a plant network and propagation of multicast packets through this network is not blocked, it may cause a multicast storm or a flood that will degrade the plant network performance. In an office network, a multicast flood is a temporary event that can be suppressed or controlled. In a plant network with EtherNet/IP sub-nets, the flood of multicast packets is a permanent phenomenon.

Modern Ethernet switches offer a variety of features helping to suppress, block, and route the IP multicast traffic, thus improving network performance, stability, and providing a higher level quality of service. However, not all of these features are effective in dealing with the IP multicast traffic generated in EtherNet/IP sub-nets.

3. Recommendations

In order to optimize network performance, design of the EtherNet/IP infrastructure should be based on the following objectives:

3.1 Minimize device load due to unwanted IP multicast traffic

Depending on sub-net configuration and required device connectivity, this objective can be achieved using Ethernet switches supporting virtual LANs (VLANs) or IP multicast routing.

If a switch is shared between for example, two isolated EtherNet/IP networks, then each network can be configured as a separate VLAN as it is shown in Figure 2. Here, ports 1, 3, 4, 5, and 6 belong to VLAN 1. Ports 2, 7, and 8 belong to VLAN 2. Since IP multicast packets are flooded only to devices inside each VLAN, devices will be less loaded than in the configuration shown in Figure 1.

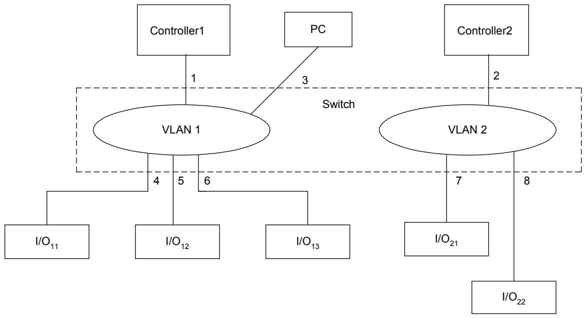

Figure 2. Isolated network configured as multiple VLANs

If EtherNet/IP devices need to share time-critical data, then they have to be connected to the same sub-net. Figure 3 depicts an example of an EtherNet/IP sub-net within a two-layer switch hierarchy. The sub-net is configured at the Layer 3 switch and consists of devices connected to three Layer 2 switches. Support of IGMP snooping in Layer 2 switches will eliminate device load due to unwanted IP multicast traffic generated in the sub-net. For example, IP multicast packets produced by controller B will be routed only to controllers A, C, and D.

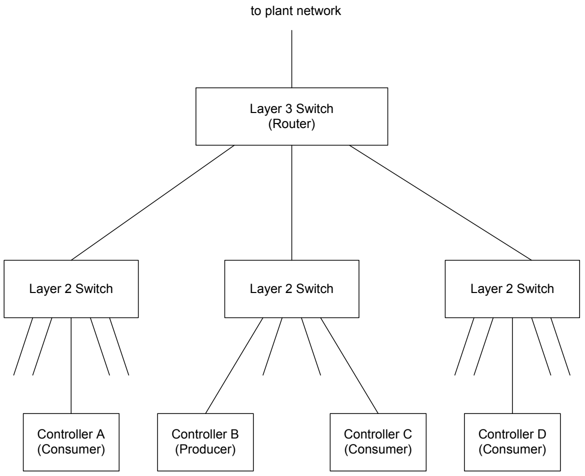

Figure 3. IP Multicast Routing Example

3.2 Minimize switch load due to unwanted IP multicast traffic

Support of IGMP snooping in Layer 2 switches in the configuration shown in Figure 3 will also eliminate switch load with the unwanted IP multicast traffic generated inside the sub-net. If, for example, IP multicast packets produced by Controller B are addressed only to Controller C and IGMP snooping is not used or not supported, then these packets will propagate through all ports of all three Layer 2 switches creating additional load on switches and end-devices.

3.3 Minimize network load due to unwanted incoming IP multicast traffic

The Layer 3 switch in Figure 3 should be configured to block the IP multicast traffic (for instance, stream video) coming from the plant network.

3.4 Block IP multicast traffic generated within the EtherNet/IP sub-net from propagation into the plant network.

This can be achieved utilizing the switch hierarchy shown in Figure 3.

3.5 Optimize switch performance

This can be achieved utilizing switches supporting the IEEE 802.1p priority queuing. In this case, more switch bandwidth can be allocated for time-critical traffic.

4. Issues

The following issues have been identified during performance and interoperability tests of EtherNet/IP networks:

- Lack of interoperability between products from different network switch vendors.
- Inconsistency of IP multicast control features (what they do and how they work) between network switch vendors and in some cases even between different classes of products produced by the same vendor.
- Lack of IP multicast control, support of the IEEE 802.3 spanning tree protocol and other appropriate features in some low-end switches, which considerably limits their use in non-isolated EtherNet/IP networks.
- Lack of industrial high-end Layer 2 and Layer 3 switches.

5. References

[1] EtherNet/IP Specification, available on www.odva.org.

6. Trademarks

EtherNet/IP is a trademark of ControlNet International and ODVA.
Ethernet is a trademark of Digital Equipment Corporation, Intel, and Xerox Corporation.
IEEE 802.1 and IEEE802.3 are trademarks of IEEE.
ControlNet is a trademark of ControlNet International, Ltd.
DeviceNet is a trademark of ODVA.