A User's Perspective on Wired EtherNet/IP Network Architectures

Presenter - Gary Workman
Authors – John Rinaldi and Gary Workman

Premise of this presentation

- From a user perspective an EtherNet/IP network is a control system network.

- People responsible for maintaining the production equipment controlled by a control system must maintain the control system networks utilized by that control system. They are entitled to know – they need to know - the boundaries of what they are responsible for.
- Devices that aren't part of a control system should not be connected to the control system networks. Problems with them or problems created by them should not become the responsibility of production maintenance personnel to diagnose and repair.

Agenda: Questions about Control System Networks

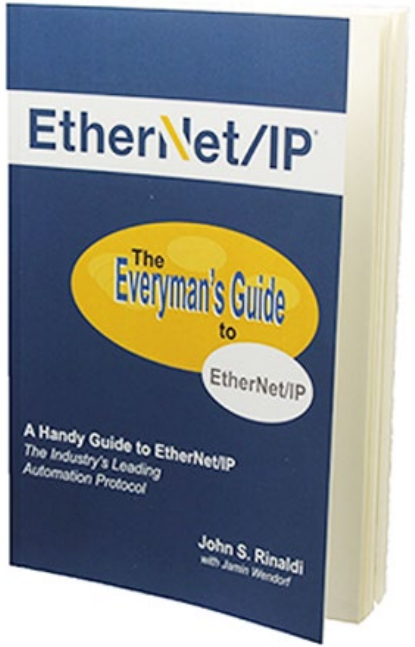
- What is a Control System Network?
- What is an EtherNet/IP Network?
- Should non-control devices be included on a Control System Network?
- What Is The Maximum Number of Nodes on EtherNet/IP Network?
- How To Architect an Efficient and High-Performing EtherNet/IP Network?
- What Are the Requirements of the Ethernet Network that hosts an EtherNet/IP network?

What is a Control System Network?

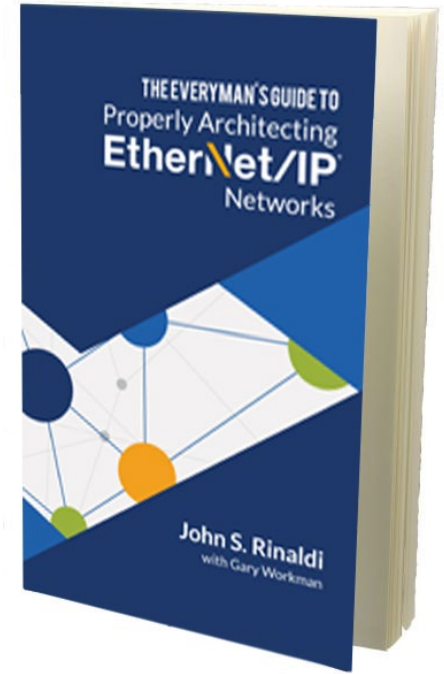
- Control Signal Data Exchange is the primary purpose of a Control System Network.
- Information sharing is the primary purpose of an Information System Network.
- Information sharing occurs on a Control System Network **ONLY** if it has bandwidth in excess of what's needed for control system signal communication.
- A Control System Network is exclusively a control network involving **ONLY** Control System devices.
- A Control System Network is an integral component of the equipment controlled by that Control System Network.

From a user's perspective: **An EtherNet/IP network is a control system network**

EtherNet/IP: The Everyman's Guide to EtherNet/IP

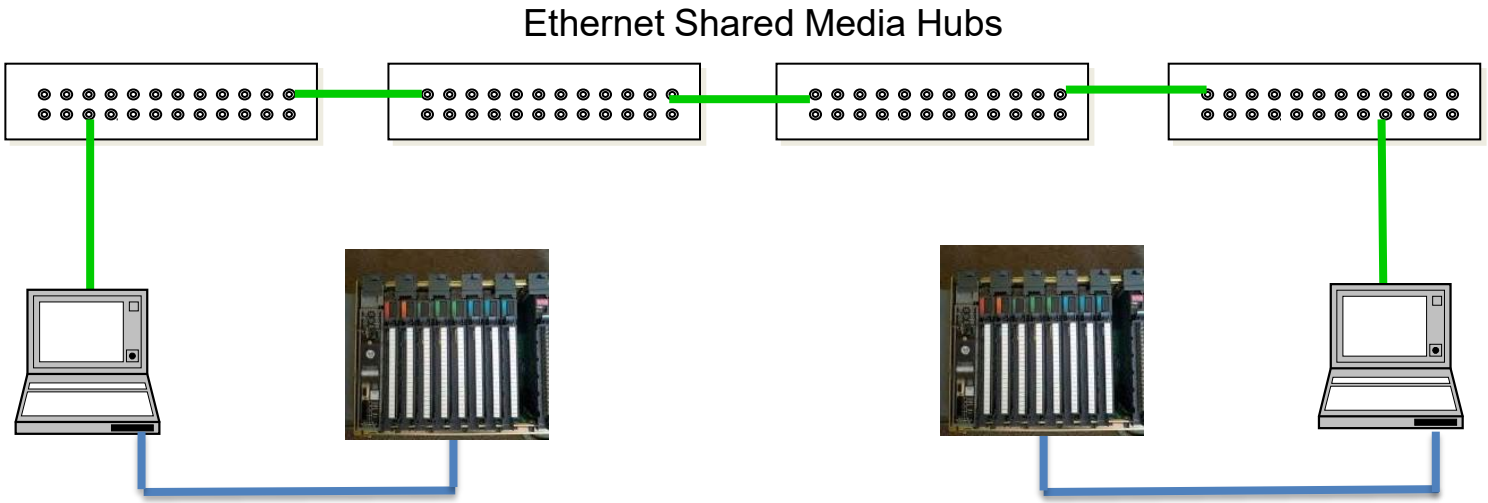


How I Spent the Covid Pandemic



What Is An EtherNet/IP Network?

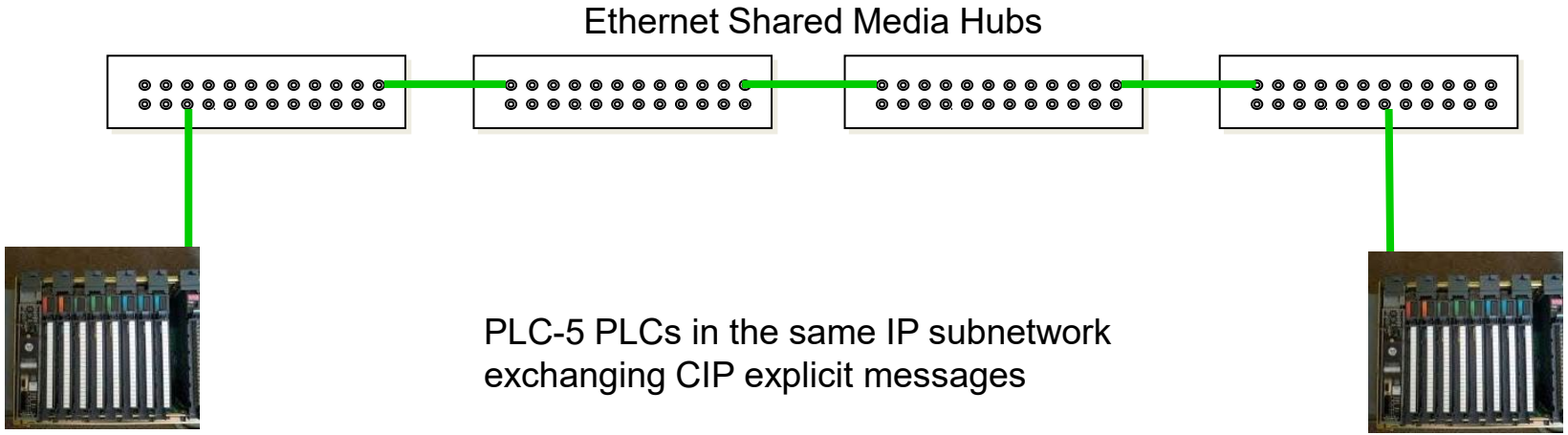
This is not an EtherNet/IP network!



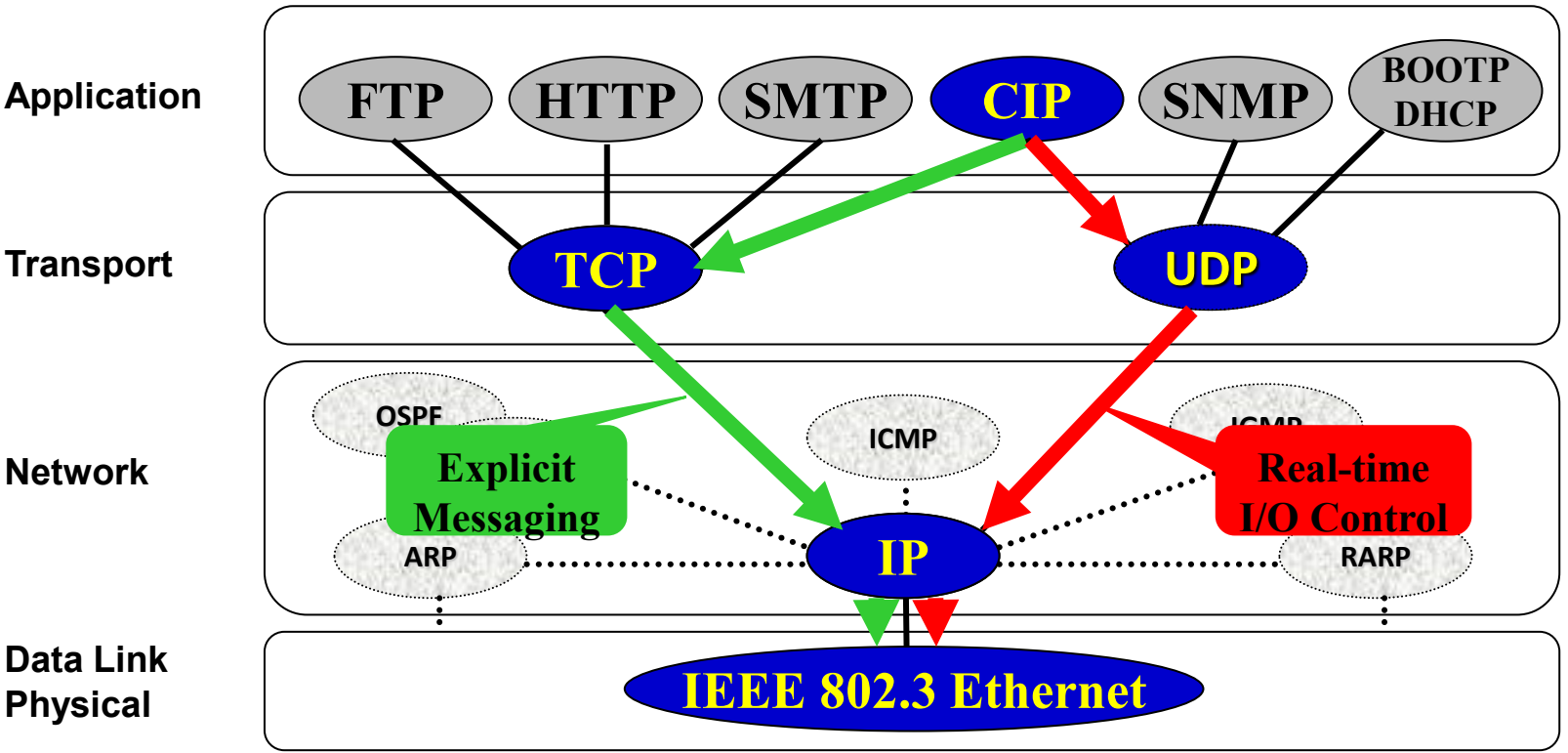
PLC-5 PLCs exchanging CIP explicit messages using ControlNet to Ethernet routers

What Is An EtherNet/IP Network?

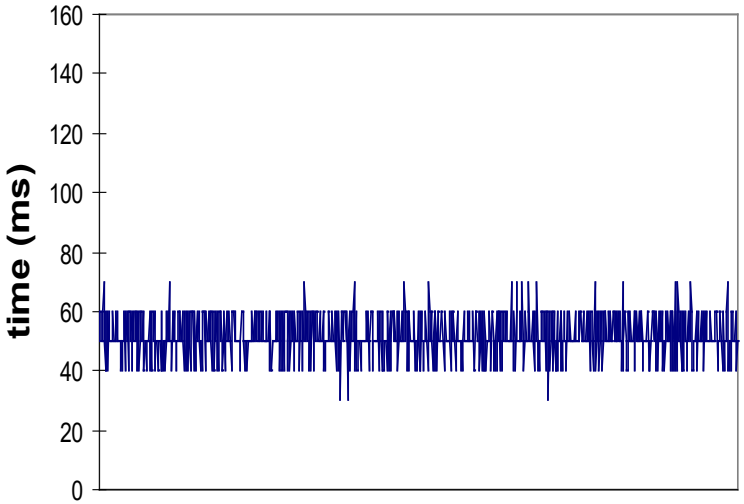
This is an EtherNet/IP network, but should it be?



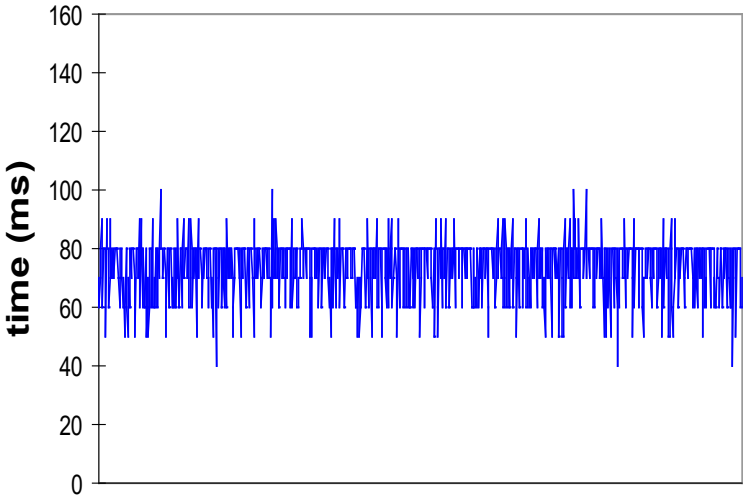
What Does The EtherNet/IP Specification Specify?



Initial PLC-5 Ethernet Performance Test Results - 1997



Ethernet Messaging Times



RIO Messaging Times

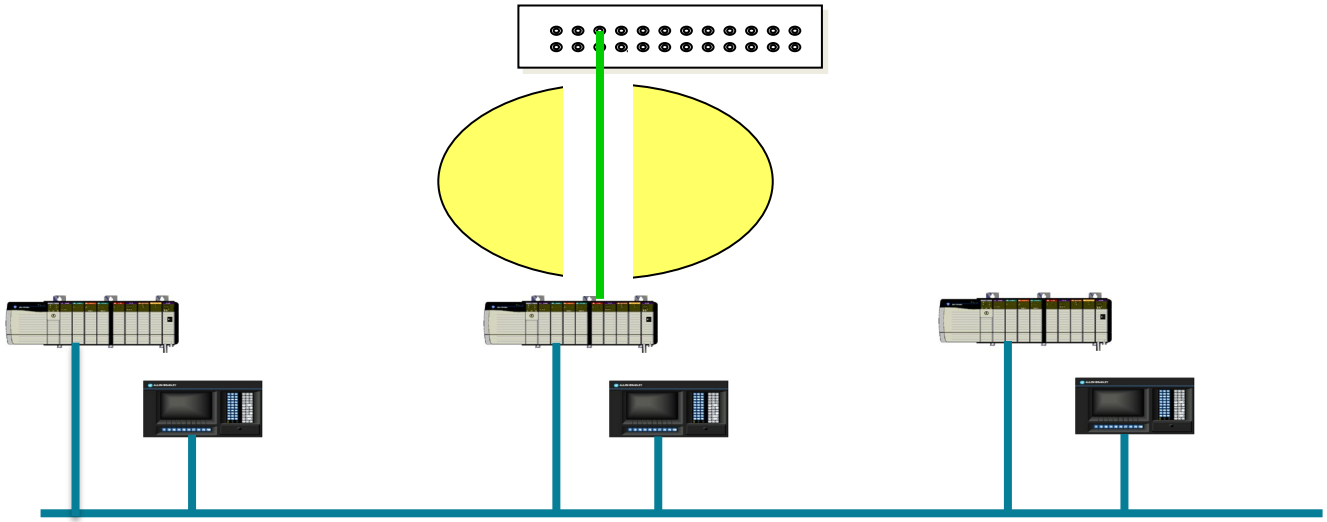
Ethernet Investigation Conclusion

"Ethernet, **if Properly Implemented**, Can Effectively Communicate Real-Time Control System Traffic"

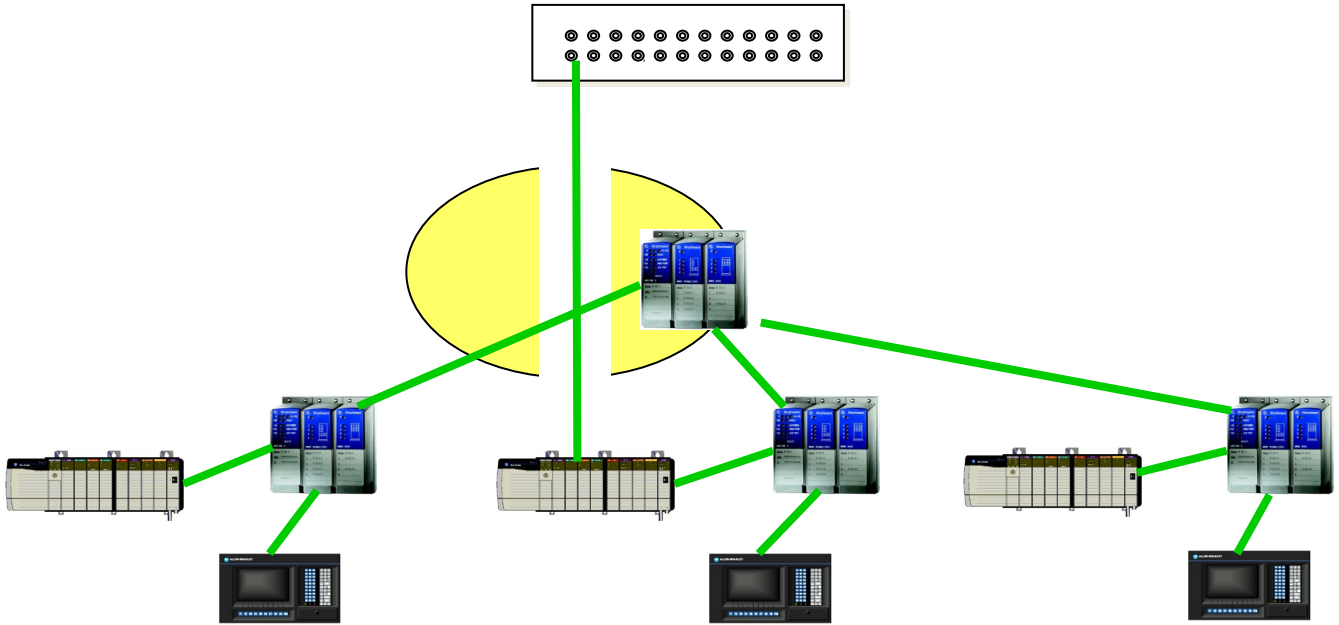
A Proper Implementation of a Control Level Ethernet Network Requires:

1. That a Device's Ethernet Network Interface Be Able to Identify and Preferentially Handle Control System Traffic.
2. The Proper Selection and Configuration of Ethernet Network Infrastructure Components

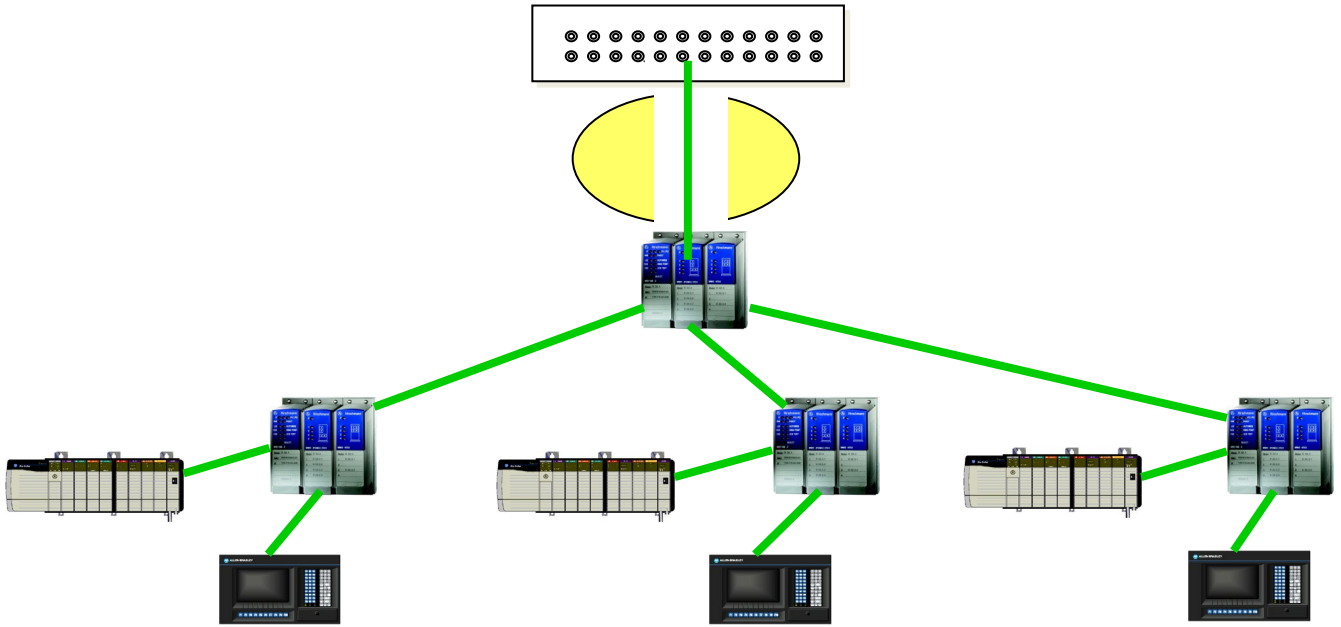
ControlNet Network to IT Ethernet Network Gateway



EtherNet/IP Network to IT Ethernet Network Gateway



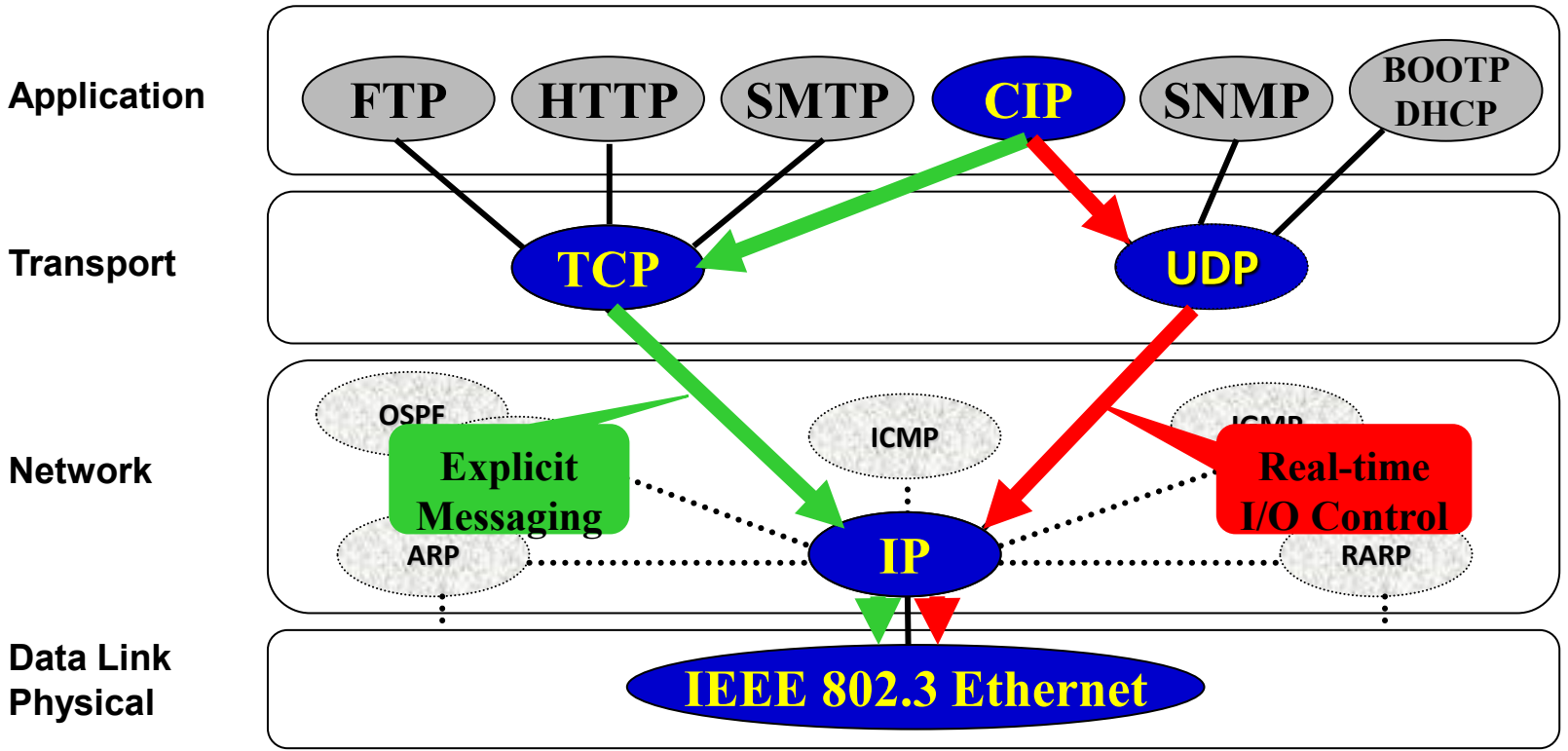
EtherNet/IP Network to IT Ethernet Network
Direct Switch to Switch Interconnection



The tremendous impact of a single Ethernet cable

- Directly connecting the infrastructure component of an EtherNet/IP network transforms it into an integral extension of the plant IT Ethernet network.
- In doing so, the EtherNet/IP network addressing policies, the network security policies, the network support policies, and the network change control policies all need to be coordinated and harmonized with the IT organization.

What is an EtherNet/IP Node?



What Constitutes an EtherNet/IP Network?

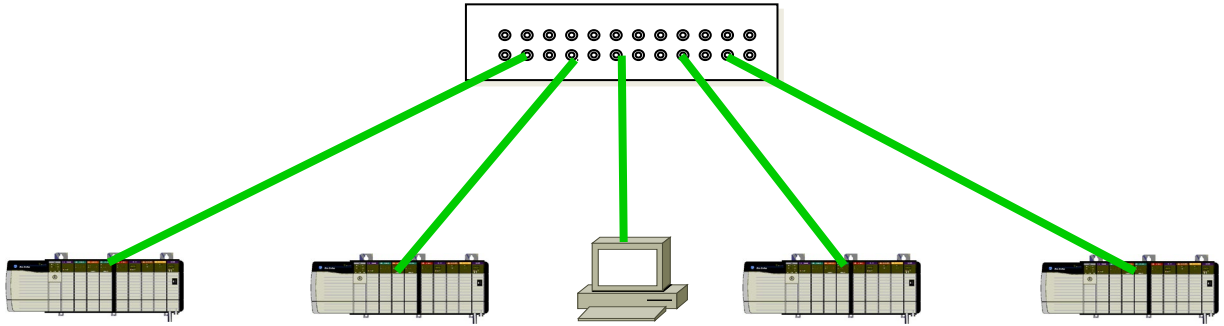
- The EtherNet/IP specifications are mute when it comes to specifying what constitutes an EtherNet/IP network. It specifies what constitutes an EtherNet/IP device, but not what constitutes an EtherNet/IP network node.
- What constitutes a network can be a nebulous concept. An internet is a network of networks. An Ethernet network can simultaneously support multiple IP subnetworks and multiple VLAN networks.
- From the EtherNet/IP specification you can surmise that an EtherNet/IP network is a collection of devices that communicate using the CIP protocol and belong to a TCP/IP subnetwork superimposed on an Ethernet network.

What Constitutes an EtherNet/IP Network?

- Are all the CIP capable end devices on the same Ethernet network members of the same EtherNet/IP network?
- Are all the CIP capable end devices in the same IP subnetwork members of the same EtherNet/IP network?
- Can end devices that are not CIP capable devices be EtherNet/IP network nodes?
- Do two CIP capable devices attached to the same Ethernet network and IP subnet, even if they never communicate with each other, create an EtherNet/IP network?
- Are non-CIP capable devices that also belong to that IP subnet and Ethernet network EtherNet/IP network nodes?

How many EtherNet/IP networks are depicted here?

Unmanaged Ethernet Switch



EtherNet/IP Capable Devices

IP Address IP Subnet Mask	**10.1.1.10** 255.255.255.0	**10.1.1.20** 255.255.255.0	**10.1.1.30** 255.255.255.0	**192.168.1.10** 255.255.255.0	**192.168.1.20** 255.255.255.0

How Large can an EtherNet/IP Network Be?

- Network size has both a geographic distance and a numerical quantity dimension.
- The broadcast “List Identity” command causes all the EtherNet/IP capable devices in an IP subnetwork to respond with a device description.
- The “List Identity” command on the first GM network with over 400 EtherNet/IP cable devices triggered a burst of broadcast ARP traffic from those devices simultaneously attempting to discover the Ethernet MAC address of the source issuing the List Identity command.

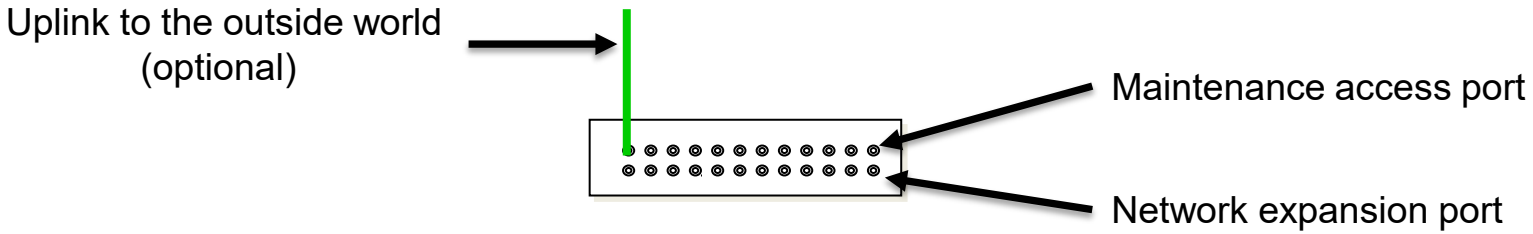
How Large can an EtherNet/IP Network Be?

- The consensus decision of the EtherNet/IP Implementors Workshop was that it is unrealistic to expect low end devices to be capable of handling such an excessive burst of broadcast traffic.
- The ODVA Conformance tests were modified to ensure that a device tolerates a burst of 250 consecutive Ethernet broadcast frames.
- GM now reserves 254 IP version 4 addresses for every EtherNet/IP network regardless of how many devices belonging to it. The identical 255.255.255.0 subnet mask is assigned to all EtherNet/IP capable devices making it extremely easy to identify the network associated with a device.

The “One Big Switch” model for EtherNet/IP network design

- Imagine if all the EtherNet/IP capable control system devices for a production tool (or a production process or a production system) could be connected to a single, non-blocking, line-speed, industrial Ethernet switch.
- By ignoring cabling costs distant devices could be connected to the imaginary switch using fiber optic cables.
- In addition to a sufficient number of ports for all the EtherNet/IP capable devices of the control system, the imaginary switch needs a few extra ports. It needs ports to occasionally host a maintenance laptop, for future network expansion, and to allow it to interconnect to the outside world.

A “One Big Switch” EtherNet/IP Network



- Any device that exclusively communicates with the outside world should not be on an EtherNet/IP network. Connect it directly to the IT network instead.
- The only non-CIP capable devices that should be allowed on an EtherNet/IP network should be devices required for the network to function if or when isolated from the outside world.
- Any device connected to the EtherNet/IP network that would generate less uplink traffic if it was connected to the IT network should be connected to the IT network.

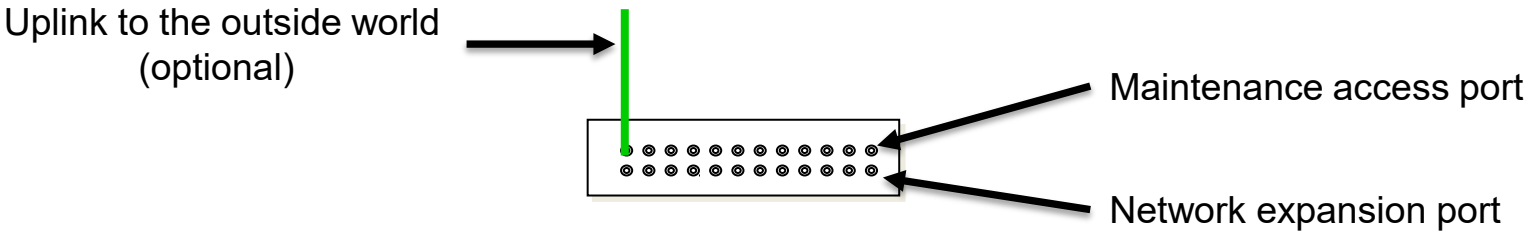
The “One Big Switch” model for EtherNet/IP network design

- The communication performance of a conceptual “One Big Switch” EtherNet/IP network exceeds that of any actual multi-switch EtherNet/IP network. It establishes an EtherNet/IP network optimum performance target.
- A “One Big Switch” EtherNet/IP network outperforms any comparable multi-switch EtherNet/IP network because the switch-to-switch links in a muti-switch network perform what would otherwise be the switch backplane interconnection of the communicating devices in a “one big switch” network.
- Striving to approach the theoretical optimum performance capability of a one big switch EtherNet/IP network is a good design approach for an actual EtherNet/IP control system network

The “One Big Switch” model for EtherNet/IP network design

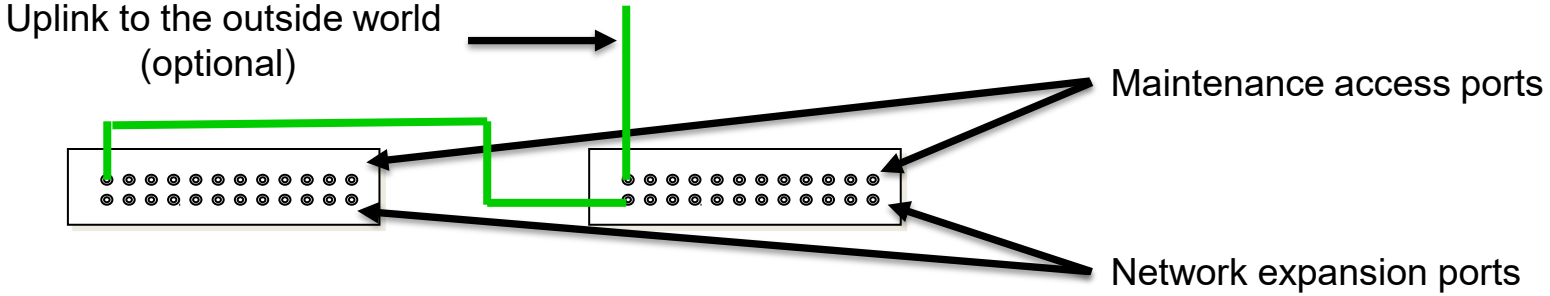
- The communication performance of a small, single switch EtherNet/IP network is identical to a “One Big Switch” EtherNet/IP network interconnecting the identical EtherNet/IP network devices running the same control programs.
- A large EtherNet/IP network becomes a multi-switch network due to practical considerations. Either the number of devices exceeds the port capacity of available switches, or the cabling costs of connecting geographically dispersed devices becomes excessive.
- Trying to best match the theoretical performance of a “one big switch” network involves maximizing the backplane utilization of the separate switches and minimizing the traffic and traffic congestion of any switch-to-switch links.

Single Switch EtherNet/IP Network



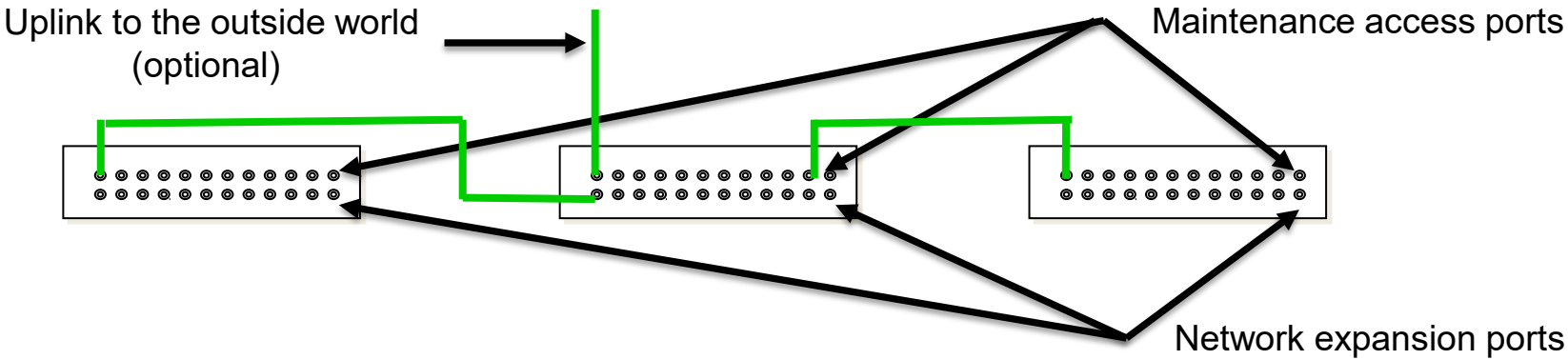
- The uplink to the outside world would be a connection to an IT network.
- Any device that exclusively communicates with the outside world should not be on an EtherNet/IP network. Connect it directly to the IT network instead.
- Any device connected to the EtherNet/IP network that would generate less uplink traffic if it was connected to the IT network should be connected to the IT network.
- The only non-CIP capable devices that should be allowed on an EtherNet/IP network are devices required for the network to function if or when isolated from the outside world.

Two-switch EtherNet/IP Network



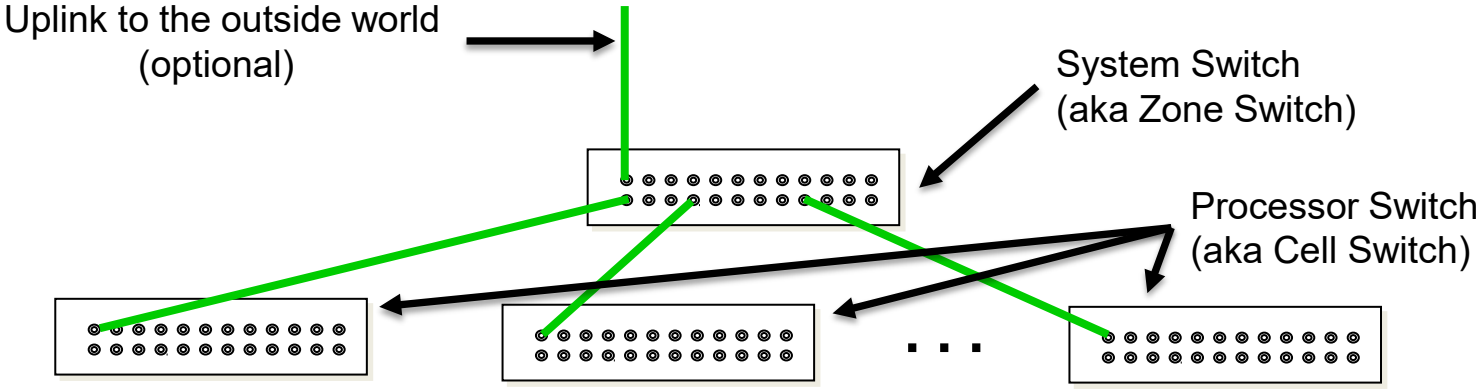
- The switch hosting devices having the most uplink traffic should be connected to the switch that is uplinked to the IT network.
- Devices should be connected to the separate switches to minimize the control signal traffic flow between the switches. This is accomplished by having controllers and the devices they control be connected to the same switch. (For GM's PLC based control system architecture, each PLC was paired with its own industrial Ethernet switch.)

Three-switch EtherNet/IP Network



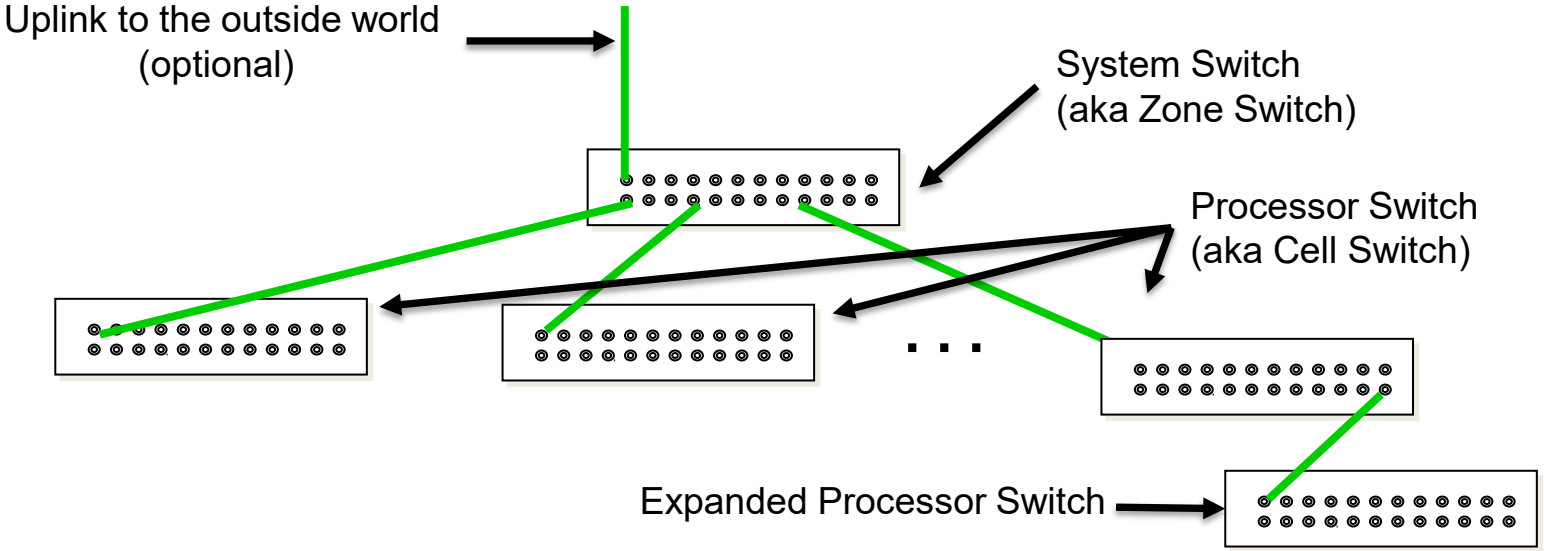
- The switch hosting the uplink to the outside world is beginning to have more ports utilized for switch-to-switch interactions leaving fewer ports for hosting end devices. For even larger EtherNet/IP networks, GM chose to dedicate a switch to performing those functions.

Typical Multi-Switch EtherNet/IP Network



- A system switch interconnects the processor switches together and (if appropriate) interconnects the EtherNet/IP network to the outside world.
- A processor switch interconnects a PLC with all the EtherNet/IP capable equipment controlled by that PLC.

Typical Large Multi-Controller Multi-Switch EtherNet/IP Network



- If a processor switch has an insufficient number of ports, it gets expanded into a multi-switch processor switch using the same minimize the switch-to-switch control signal traffic philosophy.

Two distinct levels of control system networks

- Controller level Ethernet based control system networks use traditional Ethernet switches.
- Ethernet based I/O level networks using traditional switched Ethernet switches and cabling are expensive when compared to alternative I/O level network technologies.
- Device Level Ring (DLR) technology utilizing embedded switches was developed to address I/O device level network costs and other requirements.

Interconnecting Two EtherNet/IP Networks

- If you are exchanging control signal traffic between EtherNet/IP networks, the ideal case is to have them be directly linked by a line speed, non-blocking Ethernet to Ethernet network router.
- GM encouraged Ethernet Switch manufacturers to consider adding a single hop Ethernet to Ethernet static routing capability to their layer 2+ industrial Ethernet switches. The feature is limited to static routing of traffic between a few hundred devices.

Connecting an EtherNet/IP Network to the Outside World

- An EtherNet/IP network should be both Ethernet broadcast traffic and Ethernet multicast traffic insulated from the outside world.
- Minimize the attack surface to a control system network for cybersecurity reasons. Having both a real time network interface and a non real time network interface to a control system device puts both networks at greater risk.
- The best way to connect an EtherNet/IP network to the outside world is by using an IP network router directly connected to the EtherNet/IP network.
- A reasonable alternative is to have it be directly connected to an Ethernet switch with the EtherNet/IP network being an explicitly designated VLAN of the Ethernet network.

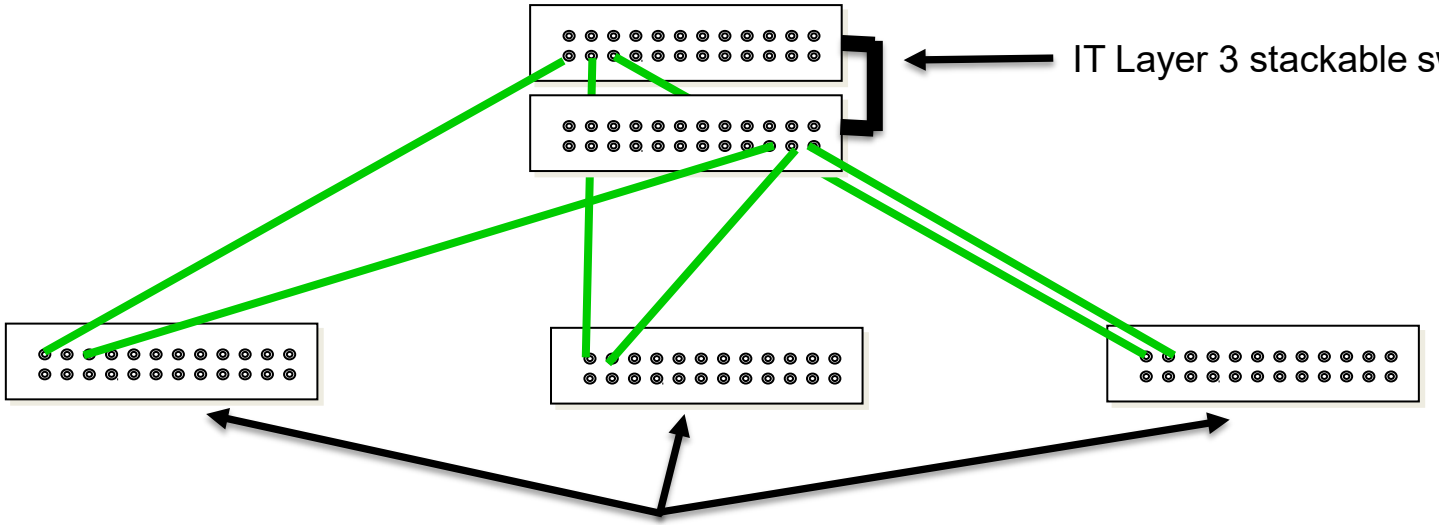
Connecting an EtherNet/IP Network to the Outside World

- GM only uses company private IP addresses for EtherNet/IP network devices.
- The outside world for a GM controller level EtherNet/IP networked device is restricted to devices in the GM plant that houses that EtherNet/IP network.
- The only direct interactions a GM controller level EtherNet/IP network device has with outside world devices not inside the local GM plant is via a security server that is inside that plant.
- The outside world for a GM I/O level EtherNet/IP network is strictly limited to a few devices on the controller level EtherNet/IP network it is connected to that are allowed to access it and know how to statically route traffic to it.

GM requirements for EtherNet/IP control traffic exchanges across the plant IT network

- Fully switched Ethernet infrastructure with redundantly powered, stackable Ethernet switches with multiple interface modules.
- Redundant path Ethernet infrastructure.
- Infrastructure QoS support for preferentially handling control signal traffic if/when network becomes congested.
- Network management support to assure redundant path availability

Layer 3 Switch Routing of EtherNet/IP Control Signal Traffic



"One Big Switch EtherNet/IP Networks

Summary

- The EtherNet/IP specifications define an EtherNet/IP device. They allows for a very open-ended definition of what constitutes an EtherNet/IP network.
- From a user perspective, EtherNet/IP devices only have utility in the context of an EtherNet/IP network.
- From a user perspective: an EtherNet/IP network is a control system network and a control system network is exclusively a control system network.
- From a user's perspective, there are Ethernet networks that are extremely poor foundations for a control system network and there are Ethernet capable devices that don't belong on control system networks.
- From a user's perspective, the EtherNet/IP specifications should not allow these situations to exist in EtherNet/IP control system networks.
- Users would benefit from the further specification of what constitutes a well designed EtherNet/IP control system network.

Thank You For Attending

QUESTIONS?

Proposal

- ODVA should consider specifying the definition of and defining the requirements for wired EtherNet/IP control system networks.