

# **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](mailto: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.

## **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 technology (more accurately IEEE Std 802.1™ and IEEE Std 802.3™ technologies) 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 this data simultaneously. Implementation of the producer/consumer data exchange is based on the Internet Protocol (IP) 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

Performance of the time-critical data exchange can be illustrated based on the following example. The currently achievable average end-to-end response time in an EtherNet/IP™ based control system with eight producers and one consumer is 7ms.

### **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 data 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 Address Resolution Protocol (ARP), Bootstrap Protocol (BOOTP), Dynamic Host Configuration Protocol (DHCP), Simple network Management Protocol (SNMP), Internet Group Management Protocol (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:

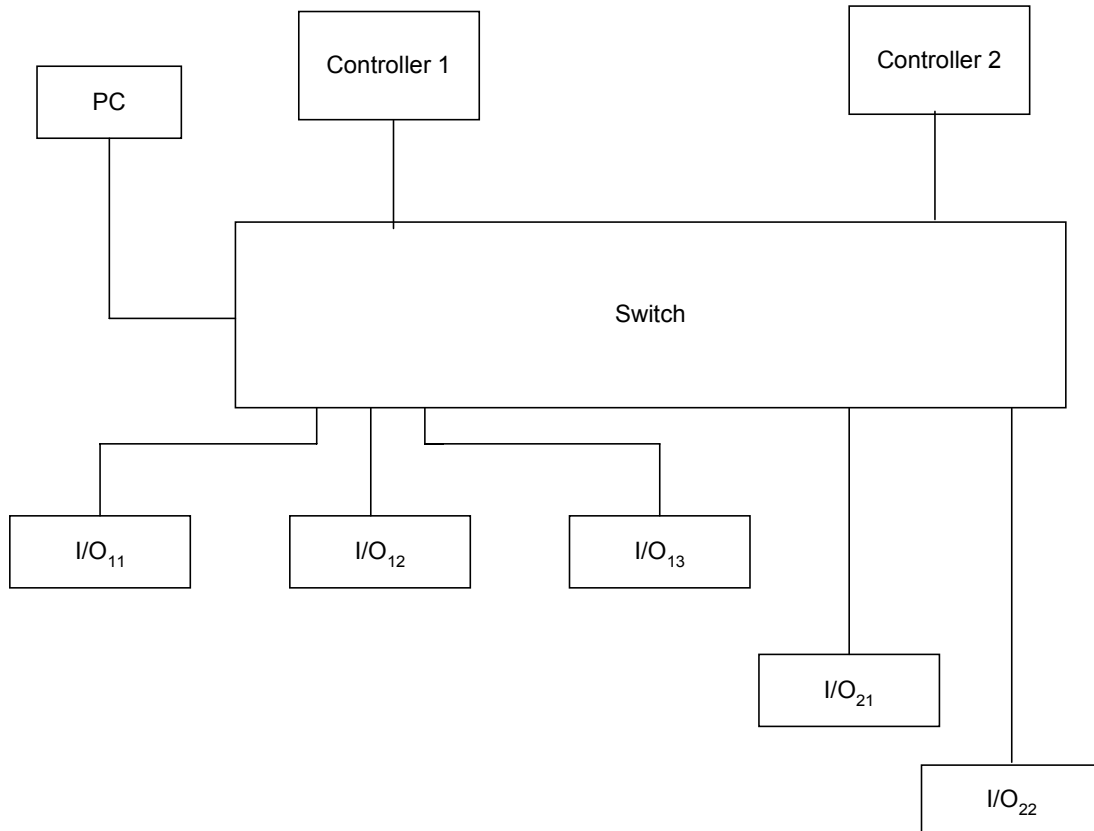
- Input/Output (I/O) data and status produced by a remote I/O device for consumption by one or more programmable controllers
- Data produced by a programmable controller for consumption by one or more programmable controllers

Although EtherNet/IP™ supports change-of-state and cyclic reporting, in a typical control system data exchange is predominately cyclic. The time-critical traffic is normally generated at an aggregate 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<sub>11</sub> 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<sup>TM</sup> 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<sup>TM</sup> 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 and stability and providing required level of quality of service. However, not all of these features are effective in dealing with the IP multicast traffic generated in EtherNet/IP<sup>TM</sup> sub-nets. For instance, among the three IP multicast control features mentioned above only IP routing can be considered for control of the EtherNet/IP<sup>TM</sup> multicast traffic. The following section provides objectives directing design of an EtherNet/IP<sup>TM</sup> network infrastructure and identifies features, which must be supported by this infrastructure in order to achieve them.

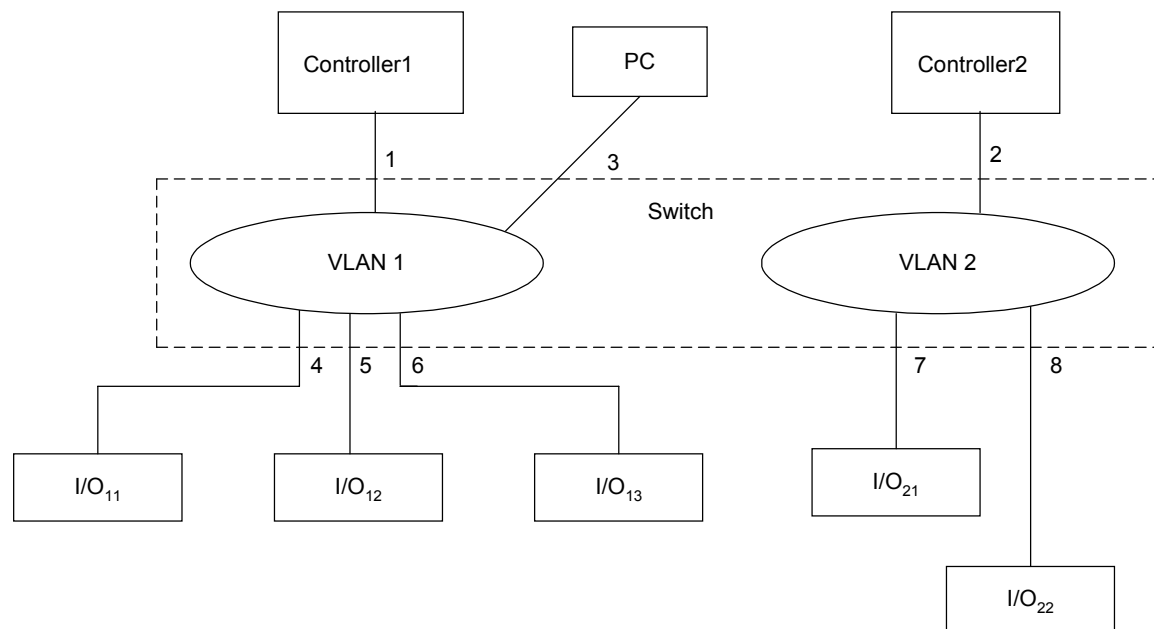
## RECOMMENDATIONS

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

### 1. Minimize device load due to unwanted IP multicast traffic

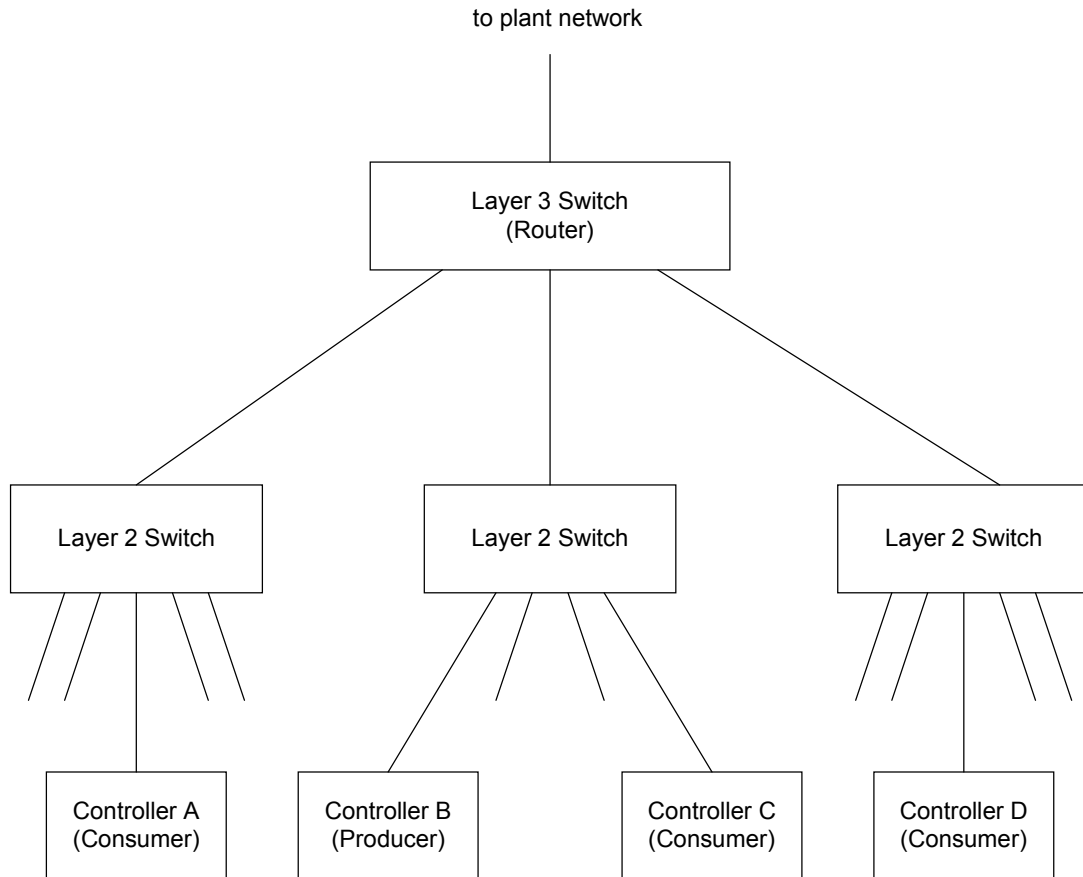
Depending on sub-net configuration and required device connectivity, this objective can be achieved using Ethernet switches supporting virtual LANs (VLANs) and IP multicast routing.

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 VLAN. Figure 3 depicts an example of an EtherNet/IP™ VLAN within a two-layer switch hierarchy. The VLAN is configured at the Layer 3 switch and consists of devices connected to three Layer 2 switches. If Layer 2 switches in this example do not support IP multicast routing, then multicast packets from Controller B (Producer) will flood all ports of these switches. Support of Internet Group Management Protocol (IGMP) snooping, or other functionally equivalent feature, in Layer 2 switches will eliminate multicast flood through them and, as a result of that, additional load in end-devices due to unwanted IP multicast traffic, which, in its turn, will improve control system performance. When IGMP snooping is enabled, IP multicast packets produced by Controller B will be routed only to controllers A, C, and D registered with the Layer 3 switch built-in router as members of the same multicast group.



**Figure 3: IP Multicast Routing Example**

## 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 VLAN. If, for example, IP multicast packets produced by Controller B are addressed only to Controller C and IGMP snooping is activated, then this traffic will be confined to the Layer 2 switch to which both controllers are connected. More accurately, it will be routed only between the switch ports to which these controllers are connected. Engagement of IGMP snooping will thus eliminate load on the other two switches due to this traffic.

## 3. Minimize network load due to unwanted incoming IP multicast traffic

EtherNet/IP<sup>TM</sup> network performance must not be degraded due to unwanted multicast traffic (for instance, stream video) propagating from the plant network and loading switches and end-devices. The Layer 3 switch in the example shown in Figure 3 should be configured to block this traffic. One of the features that could be used in this case is the Time-To-Live (TTL) Threshold. The Layer 3 switch has, by definition, a built-in router. The TTL Threshold may be set on the router port (in this case a virtual port) connecting it to the VLAN considered in sections 1 and 2. Multicast packets forwarded by the router to this VLAN will be checked against the threshold and discarded if their TTL is less than the specified one.

#### **4. Block IP multicast traffic generated within the EtherNet/IP™ sub-net from propagation into the plant network.**

This can be achieved utilizing the TTL Threshold feature described in section 3. The TTL Threshold will be set, in this case, on the router port connecting it to the VLAN containing the uplink to the plant network.

### **TEST RESULTS**

EtherNet/IP™ examples shown in Figures 1 to 3 are simplified versions of configurations used during performance and interoperability tests of Rockwell Automation EtherNet/IP™ products. VLANs and IGMP Snooping have successfully tested in configurations utilizing Cisco Catalyst 3550 (Layer 3) and 2950 (Layer 2) switches and Enterasys Networks Vertical Horizon VH-2403-L3 (Layer 3) and 2H252-25R Smart Switch 2200 (Layer 2) switches.

### **CONCLUSIONS**

In this paper, we have characterized the EtherNet/IP™ traffic and provided recommendations aimed to optimize network, and ultimately control system, performance. These recommendations are based on utilization of switching devices in the EtherNet/IP™ infrastructure that possess specific features, like IGMP Snooping, aiming to minimize end-device and switch loading with unwanted traffic as well as propagation of the such a traffic to and from a plant network.

### **ISSUES**

The following issues have been identified during performance and interoperability tests of EtherNet/IP™ products performed by Rockwell Automation:

- 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.

### **GLOSSARY OF TERMS**

Terms defined below have been copied from [2] and [3] with some tailoring to EtherNet/IP™ terminology where appropriate.

#### **IEEE 802.1**

The IEEE standard for bridging 802.3 local area networks (LANs).

#### **IEEE 802.3**

The IEEE standard for Ethernet.

**Address Resolution Protocol (ARP)**

A protocol used to dynamically bind a high-level IP address to a low-level physical hardware address. Within the scope of this paper it means a protocol that converts an IP address into an Ethernet address. ARP is used across a single physical network and is limited to networks, like Ethernet, which support broadcast.

**BOOTstrap Protocol (BOOTP)**

A protocol a node uses to obtain its IP Address, Subnet Mask and Gateway Address from a server.

**Broadcast**

A transmission method, by which a packet is sent to multiple, unspecified recipients. Broadcast transmission is supported by Ethernet and IP protocols.

**Dynamic Host Configuration Protocol (DHCP)**

A protocol a node uses to obtain its IP Address, Subnet Mask and Gateway Address from a server. A superset of the BOOTP.

**Internet Group Management Protocol (IGMP)**

A protocol that nodes use to keep local routers apprised of their membership in multicast groups. When all nodes leave a group, routers no longer forward packets that arrive for the group.

**IGMP Snooping**

A function that constrains flooding of multicast traffic through Layer 2 switch ports by dynamically configuring them so that multicast traffic forwarded only to those ports that are associated with nodes belonging to a specific IP multicast group.

**Layer 2 (Data Link Layer or Level)**

A reference to the Data Link layer communication (e.g., frame formats) or Data Link layer connections derived from the ISO 7-Layer Reference Model. For local area networks, layer 2 refers to physical frame format and addressing. Thus, for an EtherNet/IP<sup>TM</sup> network a layer 2 address is an Ethernet address.

**Layer 3 (Network Layer or Level)**

A reference to the Network layer communication derived from the ISO 7-Layer Reference Model. For TCP/IP networks, layer 3 refers to IP and the IP packet format. Thus, a layer 3 address is an IP address.

**Multicast**

A transmission method, by which a packet is sent to a selected subset of all possible recipients. A node can belong to one or more multicast groups. Multicast transmission is supported by Ethernet and IP protocols. Approximately half of EtherNet/IP<sup>TM</sup> UDP packets are sent via multicast.

**Simple Network Management Protocol (SNMP)**

A standard protocol used to monitor nodes, switches, routers, and networks to which they are attached.

### **Spanning Tree Protocol (STP)**

A switch (or bridge) protocol that uses the spanning-tree algorithm, enabling a switch to dynamically work around loops in a network topology by creating a spanning tree. Switches exchange special messages with other switches to detect loops, and then remove the loops by shutting down selected switch interfaces. Refers to both the IEEE 802.1 Spanning-Tree Protocol standard and the earlier Digital Equipment Corporation Spanning-Tree Protocol upon which it is based.

### **Time To Live (TTL)**

A technique used in best-effort delivery systems to avoid endlessly looping packets. For example, each IP packet is assigned an integer TTL when it is created (TTL is a field in the IP packet header). Each router decrements the TTL field when the packet arrives. A router discards any packet when TTL reaches zero.

### **Unicast**

A transmission method by which a packet is sent to a single destination. All of EtherNet/IP<sup>TM</sup> TCP packets and approximately half of UDP packets are sent via unicast.

### **Virtual LAN (VLAN)**

Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.

## **REFERENCES**

- [1] EtherNet/IP<sup>TM</sup> Specification, available on <http://www.odva.org>.
- [2] Comer, Douglas E., "Internetworking with TCP/IP, Volume 1: Principles, Protocol, and Architecture," Prentice Hall, 1995.
- [3] Dictionary of Internetworking Terms and Acronyms, available on <http://www.cisco.com/>

## **TRADEMARKS**

EtherNet/IP<sup>TM</sup> is a trademark of ControlNet<sup>TM</sup> 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<sup>TM</sup> is a trademark of ControlNet International, Ltd.  
DeviceNet<sup>TM</sup> is a trademark of ODVA.