Single hop inter-VLAN routing – a capability that EtherNet/IP I/O can take advantage of – a feature that suppliers of advanced, managed, industrial Ethernet switches should consider implementing

Gary Workman
General Motors– Manufacturing Engineering Vehicle Systems

Presented at the ODVA
2014 ODVA Industry Conference & 16th Annual Meeting
March 11-13, 2014
Phoenix, Arizona, USA

Abstract

Companies contemplating the wide spread adoption of Ethernet I/O networks will quickly encounter the problem of how to segment their industrial Ethernet networks. Even for a small manufacturing concern, a facility-wide Ethernet network will be segmented into multiple physical or logical Ethernet network segments. A related problem then becomes how to enable devices on different Ethernet network segments to communicate with each other.
This paper will discuss the preferred network architecture that GM Vehicle Systems intends to pursue for segmenting EtherNet/IP control level and EtherNet/IP device level networks as it begins the process of migrating DeviceNet I/O networks to EtherNet/IP I/O networks. The proposed architecture will route EtherNet/IP implicit message traffic between controllers and the EtherNet/IP capable I/O devices controlled by those controllers. To realize the proposed architecture in a cost effective manner, General Motors will need industrial Ethernet switch suppliers to support a single hop inter-VLAN routing feature.

There is a distinct difference between switching and routing Ethernet traffic. Switching is an ISO/OSI reference model layer 2 activity while routing is an ISO/OSI reference model layer 3 activity. Switching occurs between devices on the same logical network. Routing occurs between devices on different logical networks.
A single hop inter-VLAN routing feature provides line speed routing between devices that would otherwise be using line speed switching, but can't because the devices belong to different logical Ethernet networks. It is the feature of a true layer 3 switch that remains when you minimize its routing functions to only support the most trivial form of Ethernet network to Ethernet network routing possible.

GM Vehicle System's Current Situation

GM started out designing EtherNet/IP networks as controller level control system networks. As GM is contemplating the transition from DeviceNet I/O to EtherNet/IP I/O, the need to segment EtherNet/IP networks into multiple EtherNet/IP network segments has become readily apparent. There are simply not enough unused IP addresses in currently deployed EtherNet/IP networks to assign to all of the I/O devices on all of the equipment controllers. GM is not unique. Other companies contemplating the wide spread adoption of Ethernet I/O networks will quickly encounter the problem of how to segment their industrial Ethernet networks.

GM has a PLC-centric control system architecture for the vast majority of vehicle assembly plant automated equipment. An industrial Ethernet switch is directly associated with every PLC and interconnects that PLC with all of the EtherNet/IP capable robot controllers and process controllers that are coordinated by that PLC. This switch is called a processor switch. If, including the PLC, there are more Ethernet capable devices in the span of control of a single PLC than ports available on the processor switch, one or more additional industrial Ethernet switches are cascaded off the processor switch as necessary.

Frequently there are a cluster of PLCs controlling the tooling that processes a common part, and where there are, the separate processor switches are uplinked to an industrial Ethernet switch termed a system switch. (See figure 1.)

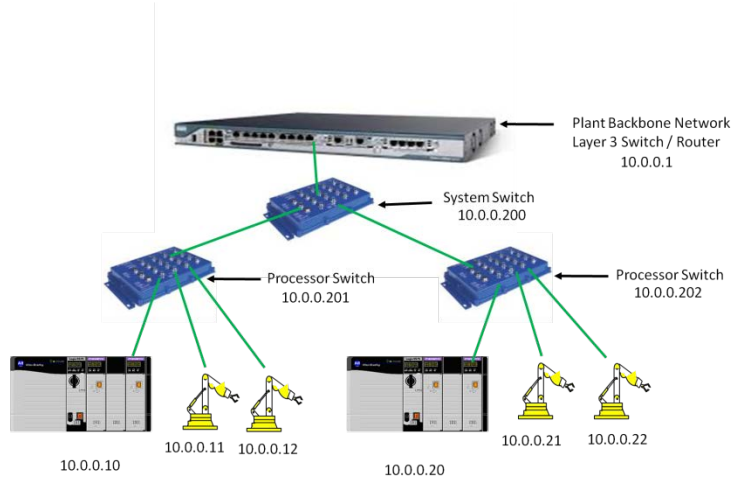

Figure 1: GM's PLC centric EtherNet/IP network architecture

In GM's EtherNet/IP network designs today, the industrial Ethernet switches and all of the equipment attached to them share a common network address range and no EtherNet/IP network has more than 250 devices. A decade long experience with implementing EtherNet/IP networks for automotive assembly plant tooling has demonstrated that very few EtherNet/IP networks should be, or need to be, larger than 250 nodes in size.

An absolute design limit of 254 nodes is imposed on GM's EtherNet/IP networks today. Problems were experienced with background Ethernet broadcast traffic on some of the early EtherNet/IP networks initially installed that were larger than that. Now, for consistency, an IP subnet mask of 255.255.255.0 is universally used for every EtherNet/IP capable device.

The maximum size of a logical EtherNet/IP network is a key concept for this paper. The ability of the least capable device to tolerate random background broadcast traffic is one theoretical determinant of the maximum size network that device should belong to. Years ago, working with the ODVA EtherNet/IP Implementor Workshops, the guideline that a reasonably capable EtherNet/IP device should be able to tolerate a nominal "burst" of ARP (address resolution protocol) broadcast traffic was established. Actual broadcast traffic recorded from a GM production network with 200 devices reacting to a broadcast EtherNet/IP command from a diagnostic laptop just added to the network was used to determine the characteristics of the nominal burst of ARP broadcast traffic.

As part of that investigation, the broadcast traffic control features available on Ethernet switches were enabled in an effort to minimize the effects of the broadcast traffic. While those features are effective at restricting or eliminating a continuous stream of broadcast traffic, the reaction time of those types of broadcast traffic filters is a significant fraction of a second or longer. Intense, short duration bursts of legitimate broadcast traffic were unaffected by the switch broadcast traffic control features and were propagated throughout the network.

The easiest way to grow a network is to simply add devices to the network. That can be done until you run out of IP addresses for the network. Expanding the maximum size of an existing network requires reconfiguring the IP address of every current member of that network and also expands the broadcast domain of that network.
In GM's EtherNet/IP networks today, all of the PLCs and all of the robot controllers have DeviceNet I/O networks. If every DeviceNet capable device today was replaced with an EtherNet/IP capable device, the EtherNet/IP networks would have to become approximately 10 times larger than they are today, or there would need to be at least 10 times more of them. GM's choice is to keep the existing size limitation for an EtherNet/IP network and increase the number of them.

Today, when control system engineers want to deploy a larger than standard size EtherNet/IP network, they are required to break the theoretically larger network into two or more appropriately sized EtherNet/IP networks. The separation is designed to result in having the minimum number of real-time control traffic exchanges between the

multiple alternative networks. Expanding the maximum size of an existing network is not an action that would be seriously considered.

Two different techniques for exchanging EtherNet/IP real-time traffic between PLCs on different EtherNet/IP networks are supported. If the EtherNet/IP networks are physically close to each other, an additional Ethernet interface card can be added to one of the PLCs and addressed to have that PLC become a member of both EtherNet/IP networks. The new Ethernet interface card is given an unused IP address from the other EtherNet/IP network and connected to an industrial Ethernet switch in the other EtherNet/IP network. (See figure 2.)

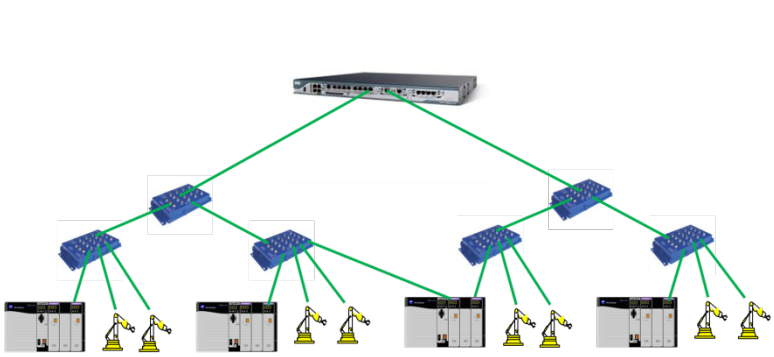

Figure 2: Communicating EtherNet/IP implicit message traffic between EtherNet/IP networks
Option 1: Having a PLC belong to both networks

The second technique used works even when the EtherNet/IP networks are distantly remote from each other. GM's EtherNet/IP networks uplink to the IT plant backbone Ethernet network using a commercial grade layer 3 switch. The second techniques for exchanging EtherNet/IP real-time traffic between PLCs on different EtherNet/IP networks is to simply route (unicast) EtherNet/IP real-time traffic across the plant IT backbone Ethernet network. (See figure 3.)

It is with a healthy dose of irony that the term "simply" is used in the prior sentence. Years of time and man-years of effort have been invested ensuring that routing EtherNet/IP implicit message traffic across the IT plant network infrastructure is an appropriate and reliable means of implementing long distance control traffic exchanges between PLCs.

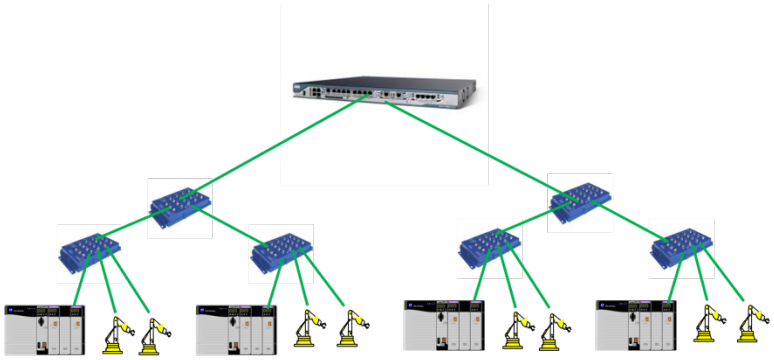

Figure 3: Communicating EtherNet/IP implicit message traffic between EtherNet/IP networks
Option 2: Routing EtherNet/IP implicit message traffic through the plant backbone network

In comparing the two techniques, it is quickly discovered that routing EtherNet/IP implicit message traffic is the easier and more cost effective method to use. The one PLC becoming a member of multiple EtherNet/IP networks technique requires an extra PLC Ethernet interface card and its associated IP address, consumes extra industrial Ethernet switch port, and needs an extra cable to be installed (for connecting the extra interface card to the extra switch port).

Meanwhile, trusting the IT plant backbone network to route EtherNet/IP traffic between EtherNet/IP networks consumes an infinitesimal amount of bandwidth and incurs a few tens of microseconds in extra switch hop delays at the cost of configuring a new EtherNet/IP connection - a configuration effort that is required when using either technique. It should be noted that the routing technique – without extra effort - only supports unicast EtherNet/IP communication, and that the extra switch hops do involve a slightly (trivially) higher risk of communication disruption. (See figure 4.)

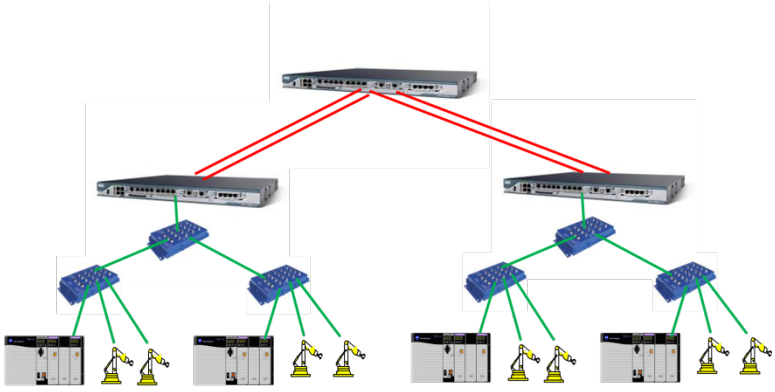

Figure 4: Communicating EtherNet/IP implicit message traffic between EtherNet/IP networks
Option 2: Routing EtherNet/IP implicit message traffic through the plant backbone network

Background - Switching vs. Routing Ethernet traffic

There is a significant difference between switching and routing Ethernet traffic. Switching is an ISO/OSI reference model layer 2 activity while routing is an ISO/OSI reference model layer 3 activity. The layer 2 protocol data unit is termed a frame while the layer 3 protocol data unit embedded within a frame is called a packet.

Switching occurs between devices on the same logical network. Routing occurs between devices on different networks. Routing is used for communication even between different logical networks utilizing the same communication technology. (See figure 5.) Adding to some of the terminology confusion, routing between two Ethernet networks is frequently called layer three switching.

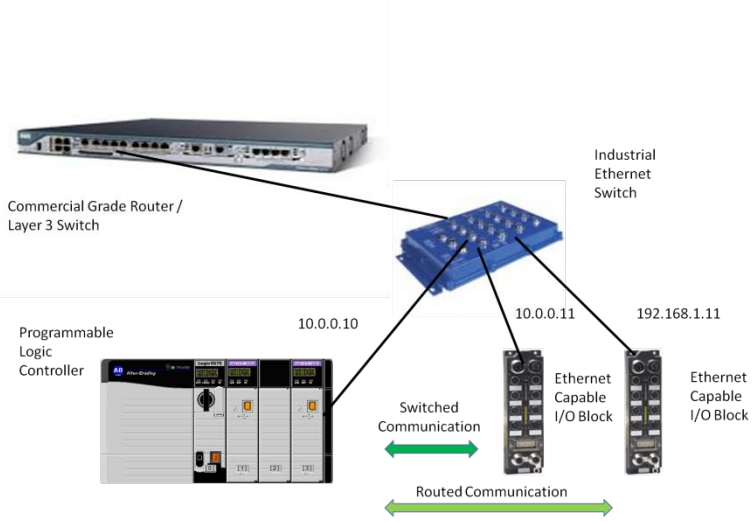

Figure 5: Introducing the difference between switched and routed communication (notice the device IP addresses)

On a switched (ISO layer 2) Ethernet network, a device wanting to communicate with another device on the same network embeds an IP packet addressed to the other device in an Ethernet frame also addressed to the other device, and transmits that frame to the destination device. (See figure 6.) If the device needs to communicate with a device on a different Ethernet network, it embeds an IP packet addressed to the other device in an Ethernet frame addressed to a router on its own network, and transmits the frame to that router. (See figure 7.)

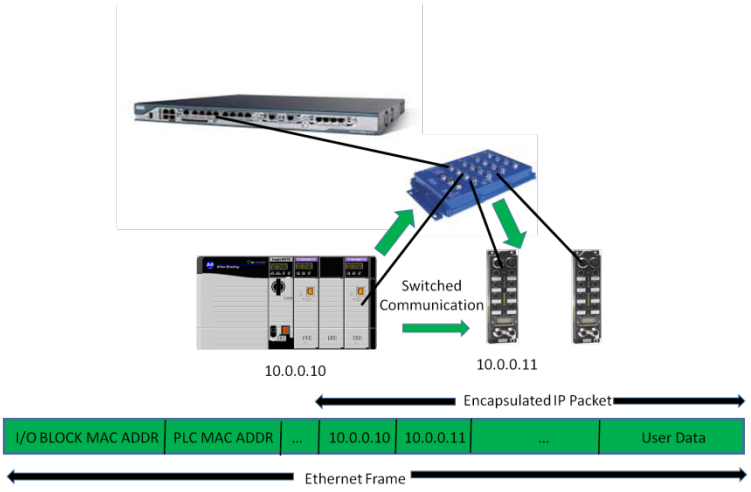

Figure 6: Switched communication – communicating devices belong to the same logical Ethernet network

A switch uses the destination Ethernet address of an incoming frame to process that Ethernet frame. The switch ignores the IP packet destination address in the Ethernet frames that it receives.

A router owns the destination Ethernet address of an Ethernet frame delivering an IP packet to it. It processes the packet based on the IP destination address - as well as other data contained in the IP packet header.

Consider the situation where the originator and the destination devices involved in an instance of communication are both connected to the same Ethernet switch. The switch simply forwards the Ethernet frame received from the originating device to the port that it has learned is servicing the destination device PROVIDED THAT both devices are members of the same logical Ethernet network.

When the originator and destination devices involved in an instance of communication are both connected to the same Ethernet switch but are not members of the same logical Ethernet network, the switch

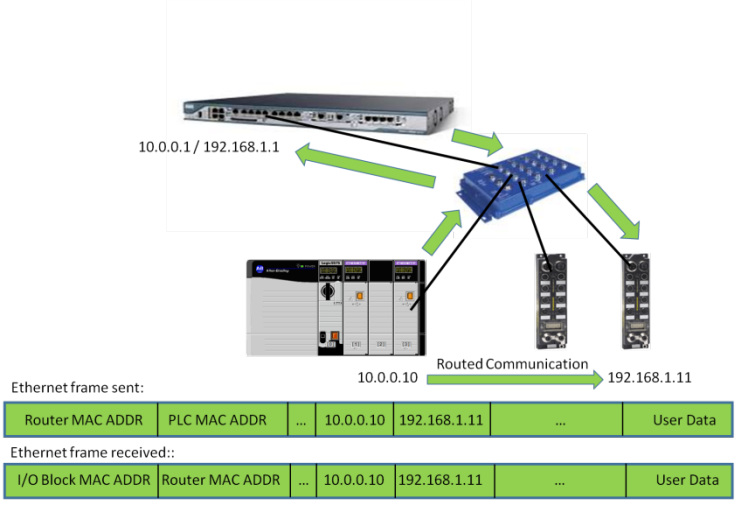

Figure 7: Routed communication – communicating devices belong to different logical Ethernet networks

forwards the Ethernet frame received from the originating device to a switch port servicing a router needed to route the user data (being transported within the frame) to the different Ethernet network. That router will use the IP address of the destination device to determine that the user data has to be sent (back) to the switch that is hosting the destination device. The switch will subsequently receive a newly created frame from the router (containing the user data sent from the originating device) and forward it to the port that services the destination device. This extra processing and redundant message handling will occur even though the switch is directly hosting both the originator and destination devices. The amount of extra processing, and extra bandwidth utilization needed to deliver the information will increase as the number of switches between this switch and the router grows.

This situation – Ethernet capable devices connected to the same Ethernet switch that frequently communicate with each other but belong to different logical Ethernet networks – will likely occur more often with the growth of Ethernet I/O networks. A second contention is that many of the devices on industrial Ethernet I/O networks will only want or need to communicate with devices in close proximity to themselves.

Proposal

One possible solution to the situation described above would be to replace the Ethernet switch in the scenario with a layer 3 switch (A.K.A. a routing switch). The layer 3 switch switches when it can, but it is also an optimized router specifically designed for routing traffic between Ethernet networks.

Because a layer 3 switch is a router, it is both more complex than a (layer 2) switch to configure and more expensive than a (layer 2) switch to procure. Complex and expensive are two attributes that people adopting and implementing Ethernet I/O networks try to avoid.

A useful capability would be for the Ethernet switch in the scenario described above to support an advanced feature that can best be characterized as single hop, inter-VLAN routing. This feature would provide line speed routing between devices that would otherwise be using line speed switching - if only both devices were members of the same logical Ethernet network. Single hop inter-VLAN routing is the feature of a layer 3 switch that remains when you minimize its routing functions to only support the most trivial form of Ethernet network to Ethernet network routing possible. (See figure 8.)

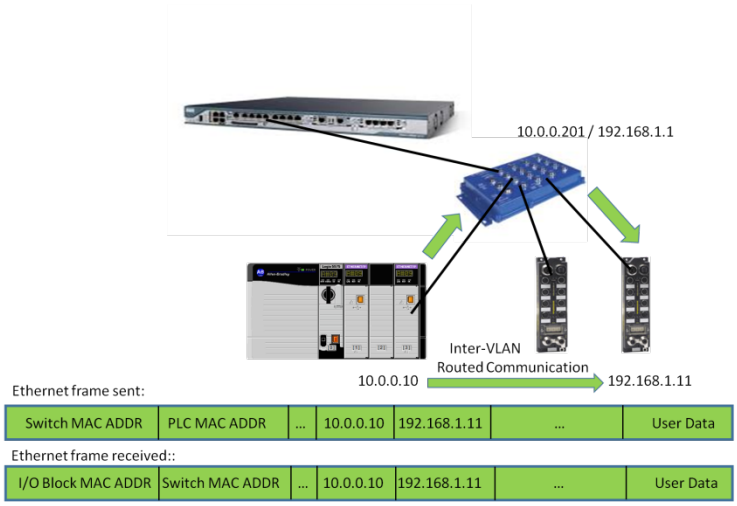

Figure 8: Routed communication via switch with single hop inter-VLAN routing feature

For a router routing IP traffic between similar Ethernet networks, four fields of a received frame are modified in the process of routing that frame. The IP TTL (Time to live) field is decremented by one indicating that the packet has been processed by the router. As a result of that change, the IP header checksum needs to be recalculated. The other two changes are to the source and destination MAC address fields. The destination MAC address field of a frame delivered to a router is the router's MAC address. That address replaces the previous MAC source address and becomes the source MAC address of the new frame that is sent from the router. A new "next hop" MAC address determined by the router from performing its routing function becomes the destination MAC address of the newly modified frame being sent from the router. A single hop inter-VLAN router needs to modify these four fields when it performs its routing function.

For a single hop inter-VLAN router feature, the "next hop" MAC address needs to be the destination device MAC address. If not, the router would be participating in a multi-hop routing scenario. One key exception to the single hop rule is for the inter-VLAN routing function of the VLAN that the switch management entity belongs to. In that specific case, the switch has awareness of its own default gateway. It is therefore able to route any traffic delivered to it from other devices on its own Ethernet network destined for a network it is not able to provide inter-VLAN routing services for. It forwards those packets to its default gateway.

The way to activate a single hop inter-VLAN routing capability on a switch is to define virtual router interfaces for the VLANs serviced by the switch that you want to route between. A virtual router interface is created by assigning the switch an unused address from the VLAN address range and specifying the subnet mask for that VLAN. If there is no default gateway provided for the virtual router interface, the only thing that can be done with traffic addressed to an unknown destination address is to discard it. In effect, if a destination device can not directly respond to an ARP request issued by the switch, a single hop routing function on that switch will be unable to route traffic to that device. The final configuration task is to identify which ports are supporting devices from which VLANs.

End devices that are serviced by the switch take advantage of the routing capabilities of the switch by specifying one of the switch's virtual router interfaces to be the gateway device address in the end device's IP address configuration.

A concrete addressing example:

Design a GM style EtherNet/IP system level network using the 10.0.0.xxx IP addressing range. Configure every industrial Ethernet switch in the system level network be members of that address range. Have every industrial Ethernet switch be capable of single hop inter-VLAN routing. Configure each industrial Ethernet switch to have its IP address also be a virtual router interface address for the 10.0.0.xxx network. Configure the address 192.168.1.1 to be a virtual router interface address for a 192.168.1.xxx network in every switch. With this common configuration in each switch, every switch is capable of supporting an independent EtherNet/IP I/O network with a 192.168.1.xxx addressing range.

In this example, with controllers connected to separate single hop inter-VLAN routing switches, each has access to its own range of IP addressable I/O devices, but the I/O devices controlled by separate controllers can have identical IP addresses. (See figure 9.)

In this example, a PLC can communicate with the 192.168.1.xxx addressed I/O devices directly connected to its processor switch, and only with the I/O devices connected to its processor switch. Note that the I/O devices can send unidirectional information to any end device on the 10.0.0.xxx network, but can only communicate in a bi-directional fashion with the 10.0.0.xxx addressed devices that have the address of their local processor switch listed as the gateway device address in their IP address configuration.

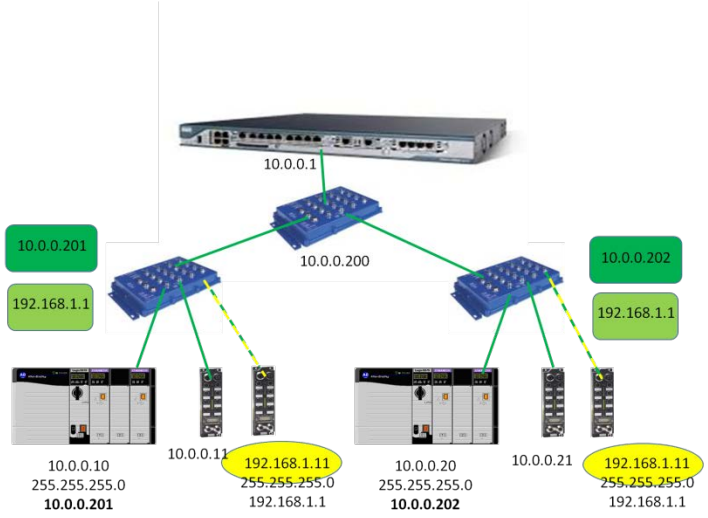

Figure 9: End devices take advantage of the single hop inter-VLAN routing feature by having their default gateway addresses point to a virtual router interface configured on the switch.

There is a strong user desire to be able to utilize identical Ethernet I/O networks for identical machines, even to the extent of using identical addresses for the I/O devices on those machines. With identically addressed I/O devices, a single control program can be copied and used by multiple machines. The identical program works on multiple machines because the machine controller is the master device and it initiates communication with the (slave) I/O devices. This communication behavior allows the separate machine controllers to have unique IP addresses while the I/O devices on the different machines have identical I/O addresses.

Advantages of the single hop inter-VLAN routing feature:

Single hop inter-VLAN routing offers a limited, local routing capability. It allows limited access private networks to be built. The SNMP traffic statistics collected by the switch for ports that are supporting private networks are available for remote monitoring and management support of the private network.

Limitations of the single hop inter-VLAN routing feature:

Only unicast EtherNet/IP traffic can be routed using this feature. Traffic is routed only for end devices that specify a pre-defined routing interface address configured on the switch as the gateway address in their IP addresses configuration.

Alternatives to the single hop inter-VLAN routing feature:

There are multiple alternatives to a managed switch implementing the single hop inter-VLAN routing feature for communicating with privately addressed networks. A hypothetical alternative would be for the controller Ethernet interface card to simultaneously support multiple IP addresses on the same Ethernet interface. No equipment controller supplier offer, or even appear to be considering the idea of offering this feature.

One obvious alternative is to replace the advanced layer 2 switch with a true layer 3 switch. However, that solution requires universally unique end device addresses. Also, wanting to avoid the expense and complexity to both install and operate a layer 3 switch is what led to exploring the minimalist router proposal in the first place.

A second alternative is to have the I/O network be a truly isolated Ethernet network rather than a logically segregated, partially isolated network. The truly isolated networks require separate Ethernet interfaces on the controller for each network it belongs to. Troubleshooting problems involving an isolated network can only occur by utilizing devices attached to the isolated network. This solution is not available for controllers that don't support multiple Ethernet interfaces.

The idea for the single hop inter-VLAN router feature grew out of the frustration of trying to develop an Ethernet I/O network architecture for a PLC with a single Ethernet interface. Desire for it grew with the recognition that there were potential cost savings in reducing the number of Ethernet interfaces required even on a PLC that supports multiple Ethernet interfaces.

A third alternative is to expand the maximum allowable size of the network. This is potentially difficult to do with an existing network. The IP addresses of every device in the existing network need to be reconfigured. The 'new' network addresses to be used in the network expansion may already be in use elsewhere and have to be recovered. You also need to ensure that every device in a very large Ethernet network can tolerate the worst case background broadcast traffic conditions experienced by the network.

A forth alternative is to use a Network Address Translation (NAT) gateway. The NAT gateway exposes some devices on the private network to the outside world while simultaneously making devices from the outside world appear to be local devices on the private network. One drawback of the NAT gateway is that devices serviced by the gateway have multiple IP addresses – a device is known by a different IP address by devices on different sides of the gateway. Cascaded NAT gateways can become very difficult to manage.

Examples of each of these alternative styles of Ethernet I/O networks will likely be implemented in different situations by different companies. Truly isolated private Ethernet I/O networks will probably be extensively implemented, at least initially. Isolated, private networks require the minimum amount of coordination and advanced planning. Unfortunately, that network design also results in the greatest amount of device isolation. The single hop inter-VLAN feature proposed here offers interesting possibilities for EtherNet/IP based I/O network designs if industrial Ethernet switch suppliers choose to implement it.

It is possible to extend the scope of a privately addressed VLAN by combining the idea of single hop inter-VLAN routing with the idea of trunking that VLAN between multiple switches. To minimize any communication path inefficiencies in routing traffic to and from that VLAN, each of the switches supporting devices that need routing services for that VLAN should also support a virtual router interface for that VLAN. Note that in doing this, every virtual router interface implemented in the VLAN consumes a unique IP address from the IP address subnet range of that VLAN. (See figures 10 and 11.)

Today, a typical machine control I/O device only needs to communicate with at most a few devices, control messages exchanges with a controller being the most important of those communications. For most I/O devices, most communication to anything other than the controller will be to devices located in reasonably close proximity to it.

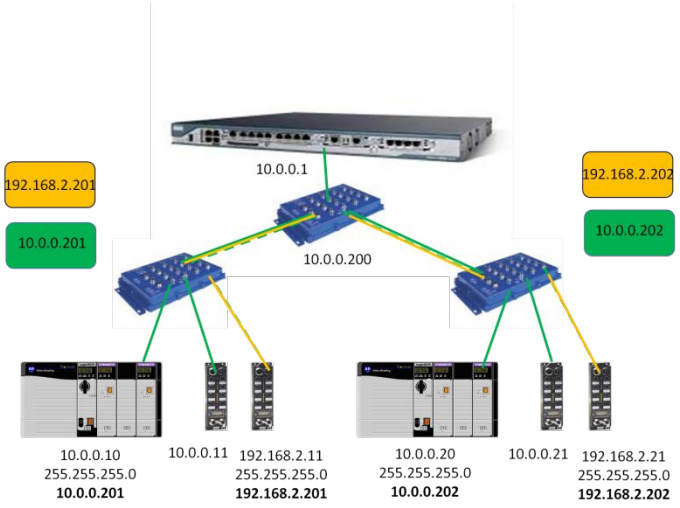

Figure 10: Combining single hop inter-VLAN routing with trunking VLAN traffic between switches

A legitimate and reasonable question to ask is: "What is the value in assigning a globally unique IP address to an I/O device?" For the overwhelming majority of I/O devices in the overwhelming majority of circumstances, the answer is: "Nothing". The nearly universal case today is that there are extremely few devices that need to or would benefit from communicating with any random EtherNet/IP capable I/O device. There are also numerous reasons for isolating and/or securing an I/O device so that it is only able to communicate with at most a few other devices.

What devices need to communicate with a typical I/O device? Conversely, which devices does a typical I/O device have legitimate and productive reasons for communicating with? The controller (obviously) has a need to talk to an I/O device. An I/O device could reasonably be expected to communicate with a network monitoring application and/or occasional network troubleshooting tool, or maybe a time server, a name server, or an address server. More sophisticated devices might also be expected to communicate preventative maintenance information to a maintenance server.

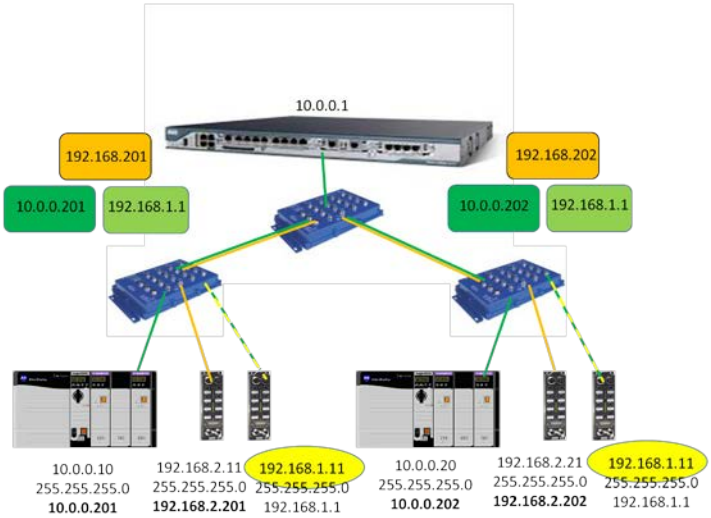

Figure 11: Combining single hop inter-VLAN routing with trunking VLAN traffic between switches

Historically, on proprietary control networks, I/O devices only communicated with their controller. Now, even with the Internet of Things, if there is a need for communicating with distantly remote devices it will likely take place through a local security server.

For GM tooling applications today networked I/O devices use DeviceNet. From a communication perspective, they communicate to their controller using the pre-defined master/slave connection. Early in their operational life they may have talked to a laptop computer to exchange configuration information. They also may infrequently communicate low priority explicit message traffic with a diagnostic support tool. Overall, that type, level, and method of communication is doing a reasonable and productive job.

The idea of converting from DeviceNet I/O to EtherNet/IP I/O will not be an appealing proposition if it will cost more to accomplish essentially the same task DeviceNet is successfully doing today. GM has been monitoring the evolution and growth of Ethernet based I/O devices for years. A variety of Ethernet I/O network architectures have been investigated trying to find one that is cost comparable to the DeviceNet I/O control system architectures in use today.

The ability to use unicast EtherNet/IP communication, realized several years ago, allowed architectures that employ unmanaged switches to be considered, significantly lowering the projected cost differential between tools built with DeviceNet I/O and hypothetical, comparable tools designed with EtherNet/IP I/O. The projected EtherNet/IP I/O

cost penalty vs DeviceNet I/O decreased even more when DLR (Device Level Ring) embedded switch technology devices started becoming available. The possibility of linear topology EtherNet/IP I/O networks enabled by the DLR embedded switch technology is appealing. A linear topology network essentially mirrors the wiring topology we currently use in DeviceNet networks, and the negligible additional cost of an embedded switch within devices eliminates the need for and expense of stand-alone Ethernet switches at this level of an Ethernet network architecture.

The anticipated EtherNet/IP I/O network architecture for manufacturing assembly plant tooling PLCs exclusively using EtherNet IP I/O is depicted in figure 12. It only works if processor switches implementing the single hop inter-VLAN routing feature become available.

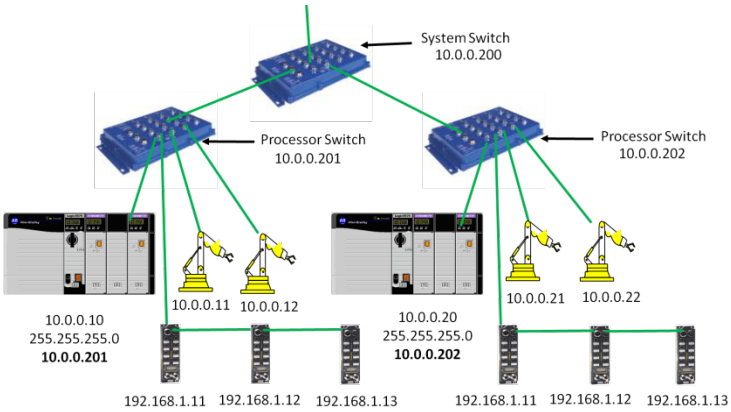

Figure 12: GM's proposed EtherNet/IP I/O network architecture for PLC I/O networks

Summary and Conclusion

TCP/IP capable devices on the same Ethernet network segment need to be assigned IP addresses with a common IP subnetwork address. Any and all traffic exchanged between Ethernet capable devices on the same IP subnetwork can be conveyed by Ethernet (layer 2) switches. Ethernet capable devices on different IP subnetworks can only indirectly communicate with each other. They need one or more routers and/or gateway devices to assist in the process of exchanging traffic between each other.

Inter-VLAN routing allows for switch-like performance when communicating between devices connected to the same physical switch but assigned to different IP subnetworks. Single hop inter-VLAN routing is a minimalist layer 3 routing feature that could be implemented on advanced layer 2 Ethernet switches. There are numerous situations where EtherNet/IP capable Ethernet I/O networks would benefit from switches that have a single hop inter-VLAN routing capability.

For control programs today that use device IP addresses within the control program to reference the controlled devices, a requirement to use uniquely addressed I/O devices would require the control program to be modified for every machine using it. A single hop inter-VLAN routing capability allows users to implement Ethernet I/O networks on different machines, each using identical IP addresses, in a cost effective manner.