Cisco Systems

Technology Brief

Ethernet, Hubs, Switches, and the Evolving **Factory** Network

Abstract

Factory automation networks, whether small or large, need an intelligent network that provides a scalable and secure infrastructure. This foundation must be based on intelligent Ethernet switches that deliver high availability, quality of service (QoS), and network security. Hubs and unmanaged switches cannot provide the necessary support for real-time applications that are essential to modern factory networks.

Background

Ethernet was designed to be a multiple-device, connection-based network scheme very similar to a multidrop wiring scheme (also known as a shared medium). Early Ethernet implementations connected multiple network devices to a common backbone via a single cable. Because of this physical layout characteristic, multiple devices can transmit data at the same time, creating data collisions within the shared medium. In order to allow for multiple transmitters, the carrier sense multiple access collision detect (CSMA/CD) scheme was invented. With CSMA/CD, each network interface listens for an idle period before it starts transmitting. After the data is transmitted, the interface listens for collisions with other transmitting devices. If a collision is detected, the network interface waits a random amount of time before retransmitting its data.

Because of this random backoff period, early Ethernet systems were considered non-deterministic and not selected for early-generation factory networks. Factory network managers decided to use other technologies to ensure that their data connections were real-time and determistic.

Hubs

Hubs were invented as a cost-effective way of attaching multiple devices to a common central point in a star topology. This reduces many issues relating to the cabling of multiple hosts on a single cable. Hubs are implemented as simple multiport repeaters and every transmission is heard by every host connected to the hub. In other words, traffic flows to and from all ports in parallel. Therefore, hub-based networks still experience collisions and non-deterministic behavior.

Unmanaged Switches

An Ethernet switch functions much like a hub, in that it provides a cost-effective method for attaching multiple devices to a common network connection. But instead of bridging all the ports together in a common pool, an Ethernet switch builds a table of ports and the corresponding Media Access Control (MAC) addresses for each end device. Traffic is then forwarded only to the appropriate ports. In addition, an Ethernet switch usually has an internal backbone that is much faster than the combined speed of all the ports, thereby eliminating collisions. As long as the uplink ports do not become congested, collisions do not occur and no packets are lost.

Some Ethernet switches are unmanaged, meaning that the configuration cannot be changed and the status cannot be monitored. These switches do not contain any facility for turning on advanced features. End devices on these switches are grouped into one network segment or LAN.

In factory networks, where it is very common to multicast packets based on a one-to-many distribution model (such as producer to consumer, or publisher to subscriber), unmanaged switches essentially behave like hubs. Because multicast traffic is flooded to all the end-station ports in unmanaged switches, end devices may become overwhelmed with traffic not destined to them.

Intelligent Ethernet Managed Switches

Intelligent Ethernet switches provide a number of advanced features for factory automation. First, the user can set up virtual LANs (VLANs) to segment devices into logical workgroups. VLANs allow end-devices to be grouped together (in the same subnet, for example) even if they are in different locations. Therefore, machine controllers in one building can be grouped together with machine interfaces in another and treated as if they were physically next to each other.

A second major advantage of intelligent Ethernet switches is their ability to manage multicast traffic. Instead of flooding that traffic to all users, they use Internet Group Management Protocol (IGMP) to direct the traffic only to the desired recipients. Some packet line cards and multiple I/O devices have a limited capacity for received packets, and by using IGMP, an intelligent Ethernet switch can protect those end devices from unwanted traffic.

The third major advantage is QoS and queue management. By assigning a priority to time-sensitive data, intelligent Ethernet switches can elevate that traffic above lower-priority data. This ensures that high-priority traffic always traverses the network even if the network becomes congested. Without QoS and queue management, high-priority traffic may be delayed or dropped during congested periods.

Intelligent Ethernet switches allow the user to set up 801.q trunk interfaces. Via these trunk interfaces, traffic is marked with tags to indicate the particular VLAN the end device is in and the QoS priority for that particular data stream. Without the ability to set up trunk interfaces, there is no way to mark and pass on the QoS values, or to identify the VLAN origin of the data stream.

Lastly, intelligent Ethernet switches provide mechanisms to ensure network security via protocols such as 802.1x, port security, MAC address notification, Dynamic Host Configuration Protocol (DHCP) interface tracking, and many more. Each feature can be configured and tailored to the particular needs of the factory floor. By using access control lists (ACLs), certain traffic patterns can be directed to specific ports, preventing network intruders from accessing critical information. Likewise, by using these same ACLs and some of the QoS features mentioned above, the intelligent Ethernet switch can prevent an intruder from congesting the network.

Conclusion

As factory network managers start to deploy Ethernet as part of their overall network strategy, it is important to understand how Ethernet has evolved. Likewise, it is important to understand the differences between hubs, unmanaged switches, and managed intelligent switches. Only intelligent switches provide the necessary feature set to build robust and manageable networks. Intelligent Ethernet switches can be easily deployed today with the aid of simple, graphical interface tools and a standard PC browser, and network management tools such as HP Openview or Cisco Works.

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: +65 317 7777
Fax: +65 317 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

WH/LW3886 1102