Industrial **Ethernet**: A Control Engineer's Guide

Article Summary

As part of a continuing effort to make their organizations more efficient and productive, manufacturers are rapidly migrating to Industrial Ethernet technology. This standards-based technology enables organizations to control costs by moving from costly proprietary systems to a proven technology that is more secure, reliable, and deterministic.

This white paper provides an overview of Ethernet technology and its benefits in the data networking environment. It discusses the benefits of using a switched Ethernet architecture in industrial networking environments, including:

- Determinism
- Latency
- Minimal packet loss
- Broadcasts and multicast support
- Network analyzer monitoring
- Standardized infrastructure

Industrial Ethernet applies the Ethernet standards developed for data communication to manufacturing control networks. By implementing an intelligent Industrial Ethernet solution, organizations can build a manufacturing infrastructure that delivers the resiliency and network security of traditional fieldbus solutions, as well as improved bandwidth, open connectivity, and standardization that Ethernet provides. Industrial Ethernet provides organizations substantially greater control over their networked manufacturing equipment.

Introduction

As manufacturers seek to improve processes, reduce expenses, and improve productivity, many are turning to Ethernet technology on the factory floor. This migration is rapidly gaining momentum. According to a recent ARC Advisory Group study, the worldwide market for Industrial Ethernet devices is expected to grow at a rate of more than 84 percent over the next five years. Once considered a solution that was limited to corporate network environments, Ethernet technology has proven to be a robust alternative that can meet the unique needs of the manufacturing arena.

Industrial Ethernet networks that use intelligent switching technology can offer a variety of advantages compared to traditional industrial network installations. Industrial Ethernet applies the Ethernet standards developed for data communication to manufacturing control networks. The technology can be deployed using a switched Ethernet architecture that has proven successful in multiple critical applications in different markets. Because the technology is based on industry standards, Industrial Ethernet enables organizations to save money by moving away from expensive, proprietary systems. At the same time, it delivers the network security, performance, and availability required to support critical manufacturing applications.

To deploy this new technology, engineers on the manufacturing floor should be familiar with some of the important concepts behind Industrial Ethernet. This paper will provide a general overview of the most important traditional Ethernet technologies in use today. It will also discuss how Industrial Ethernet upgrades traditional, proprietary factory-floor networks to a low-cost, high-performance, scalable architecture. Finally, this paper will review some of the intelligent features that make Industrial Ethernet an attractive choice for manufacturing organizations.

What Is Ethernet?

Ethernet is the major local-area network (LAN) technology in use today, and is used for approximately 85 percent of the world's LAN-connected PCs and workstations. Ethernet refers to the family of LAN products covered by the IEEE 802.3 standard, and the technology can run over both optical fiber and twisted-pair cables. Over the years, Ethernet has steadily evolved to provide additional performance and network intelligence. This continual improvement has made Ethernet an excellent solution for industrial applications. Today, the technology can provide four data rates.

- *10BASE-T Ethernet* delivers performance of up to 10 Mbps over twisted-pair copper cable.
- *Fast Ethernet* delivers a speed increase of ten times the 10BASE-T Ethernet specification (100 Mbps) while retaining many of Ethernet's technical specifications. These similarities enable organizations to use 10BASE-T applications and network management tools on Fast Ethernet networks.
- *Gigabit Ethernet* extends the Ethernet protocol even further, increasing speed tenfold over Fast Ethernet to 1000 Mbps, or 1 Gbps. Because it is based upon the current Ethernet standard and compatible with the installed base of Ethernet and Fast Ethernet switches and routers, network managers can support Gigabit Ethernet without needing to retrain or learn a new technology.
- *10 Gigabit Ethernet*, ratified as a standard in June 2002, is an even faster version of Ethernet. It uses the IEEE 802.3 Ethernet media access control (MAC) protocol, the IEEE 802.3 Ethernet frame format, and the IEEE 802.3 frame size. Because 10 Gigabit Ethernet is a type of Ethernet, it can support intelligent Ethernet-based network services, interoperate with existing architectures, and minimize users' learning curves. Its high data rate of 10 Gbps makes it a good solution to deliver high bandwidth in wide-area networks (WANs) and metropolitan-area networks (MANs).

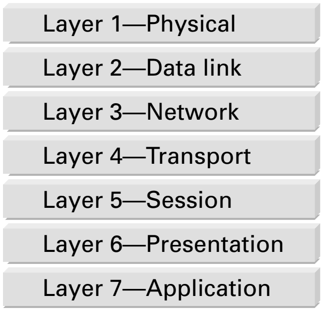
More than 300 million switched Ethernet ports have been installed worldwide. Ethernet technology enjoys such wide acceptance because it is easy to understand, deploy, manage, and maintain. Ethernet is low-cost and flexible, and supports a variety of network topologies. Although traditional, non-Ethernet-based industrial solutions have a data rate of between 500 Kbps to 12 Mbps, Ethernet technology can deliver substantially higher performance. And, because it is based on industry standards, it can run and be connected over any Ethernet-compliant device from any vendor.

The Open Systems Interconnection Reference Model

At the heart of data networking is the Open Systems Interconnection (OSI) reference model. This conceptual model describes how information from a software application in one computer moves through a network medium to a software application in another computer. The model was developed by the International Organization for Standardization (ISO) in 1984, and it is now considered the primary architectural model for intercomputer communications.

The OSI reference model divides the tasks involved in moving information between networked computers into seven smaller, more manageable task groups. These tasks are then assigned to seven layers in the OSI model. Each layer is self-contained so that the tasks assigned to it can be implemented independently. Figure 1 shows the seven OSI layers.

Figure 1
Layers of the OSI Reference Model



Functions of the OSI Layers

The seven layers of the OSI reference model can be divided into lower layers (1–4) and upper layers (5–7). The lower layers of the OSI model focus on data-transport issues while the upper layers focus on the applications. The physical layer and the data link layer are implemented in hardware and software. The lowest layer, the physical layer, is closest to the physical network medium, such as network cabling. Ethernet resides in Layer 2, as do some implementations of traditional fieldbuses such as DeviceNet, which uses the Controller Area Network (CAN) protocol. Layer 3 takes care of the logical addressing and routing (which way to send data). Its most common implementation uses the Internet Protocol (IP), which is the core of World Wide Web addressing and routing. Layer 4, the last of the lower layers, is the transport layer. It ensures that data is delivered error-free and in the correct sequence. Industrial Ethernet is broader than traditional Ethernet technology. While Ethernet technology refers only to Layer 2, most Industrial Ethernet solutions also encompass Layer 3 and 4, using IP addressing in Layer 3, and Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) in Layer 4.

The upper layers of the OSI reference model are responsible for application tasks and are usually implemented only in software. The highest layer, the application layer, is closest to the end user. Both users and application-layer processes interact with software applications that involve network communications.

For more information about the OSI reference model, visit:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introint.htm#xtocid5

Benefits of a Switched Ethernet Architecture

Organizations can choose from a variety of devices and architectures when building an Ethernet LAN. For industrial networking environments, a switched Ethernet architecture is the most appropriate choice. Switches make it possible for several users to send information over a network at the same time without slowing each other down.

In a fully switched network, there are no hubs so each Ethernet network has a dedicated segment for every node. Because the only devices on each segment are the switch and the node, the switch picks up every transmission before it reaches another node. The switch then forwards the data over to the appropriate segment. In a fully switched network, nodes only communicate with the switch and never directly with each other.

Fully switched networks employ either twisted pair or fiber-optic cabling, both of which use separate conductors for sending and receiving data. This allows nodes to transmit to the switch at the same time the switch transmits to them, for a collision-free environment. Transmitting in both directions also can effectively double the apparent speed of the network when two nodes are exchanging information. For example, if the speed of the network is 10 Mbps, each node can transmit at 10 Mbps at the same time.

Switches usually work at Layer 2 (data link) of the OSI reference model using MAC addresses, and deliver a number of important advantages compared to hubs and other LAN devices. Some of these advantages include the following:

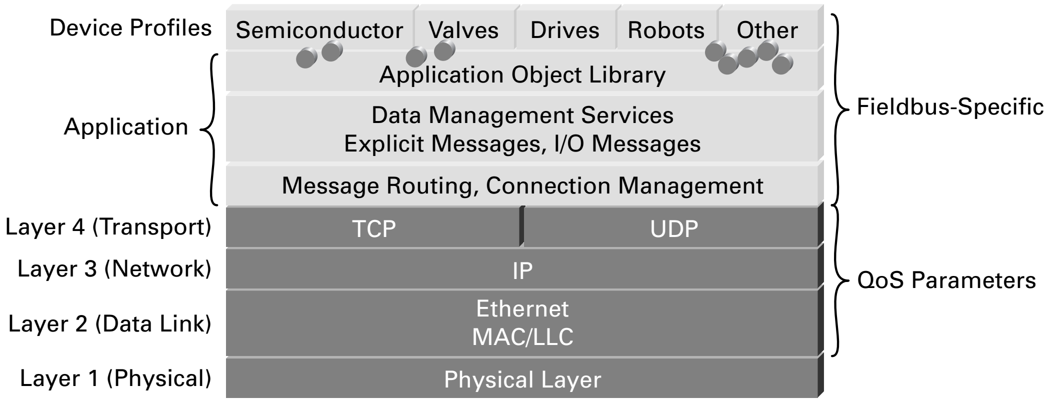
- *Determinism*—Determinism, the ability to ensure that a packet is sent and received in a specific period of time, is an important design goal for industrial networks. For the network to be deterministic, the design must be as simple and highly structured as possible.
- *Latency*—Switches normally have very low latencies, which refers to the time it takes for a network packet to transit between a source and a target. Most control operations in industrial applications can tolerate latencies of 10 to 50 milliseconds (ms). Because control traffic frames in industrial applications are usually below 500 bytes, the latency introduced by a switch at 100 Mbps is only about 30 microseconds with a worst-case scenario of close to 100 microseconds—well below the limit and 100 times faster than most applications require.
- *Packet loss under congestion*—Today's intelligent switches offer quality-of-service (QoS) features that make it possible to prioritize critical traffic so that it will not be dropped due to congestion. By implementing simple QoS parameters in an intelligent switch, organizations can prioritize critical traffic over noncritical traffic at wire speed, helping to ensure packet integrity for the control network. Even under heavy congestion, QoS features help ensure that important traffic will reach its destination.
- *Broadcasts and multicast*—Industrial applications often rely on broadcast or multicast communication. Intelligent switching platforms can dynamically configure the interfaces so that traffic is forwarded only to ports associated with requested data. This feature reduces the load of traffic crossing the network and relieves the client devices from processing unneeded frames.
- *Network analyzers*—Intelligent switches allow traffic analyzers to remotely monitor any port in a network, which saves organizations time and money and reduces the amount of hardware that must be deployed to monitor and optimize network usage.
- *Standardization*—One of the main motives for Industrial Ethernet is the need to standardize around a common infrastructure. Unlike proprietary technologies that often tie companies to a particular vendor, standardized solutions free users to choose the best application for a given solution. And a standard Ethernet network brings to the factory floor the economies of scale enjoyed by today's large base of Ethernet users, lowering costs and increasing the number of potential equipment vendors and products.

What Is Industrial Ethernet?

Recognizing that Ethernet is the leading networking solution, many industry organizations are porting the traditional fieldbus architectures to Industrial Ethernet. Industrial Ethernet applies the Ethernet standards developed for data communication to manufacturing control networks (Figure 2). Using IEEE standards-based equipment, organizations can migrate all or part of their factory operations to an Ethernet environment at the pace they wish.

Figure 2

Using Intelligent Ethernet for Automation Control

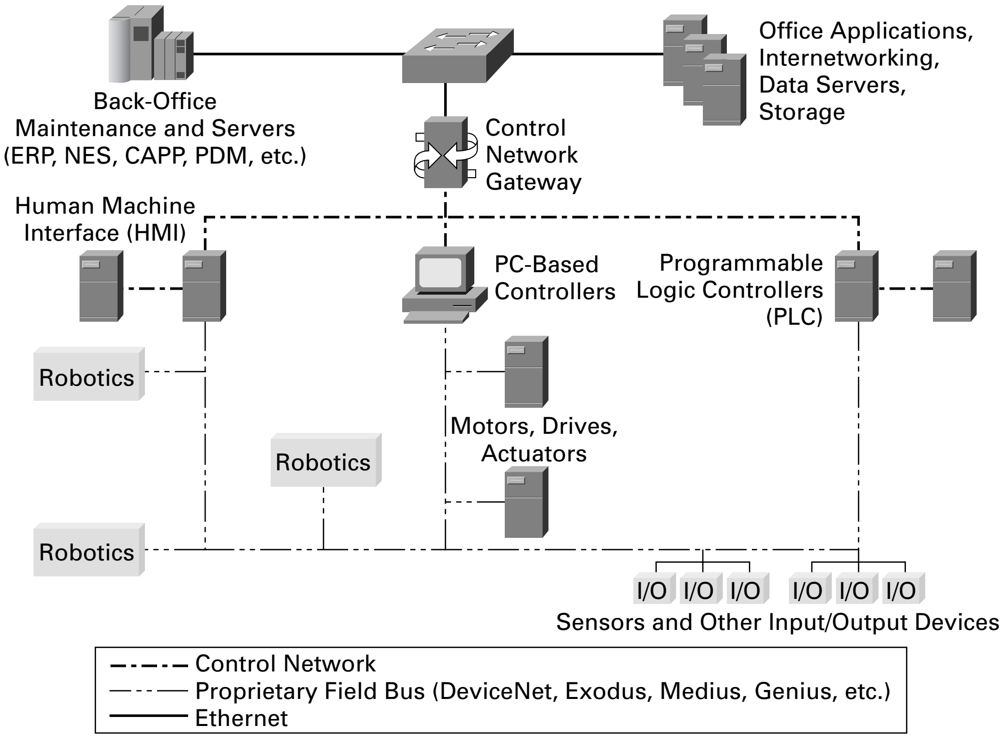


For example, DeviceNet, a device-level network based on the Common Industrial Protocol, can be ported to the Ethernet environment (Figure 3). The fieldbus data structure is applied to Layers 5, 6, and 7 of the OSI reference model over Ethernet, IP, and TCP/UDP in the transport layer (Layer 4).

The advantage of Industrial Ethernet is that organizations and devices can continue using their traditional tools and applications running over a much more efficient networking infrastructure.

Figure 3

Proprietary Fieldbus Architecture



Industrial Ethernet not only gives manufacturing devices a much faster way to communicate, but also gives the users better connectivity and transparency, enabling users to connect to the devices they want without requiring separate gateways.

Traditionally Separate Networks

Today, many manufacturing companies maintain separate networks to support their factory floor operations and business operations. Over the years, these networks were developed to respond to the different information flows and control requirements involved with manufacturing processes.

The corporate IT network supports traditional administrative functions and corporate applications, such as human resources, accounting, and procurement. This network is usually based on the Ethernet standard.

The control-level network connects control and monitoring devices, including programmable logic controllers, PC-based controllers, I/O racks, and human-machine interfaces (HMIs). This network, which has not been Ethernet in the past, requires a router or, in most cases, a gateway to translate application-specific protocols to Ethernet-based protocols. This translation lets information pass between the control network on the factory floor and the corporate network infrastructure.

The device-level network links the plant floor's I/O devices, including sensors such as transducers, photoeyes, and flowmeters, and other automation and motion equipment, such as robotics, variable frequency drives, and actuators. Interconnectivity between these devices was traditionally achieved with a variety of fieldbuses such as DeviceNet, Profibus, and Modbus. Each fieldbus has specific power, cable, and communication requirements, depending on the factory application it supports. This has lead to a replication of multiple networks in the same space and the need to have multiple sets of spares, skills, and support programs within the same organization.

Instead of using architectures composed of multiple separate networks, Industrial Ethernet can unite a company's administrative, control-level, and device-level networks to run over a single network infrastructure. In an Industrial Ethernet network, fieldbus-specific information that is used to control I/O devices and other manufacturing components are embedded into Ethernet frames. Because the technology is based on industry standards rather than on custom or proprietary standards, it is more interoperable with other network equipment and networks.

Technology Tailored for Manufacturing

Although Industrial Ethernet is based on the same industry standards as traditional Ethernet technology, the implementation of the two solutions is not always identical. Industrial Ethernet usually requires more robust equipment and a very high level of traffic prioritization when compared with traditional Ethernet networks in a corporate data network.

The primary difference between Industrial Ethernet and traditional Ethernet is the type of hardware used. Industrial Ethernet equipment is designed to operate in harsh environments. It includes industrial-grade components, convection cooling, and relay output signaling. And it is designed to operate at extreme temperatures and under extreme vibration and shock. Power requirements for industrial environments differ from data networks, so the equipment runs using 24 volts of DC power. To maximize network availability, it also includes fault-tolerant features such as redundant power supplies.

Industrial Ethernet environments also differ from traditional Ethernet networks in their use of multicasting by hosts for certain applications. Industrial applications often use producer-consumer communication, where information "produced" by one device can be "consumed" by a group of other devices (see box). In a producer-consumer environment, the most important priority for a multicast application is to guarantee that all hosts receive data at the same time. A traditional Ethernet network, on the other hand, focuses more on the efficient utilization of bandwidth in general, and less on synchronous data access. To help optimize synchronous data access, Industrial Ethernet equipment must include the intelligence and QoS features needed to enable organizations to appropriately prioritize multicast transmissions.

Increasing Industry Support

Industrial Ethernet technology is rapidly being embraced by multiple organizations and vendors, including the Industrial Ethernet Association (IEA), the Open DeviceNet Vendor Association (ODVA), Modbus.org, Fieldbus Foundation, and the Industrial Automation Open Networking Alliance (IAONA).

Network Requirements: The Need for Intelligence

When implementing an Industrial Ethernet solution, companies should be careful to select Ethernet products that offer the intelligent features required to support manufacturing applications. Network intelligence enables organizations to build a manufacturing infrastructure that matches the resiliency and network security of traditional fieldbus solutions, while at the same time providing the benefits of higher bandwidth, open connectivity, and standardization offered by Ethernet-based platforms. The important qualities behind an intelligent Industrial Ethernet solution include network security, reliability, and determinism.

Network Security

Ethernet technology can provide not only excellent performance for manufacturing applications, but a wide range of network security measures to provide both confidentiality and data integrity. Confidentiality helps ensure that data cannot be accessed by unauthorized users. Data integrity protects data from intentional or accidental alteration. These network security advantages protect manufacturing devices like programmable logic controllers (PLCs) as well as PCs, and apply to both equipment and data security.

Manufacturers can use many methods to help ensure network confidentiality and integrity. These network security measures can be grouped into several categories, including access control and authentication, and secure connectivity and management.

Access Control and Authentication

Access control is commonly implemented using firewalls or network-based controls protecting access to critical applications, devices, and data so that only legitimate users and information can pass through the network. However, access-control technology is not limited to dedicated firewall devices. Any device that can make decisions to permit or deny network traffic, such as an intelligent switch, is part of an integrated access-control solution.

When designing an access-control solution, network administrators can set up filtering decisions based on a variety of criteria, such as an IP address or TCP/UDP port number. Intelligent switches can provide support for this advanced filtering to limit network access to authorized users. At the same time, they can enable organizations to enforce policy decisions based on the IP or MAC address of a laptop or PLC.

Virtual LANs (VLANs) are another access-control solution, providing the ability to create multiple IP subnets within an Ethernet switch. VLANs provide network security and isolation by virtually segmenting factory-floor data from other data and users. VLANs can also be used to enhance network performance, separating low-priority end devices from high-priority devices.

Access controls can also include a variety of device or user-authentication services. Authentication services determine who may access a network and what services they are authorized to use. For example, the 802.1x authentication protocol provides port-based authentication so that only legitimate devices can connect to switch ports. Authentication services are an effective complement to other network security measures in a manufacturing environment.

Secure Connectivity and Management

To provide additional protection for manufacturing networks, organizations can take several approaches to authenticate and encrypt network traffic. Using virtual private network (VPN) technology, Secure Sockets Layer (SSL) encryption can be applied to application-layer data in an IP network. Organizations can also use IP Security (IPSec) technology to encrypt and authenticate network packets to thwart network attacks such as sniffing and spoofing.

VPN client software, together with dedicated VPN network hardware, can be used to encrypt device monitoring and programming sessions, and to support strong authentication. Manufacturers can also use Secure Shell (SSH) Protocol encryption for remote terminal logins to network devices. Version 3 of Simple Network Management Protocol (SNMP) also offers support for encryption and authentication of management commands and data.

Reliability

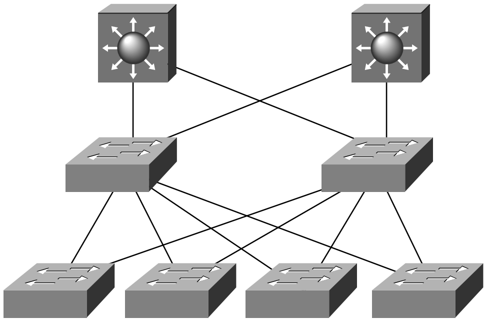
Because factory-floor applications run in real time, the network must be available to users on a continuous basis, with little or no downtime. Manufacturers can help ensure network reliability using effective network design principles, as well as intelligent networking services.

Network Topology

Manufacturers deploying an Ethernet solution should design networks with redundant paths to ensure that a single device outage does not take down the entire network. Two network topologies most often used are ring and hub-and-spoke. In hub-and-spoke designs (Figure 4), three layers of switches are usually installed. The first layer is often referred to as the access layer. These switches provide connections for end-point devices like PLCs, robots, and HMIs. A second layer called the distribution layer provides connectivity between the access-layer switches. And a third layer called the core layer provides connectivity to other networks or to the Internet service provider (ISP) via routers. The distribution layer may include switches with routing functions to provide inter-VLAN routing. Access-layer switches, on the other hand, generally provide only Layer 2 (data link) forwarding services. For optimum performance, network equipment at each of these layers must be aware of the information contained within the Layer 2 through Layer 4 packet headers.

Figure 4

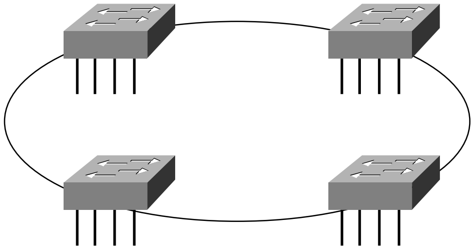
Hub-and-Spoke Network Topology



In ring topologies (Figure 5), all devices are connected in a ring. Each device has a neighbor to its left and right. If a connection on one side of the device is broken, network connectivity can still be maintained over the ring via the opposite side of the device. In some situations, manufacturers install dual counter-rotating rings to maximize availability. In a ring topology, each switch functions as both an access-layer and as a distribution-layer switch.

Figure 5

Ring Topology]



Spanning Tree Protocols

To prevent loops from being formed in the network when devices are interconnected via multiple paths, some organizations use the Spanning Tree Protocol. If a problem occurs on a network node, this protocol enables a redundant alternative link to automatically come back online.

The traditional Spanning Tree Protocol has been considered too slow for industrial environments. To address these performance concerns, the IEEE standards committee has ratified a new Rapid Spanning Tree Protocol (802.1w). This protocol provides subsecond convergence times that vary between 200 and 800 ms, depending on network topology. Using 802.1w, organizations can enjoy the benefits of Ethernet networks, with the performance and reliability that manufacturing applications demand.

Another spanning-tree option is Multiple Spanning Tree Protocol (802.1s). This enables VLANs to be grouped into spanning-tree instances. Each instance has a spanning-tree topology that is independent from other spanning-tree instances. This architecture provides multiple forwarding paths for data traffic, enables load balancing, and reduces the number of spanning-tree instances needed to support a large number of VLANs.

Using Option 82

Ethernet switches provide excellent connectivity and performance; however, each switch is another device that must be managed on the factory floor. To make switched Ethernet networks easy to support and maintain, intelligent switches include built-in management capabilities. These intelligent features make it easy to connect manufacturing devices to the network, without creating additional configuration tasks. And they help minimize network downtime if part of the network should fail. One of the most useful intelligent features in a switched Ethernet network is Option 82.

In an Ethernet network, Dynamic Host Configuration Protocol (DHCP) lets devices dynamically acquire their IP addresses from a central server. The DHCP server can be configured to give out the same address each time or generate a dynamic one from a pool of available addresses.

Because the interaction of the factory-floor devices requires specific addresses, Industrial Ethernet networks usually don't use dynamic address pools. However, static addresses can have drawbacks. Because they are linked to the MAC address of the client, and because the MAC address is often hard-coded in the network interface of the client device, the association is lost when a client device fails and needs to be replaced.

Extended fields in the DHCP packet can be filled in by the switch, indicating the location of the device requesting an IP address. The 82nd optional field, called Option 82, carries the specific port number and the MAC address of the switch that received the DHCP request. This modified request is sent on to the DHCP server. If an access server is Option 82-aware, it can use this information to formulate an IP address based on the Option 82 information. Effective use of Option 82 enables manufacturers to minimize administrative demands and maintain maximum network uptime even in the event of the failure of individual devices.

Determinism

Because manufacturing processes depend on the precise synchronization of processes, network determinism must be optimized to deliver the best possible performance. Data must be prioritized using QoS to ensure that critical information is received first. And the multicast applications that are prevalent in manufacturing environments must be well-managed using Internet Group Management Protocol (IGMP) snooping.

The Producer-Consumer Model in Industrial Ethernet

Many Industrial Ethernet applications depend on IP multicast technology. IP multicast allows a host, or source, to send packets to another group of hosts called receivers anywhere within the IP network using a special form of IP address called the IP multicast group address.

While traditional multicast services, such as video or multimedia, tend to scale with the number of streams, Industrial Ethernet multicast applications do not. Industrial Ethernet environments use a producer-consumer model, where devices generate data called "tags" for consumption by other devices. The devices that generate the data are producers and the devices receiving the information are consumers. Multicast is more efficient than unicast, because consumers will often want the same information from a particular producer. Each device on the network can be both a producer and a consumer of traffic.

While most devices generate very little data, networks with a large number of nodes can generate a large amount of multicast traffic, which can overrun end devices in the network. Using mechanisms like QoS and IGMP snooping, organizations can control and manage multicast traffic in manufacturing environments.

Quality of Service

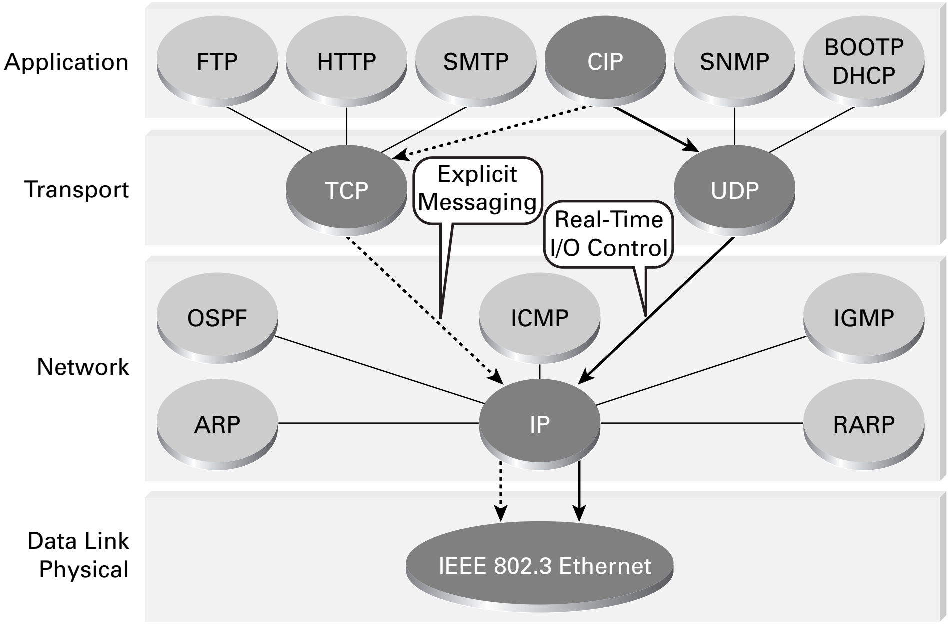
An Industrial Ethernet network may transmit many different types of traffic, from routine data to critical control information, or even bandwidth-intensive video or voice. The network must be able to distinguish among and give priority to different types of traffic.

To address these issues, organizations can implement QoS using several techniques. QoS involves three important steps. First, different traffic types in the network need to be identified through classification techniques. Second, advanced buffer-management techniques need to be implemented to prevent high-priority traffic from being dropped during congestion. Finally, scheduling techniques need to be incorporated to transmit high-priority traffic from queues as quickly as possible.

In Layer 2 switches on an Ethernet network, QoS usually prioritizes native, encapsulated Ethernet frames, or frames tagged with 802.1p class of service (CoS) specifications. More advanced QoS mechanisms take this definition a step further. For example, advanced Ethernet switches can study and interpret the flow of QoS traffic as it is processed through the switch.

A switch can be configured to prioritize frames based on given criteria at different layers of the OSI reference model (Figure 6). For example, traffic could be prioritized according to the source MAC address (in Layer 2) or the destination TCP port (in Layer 4). Any traffic traveling through the interface to which this QoS is applied is classified, and tagged with the appropriate priority. Once a packet has been classified, it is then placed in a holding queue in the switch, and scheduled based on the scheduling algorithm desired.

Figure 6
Applying QoS to Industrial Applications



In an Industrial Ethernet application, real-time I/O control traffic would share network resources with configuration (FTP) and data-collection flows, as well as other traffic, in the upper layers of the OSI reference model. By using QoS to give high priority to real-time UDP control traffic, organizations can prevent delay or jitter from affecting any control functions.

IGMP Snooping

Many manufacturing applications depend on multicast traffic, which can introduce performance problems in the network. To address these challenges in an Industrial Ethernet environment, organizations can deploy IGMP snooping. IGMP snooping limits the flooding of multicast traffic by dynamically configuring the interfaces so that multicast traffic is forwarded only to interfaces associated with IP multicast devices. In other words, when a multicast message is sent to the switch, the switch forwards the message only to the interfaces that are interested in the traffic. This is very important because it reduces the load of traffic traversing through the network. It also relieves the hosts from processing frames that are not needed.

In a producer-consumer model used by Industrial Ethernet, IGMP snooping can limit unnecessary traffic from the I/O device that is producing, so that it only reaches the device consuming that data. Messages delivered to a given device that were intended for other devices consume resources and slow performance, so networks with many multicasting devices will suffer performance issues if IGMP snooping or other multicast limiting schemes are not implemented.

The IGMP snooping feature allows Ethernet switches to “listen” to the IGMP conversation between hosts. With IGMP snooping, the Ethernet switch examines the IGMP traffic coming to the switch and keeps track of multicast groups and member ports. When the switch receives an “IGMP join” report from a host for a particular multicast group, the switch adds the host port number to the associated multicast forwarding table entry. When it receives an IGMP “leave group” message from a host, it removes the host port from the table entry. After the switch relays the IGMP queries, it deletes entries periodically if it does not receive any IGMP membership reports from the multicast clients. A Layer 3 router normally performs the querying function.

When IGMP snooping is enabled in a network with Layer 3 devices, the multicast router sends out periodic IGMP general queries to all VLANs. The switch responds to the router queries with only one “join” request per MAC multicast group. The switch then creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an IGMP join request. All hosts interested in this multicast traffic send “join” requests and are added to the forwarding table entry.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, in a managed switch, organizations can statically configure MAC multicast groups. This static setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined settings and settings learned via IGMP snooping.

Conclusion

The migration to Ethernet in manufacturing environments has been growing steadily as companies recognize the many benefits that Industrial Ethernet can deliver. According to an ARC Advisory Group study, the market for Industrial Ethernet devices grew at more than a 50 percent annual rate from 2001 to 2003.

The reasons behind the success of Industrial Ethernet are clear. The technology lets manufacturers standardize and consolidate their different manufacturing network architectures, using products offered by a variety of equipment vendors. Because Industrial Ethernet is a standards-based technology, it enables companies to take advantage of economies of scale, while still providing the flexibility needed to support their specific factory-floor requirements. Because Industrial Ethernet uses the intelligent networking features found in corporate data Ethernet environments, organizations can enjoy substantially greater control over their networked manufacturing equipment.

A well-implemented Industrial Ethernet network can do much more than simply emulate the functions of a traditional manufacturing network. It enables companies to more closely link their internal data networks with the factory floor to make the entire company's operations more efficient. And by enabling manufacturers to tap the innovation underway that supports the millions of existing Ethernet networks, it can make possible a wide range of new applications to support business needs well into the future.

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe