Creating The Invisible Network

Brian Oulton

Director, Global Vertical Marketing – Industrial, Belden Inc.

Knowing how to transition your current industrial Ethernet infrastructure into a robust, invisible network that supports the varying demands placed on your production operations is key to building a competitive business ready for an ever-changing marketplace.

The data demands of a modern production facility — be it in the process industries or discrete manufacturing — require a communications infrastructure that can grow with the diverse range of demands placed on the business by supply chain partners and customers. This means that your communications network must be able to dramatically scale and adapt on the fly without the need for adjustments or upgrades each time a change is needed. Maintaining this kind of advanced network, however, has required a level of network infrastructure management from production personnel who should instead be spending their time on productivity improvements.

With the recent expansion of industrial Ethernet technology on the plant floor, there now exists an opportunity to meet these networking infrastructure requirements without the need for a great deal of network maintenance involvement from operations.

To help you assess your current industrial Ethernet infrastructure and understand what gaps need to be addressed to create a robust, invisible network that requires little maintenance to scale and adapt to changing business requirements, this article will explain how to: future proof your network for bandwidth requirements, provide for the ability to layer in new applications as needed, and properly select switches and cabling based on environmental and application specifics.

Create a Network Backbone

Instead of a flat network of switches connected to each other, creating an infrastructure based on a backbone to which a series of smaller networks can be connected is more strategic. Backbones are a series of fast, high-throughput switches that run throughout your production operations and connect to your enterprise network. These backbones are usually connected with fiber cable and connect to each other at 10 Gb/s or 40 Gb/s rates, while connecting to the next level of switches at 1 Gb/s or 10 Gb/s rates. Make the backbone switches resilient with redundant power supplies, and make the backbone network resilient by wiring it in a ring or other resilient methods.

Segment Your Network

Once your backbone is established, start thinking about your network the same way you think about your production equipment and processes. In other words, your network should be set up in pieces so

that that each part is controlled and wired separately from the rest of the equipment for ease of management and minimal downtime to your entire process. The first step in this process involves creating a number of small networks (called subnets), with all of a subnet's devices connected to one or more connected switches. Next, add switches with layer 3 firmware, connect each subnet to a layer 3 switch and connect the layer 3 switches to backbone switches.

If it doesn't make sense for you to keep the subnets physically separate — for example, if you would end up running two different sets of wires to the same places just to support two subnets — you can create logical networks called VLANs (virtual local area networks). VLANs share the same physical infrastructure, but act like they are separate networks. Just like subnets, you'll need to use layer 3 switches to allow one VLAN to talk to another. With this infrastructure, you can add devices and switches to your subnets, and even add entire new subnets to your infrastructure.

Specify Managed Ethernet Switches

Rather than going through control cabinets and crawling around machinery looking for blinking lights, specify managed switches throughout your network. By doing this, you'll be able to connect a computer anywhere on your network and see the status of every switch and every switch port from wherever you are.

Design for Security

Assess your cyber security risks and don't forget to think about physical security; industrial Ethernet networks can support Ethernet cameras, keypad entry devices and security software, too. A key aspect of a solid security process includes updating your policies and procedures — because some people simply forget to close and lock the door. Protect your computers with the best antivirus software and be sure to enable features that check USB jump drives, DVDs, etc. Protect your network, equipment and people by enabling the security features in the layer 3 switches between your backbone and device-level (layer 2) switches. Lock the doors on your control cabinets and turn off the unused ports on your switches. Set up the security on your wireless network. At a minimum, add firewalls with even more protection than the layer 3 switches between your production networking and your enterprise network, or to separately secure each subnet if needed. As a matter of fact, ISA 99 and IEC 62443 recommend creating small secure zones using firewalls, as described above, to prevent the spread of malware.

Industrial control security is a major topic of concern and will be for the foreseeable future. A great resource for all your questions about network security is www.tofinosecurity.com, headed by security expert Eric Byres.

Assess Your Network Capacity and Data Priority

Today's industrial Ethernet switches only use a fraction of their bandwidth. So having room on the network to adequately handle production data traffic should not be an issue. However, if you're pushing

streaming video or IP phone traffic over the network, or are concerned about a precision motion control application or that your subnet may be getting too big, get the manufacturer's specs on all of the equipment and switches on the network and do the math. Another option is to monitor the existing traffic with network management software to ensure you have plenty of headroom. Good managed switches also have a feature called quality of service (QoS) to prioritize critical traffic over less important traffic.

Choose Industrial-Grade Ratings

For the network to truly be invisible and create the least maintenance issues for you, all switches, cables and connectors need to be industrial grade and installed correctly. If you don't specify industrial grade equipment, you may well end up with "office grade" materials that will underperform and become a problem. Specify bonded pair copper, strongly consider Cat 6 and fiber for all things industrial, with shielded bonded pair copper for areas with a lot of electromechanical and radio frequency noise. Specify industrial ratings for jackets and cable connectors to protect against any chemicals, moisture, sunlight, excessive tension (e.g., when pulling through conduit), and abrasion.

Summary

Building adaptable, competitive production operations is a challenge in itself. Your industrial network should not add to this challenge; it should ease it.

These 6 points represent the key critical aspects to creating a robust, reliable industrial network that can easily be adapted to meet the expected and unexpected challenges your business will face. Equally important is the fact that, by following these guidelines, you can create a network that requires minimal maintenance and provides for easy troubleshooting.