DRAMATICALLY IMPROVE PERFORMANCE ON YOUR INDUSTRIAL NETWORK

Motion.com

IGMP SNOOPING SIGNIFICANTLY INCREASES NETWORK EFFICIENCY IN AN INDUSTRIAL ETHERNET ENVIRONMENT

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations, the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links that do not need them, therefore controlling which ports receive specific multicast traffic.

Many companies use the industrial network protocol Ethernet/IP, an Open DeviceNet Vendors Association (ODVA) open standard application protocol for communications. With Ethernet, there are three different methods of sending messages over computer networks:

1. **Unicast –** One device sends a message to exactly one device (node).
2. **Broadcast –** A packet sends the message to every node on the network, as in acquiring an IP address on a new network when there is no knowledge of the specific network configuration. All devices on the same network segment will receive the same message.
3. **Multicast –** This sends messages from one node (e.g., an I/O device or sensor) to multiple receivers such as PLCs and HMIs that are interested in obtaining the status. Ethernet/IP uses multicast extensively.

Benefits of multicast on managed switches

Unmanaged switches do not have the ability to determine the nodes that need to receive the multicast traffic and will forward the communication to every node (broadcast). The unprioritized, unnecessary traffic on the network can lead to dropped packets and loss of communication.

PLC/HMI vendors strongly suggest using managed switches in networks with their PLCs. This allows multicast traffic to be controlled with Internet Group Management Protocol. IGMP and IGMP snooping identify multicast groups and group members and can dramatically improve network performance by reducing unnecessary traffic.

IGMP snooping: how it works

The Network Working Group's RFC 2236 document defines the process for IGMP operation. On power-up, all multicast routers (IGMP-enabled switches) will perform as queriers. The queriers elect a single IGMP querier by listening to all queries. If a query is received from a querier that has a lower IP address, the switch will revert to nonquery mode. When the querier switch first sees a multicast message (recognized by the Ethernet IP address range 224.0.0.0 to 239.255.255.255), the switch sends a message called an "IGMP Group query" to all nodes on the network asking which nodes want to receive the communication from that sender. The devices that want to continue receiving the communication will respond with an "IGMP Group Join" message. The querier switch then builds a table of where the messages should be sent. From that point forward, only the nodes that requested to receive the data from that sender will receive the message.

A noticeable solution

Installations experiencing slow updates may be entirely corrected by simply replacing unmanaged switches with IGMP-enabled managed switches. IGMP snooping significantly increases network efficiency and effectively manages available bandwidth on the network by decreasing unnecessary processing of packets at every node. The larger the network, the bigger the problem, the more noticeable the solution.

Jack Baldwin is an Industrial Networking Specialist with the BRAAS Division at Motion in Eden Prairie, Minnesota.