Network Segmentation Methodology Application Guide

ControlLogix and CompactLogix 5370 Segmentation Methods for Plant-wide/Site-wide Networks with OEM Convergence-ready Solutions

By Josh Matson and Gregory Wilcox, Rockwell Automation

Contents

Introduction

The purpose of this application guideis to highlight the design considerations of various network segmentation methodologies to enable:

- Plant/site engineers to segment their industrial automation and control system (IACS) plant-wide/site-wide network infrastructure to help manage IACS traffic flow and segment policies – e.g. data prioritization and security
- OEMs (machine builders/process skid builders) to develop convergence-ready solutions to help simplify integration into their customer's plant-wide/site-wide network infrastructure

The first half of this document reviews segmentation methodology for the ControlLogix® programmable automation controller (PAC). The second portion of the document reviews segmentation methodology for the CompactLogix™ 5370 PAC.

This application guide is an extension ofthe design recommendations sitedin the Cisco® and Rockwell Automation Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (DIG), Rockwell Automation publication ENET-TD001E-EN-P. Relevant chapters:

- Chapter 3, "CPwE Solution Design-Cell/Area Zone"
- Chapter 5, "Implementing and Configuring the Cell/Area Zone"
- Chapter 8, "CIP Motion"
- Chapter 9, "CIP Sync Sequence of Events"

As noted within the CPwE DIG, the Cell/Area Zone is where the industrial automation and control system (IACS) end-devices are logically grouped, then connected into the Cell/Area IACS network. This could be a specific machine/process skid, geographic area, or operational function. Figures 1a and 1b show a representative example of Cell/Area Zones divided by operational functions, such as procession, filling, and material handling. Careful planning is required to achieve the optimal design, deployment and performance from both the Cell/Area IACS network and IACS device perspective. This extension of the CPwE references architectures focus on EtherNet/IP™, which is driven by the ODVA™ Common Industrial Protocol (CIP™).

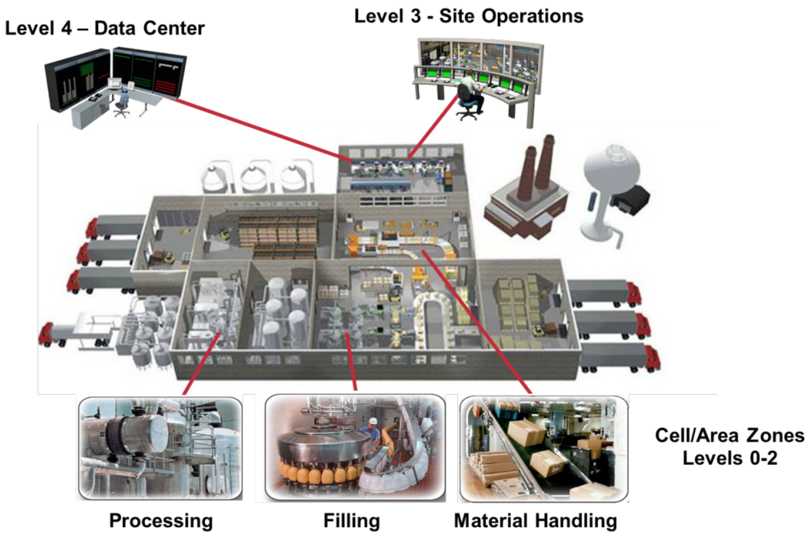


Figure 1a: Representative Example ofCPwE Cell/Area Zones

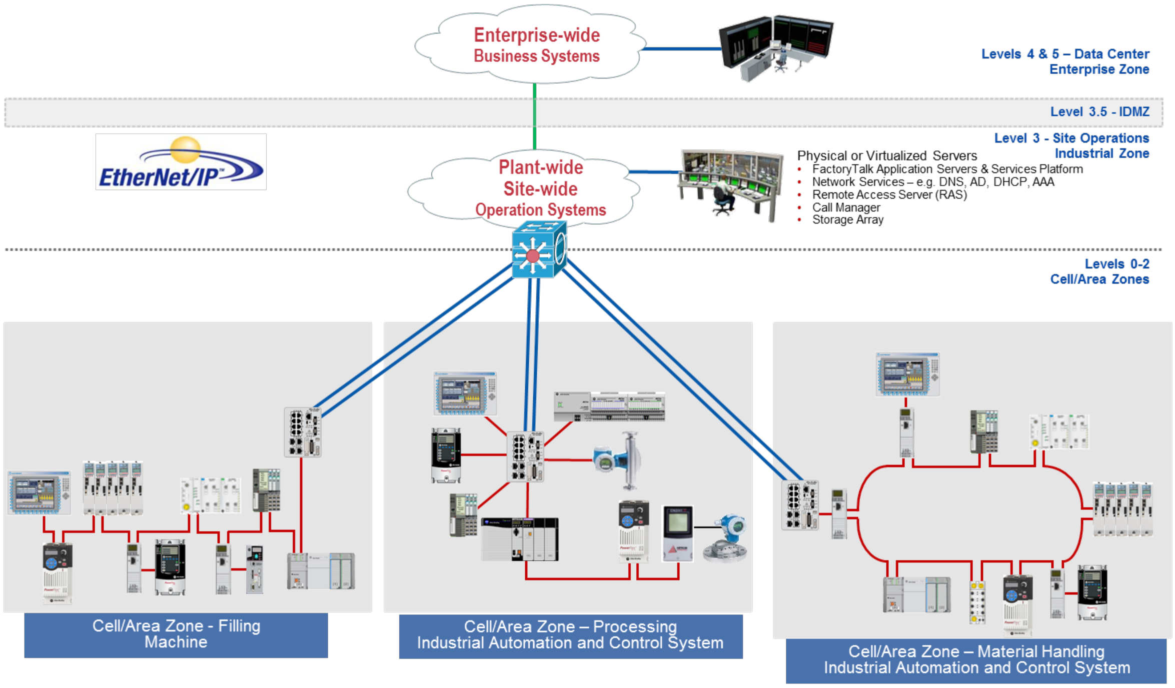

Enterprise-wide
Business Systems
Levels 4 & 5 – Data Center
Enterprise Zone
Level 3.5 - IDMZ
Level 3 - Site Operations
Industrial Zone
EtherNet/IP
Plant-wide
Site-wide
Operation Systems
Physical or Virtualized Servers
• FactoryTalk Application Servers & Services Platform
• Network Services – e.g. DNS, AD, DHCP, AAA
• Remote Access Server (RAS)
• Call Manager
• Storage Array
Levels 0-2
Cell/Area Zones
Cell/Area Zone - Filling Machine
Cell/Area Zone – Processing Industrial Automation and Control System
Cell/Area Zone – Material Handling Industrial Automation and Control System

Figure 1b: Representative Example of CPwE Cell/Area Zones

Traditionally, it was typical to have a 3-Tier networking model with different network technologies performing different control disciplines – e.g. motion, safety. These different communication standards provided natural network technology segmentation. Today, a continuing trend in industrial networking is the convergence of technology- specifically industrial automation technology with information technology. This convergence enables engineers to help enable the connection of multiple control and information application disciplines including data collection, configuration, diagnostics, discrete, process, batch, safety, time synchronization, drive, motion, energy management, voice and video through a plant-wide/site-wide EtherNet/IP network using a single industrial network technology, over a common network infrastructure.

This network technology convergence requires an industrial network design methodology utilizing network structure and hierarchy to help maintain real-time network performance. A key objective is to create smaller Layer 2 networks to create scalable and future-ready network infrastructures, minimize broadcast and fault domains, create smaller domains of trust, and reduce overall network sprawl (undisciplined network growth). Examples of structure and hierarchy would be:

- CPwE logical model – geographical and functional organization of industrial automation and control system (IACS) devices
- Campus network model - multitier switch model with Layer 2 and Layer 3 switching
- CPwE logical framework
- Segmentation methodologies
  - Multiple network interface cards (NICs) – e.g. CIP Bridge
  - Network Address Translation (NAT) appliance
  - Virtual Local Area Networks (VLANs)
  - VLANs with NAT
  - Unified Threat Management (UTM) Security Appliance

The choice of methodology to segment IACS traffic is dependent on multiple factors. Examples could be:

- Plant-wide/site-wide IACS application requirements
- OEM convergence-ready IACS applications – e.g. machine builders and process skid builders
- Company policies and procedures
- Applicable industry and regulatory standards
- Company organizational and support structure – e.g. lines of responsibilities for control system engineers and IT network engineers

This application guide will review design considerations and best practices when implementing these segmentation methodologies. For additional information on industrial network design methodology, refer to Top 10 Recommendations for Plant-wide EtherNet/IP Deployments - publication ENET-WP022.

For the purpose of this application guide, the term "future-ready" is defined as the design and deployment considerations to confirm that the industrial network can be: 1) seamlessly expanded without impacting existing network performance (e.g. latency and jitter), and 2) seamlessly enhanced with the addition of new technology and products without requiring a forklift upgrade of the network.

For the purpose of this application guide, the term "convergence-ready" is defined as the design and deployment considerations that a collaborator (e.g. OEM, system integrator, contractor) has to take into account to achieve seamless integration of their solution (e.g. machine or process skid) into their customers'plant-wide/site-wide network infrastructure.

Convergence-ready design and deployment considerations

- Use of an industrial Ethernet protocol that fully utilizes standard Ethernet and IP (such as EtherNet/IP) as the multi-discipline industrial network infrastructure
  - Common network infrastructure devices – asset utilization
  - Scalable and future-ready - sustainability
- IP addressing schema
  - Class, address range, subnetting, default gateway configuration (routability)
  - Implementation conventions – static/dynamic addressing, hardware/software configurable, NAT, domain names
- Use of Network Services
  - Segmentation methodology, data prioritization methodology
  - Managed switches, switch-level and device-level topologies
  - Network availability – loop prevention, resilient topologies and protocols
  - Security stance
    - Physical access, port security, access control lists, application security (e.g. FactoryTalk Security)
    - Alignment with emerging IACS security standards such as ISA/IEC-62443 and NIST 800-82
  - Time Synchronization Services
    - IEEE 1588 Precision Time Protocol (PTP)
    - CIP Sync applications – first fault, SOE, CIP Motion

Part 1: Converged Plantwide Ethernet Cell/Area Zone Segmentation Methods: ControlLogix Platform

Summary of Design Considerations – ControlLogix Platform

CIP Bridge

1. The only traffic that can traverse the ControlLogix backplane is CIP application layer traffic. This may impact the future-ready and convergence-ready aspects of the application.

2. Different CIP traffic types can be distributed across multiple 1756-ENxT(R) cards, reducing the bandwidth loading on any one card and allowing for scalability.

NAT

1. Network Address Translation can be implemented with one of three available devices from Rockwell Automation:

    a. Stand-alone NAT Appliance (9300-ENA)

    b. Switch based NAT (Stratix 5700)

    c. Unified Threat Management Security Appliance (Stratix 5900)

2. NAT can be combined with VLANs to provide repeatable IP subnets, providing easy application replication for machine and process skid builders

VLANs

1. It is recommended to segment networks by configuring one VLAN and one IP subnet per Cell/Area Zone for similar traffic types

2. In some cases it may be advantageous to divide individual Cell/Area Zones into smaller VLANs (Layer 2) to separate traffic types (i.e. voice/video within the Cell/Area Zone)

3. Networks utilizing multiple Virtual LANs (VLANs) require a Layer 3 capable switch to route traffic between the VLANs

4. Always utilize Inter-VLAN routing vs. VLAN trunking between Cell/Area Zones to maintain smaller Layer 2 networks

5. The native VLAN should be a dedicated VLAN (other than VLAN 1) that does not carry any user traffic

For additional information on VLANs, refer to publications:

- ENET-TD001, Converged Plantwide Ethernet (CPwE) Design and Implementation Guide
- ENET-RM002, Ethernet Design Considerations

When segmenting an IACS Network there are a few initial design considerations to make, demonstrated in example topologies below. First, will you segment your network physically by using multiple ENxT(R) cards within a single ControlLogix chassis? Or will you utilize logical segmentation using VLANs? Second, how will you segment your traffic within the Cell/Area Zone; control (I/O) and information (HMI) from the same ENxT(R) card, or segment among multiple cards?

This application guide will present multiple examples of topologies for each segmentation methodology. As noted earlier, it is up to the customer to understand their application requirements when choosing the appropriate segmentation methodology and making the final design and deployment decisions.

Example Network – Segmentation in a Plant-wide/ Site-wide Network using VLANs and Physical Segmentation – ControlLogix Platform

Figure 2 is an example of what a representative industrial automation and control system (IACS) may look like, divided into two parts. The top of the IACS is comprised of the CPwE Industrial Zone with a Cisco Catalyst 3750 StackWise™ (Layer 3) switch stack to handle and maintain packet routing. The bottom of the IACS is comprised of the Cell/Area Zones which encompasses the Stratix 5700 and 8000 (Layer 2) switches configured with a resiliency protocol for the switch-level ring topology, and the individual IACS cells/areas.

Figure 2 shows several examples of network segmentation methodology:

- CIP Bridge segmentation for Cell/Area Zone #1
- Converged switching technology configured with multiple VLANsfor Cell/Area Zones #2, #3 and #4. The concept of VLAN segmentation is well known in the information technology domain, but still a newer concept in the industrial automation domain.

As denoted by different colors, each Cell/Area Zone is segmented into VLANs to create smaller Layer 2 networks (domains) without requiring additional hardware. Smaller Layer 2 domains help to enable a modular building block approach to IACS network design and deployment. A building block approach to IACS networks helps with:

- Minimizing network sprawl through a more disciplined network design
- Scalable, future-ready IACS network design – start small then scale up as necessary
- Robustness through smaller fault and broadcast domains
- Smaller domains of trust to help simplify security policy enforcement

If data needs to be shared between the segmented Cell/Area Zones' VLANs, then the Catalyst 3750 switch, or other Layer 3 device, can be configured for inter-VLAN routing.

This configuration is typical to the Campus Model, which is explained further in the Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (DIG).

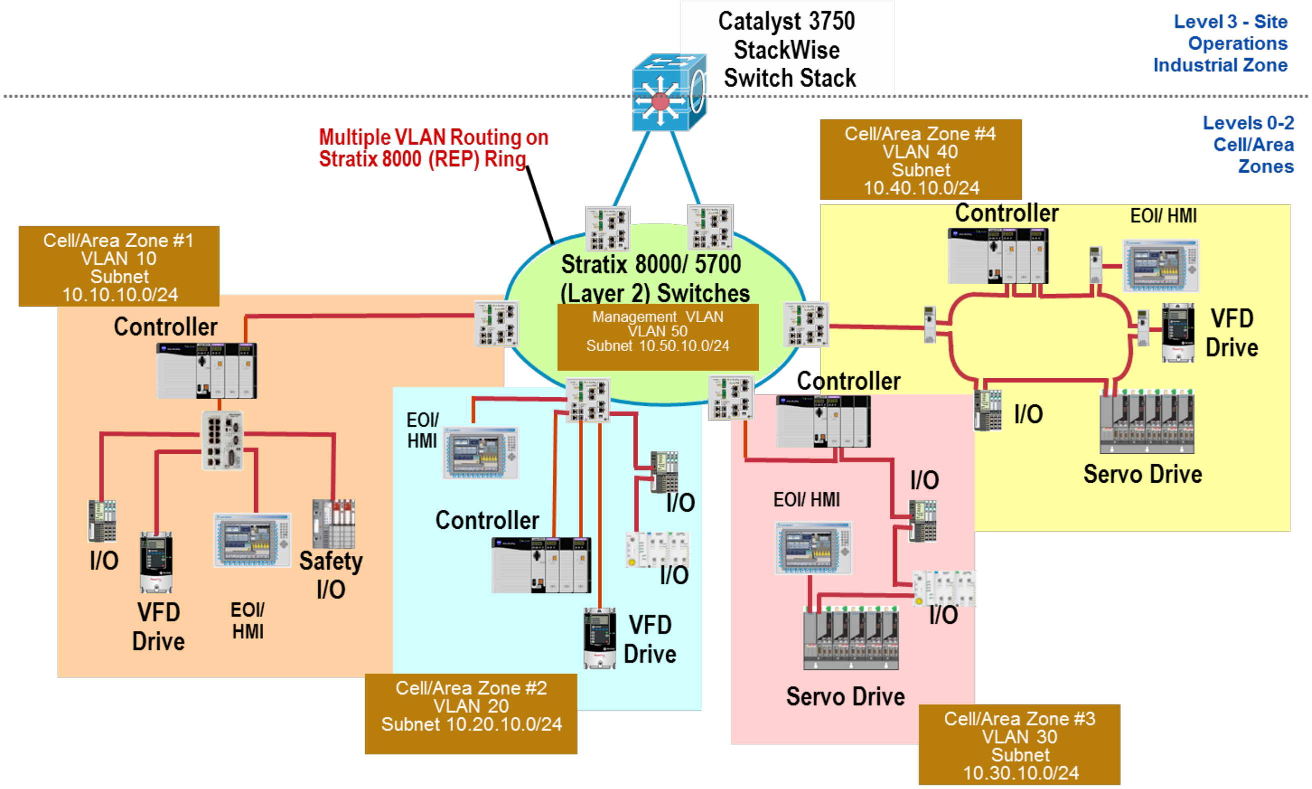


Figure 2: Industrial Zone segmented into different CPwE Cell/Area Zones

Advantages:

- Segmented network ownership demarcation lines between industrial automation and IT. Minimized network traffic loading by segmenting the multiple Cell/Area Zones from each other using VLANs
- Minimized network traffic loading by preventing unwanted network traffic (i.e. streaming video, VoIP, rogue PCs, etc.) from entering the Cell/Area Zone via VLAN configuration
- Visibility into IACS network devices for asset management
- Provides future-ready information enabled capabilities
- Scalable network architecture
- Structured approach reducing network "sprawl"

Disadvantages:

- Extended network skillset is required to configure switches, routers, network topologies and protocols

Converged Plantwide Ethernet Cell/Area Zone #1 - Multiple 1756-ENxT(R) Modules for Physical Chassis Segmentation

Physically segmenting a network can be accomplished using a 1756-ENxT(R) module (NOTE: "x" represents two types of Ethernet modules - the EN2TR and the EN3TR). The 1756-ENxT(R) module is a Network Interface Card (NIC) that resides in a 1756 ControlLogix platform and gives the Programmable Automation Controller (PAC) the ability to communicate with other devices on the EtherNet/IP network. This communication generates EtherNet/IP network traffic. This network traffic can be classified as either CIP Class 1 (I/O) traffic or CIP Class 3 (messaging) traffic.

Referring to Figure 3, using two ENxT(R)s, a CIP Bridge has been created across the ControlLogix backplane (bp). This topology has the advantage of naturally segmenting CPwE Level 0 (I/O) and Level 1 (Controller) traffic from Level 2 (Information) traffic. The only traffic that can traverse the backplane is Common Industrial Protocol (CIP) application layer traffic.

- Physically segmented network - Layer 2 traffic (e.g. broadcast traffic) cannot traverse the CIP Bridge
- Non-CIP application layer traffic cannot traverse the CIP Bridge
- The same effect can be achieved with VLANs implementation

Some special notes to remember if utilizing this segmentation methodology: 1) The CIP Bridge does not filter CIP traffic and 2) an industrial network design methodology should still be followed to implement best practices on both sides of the CIP Bridge. Cisco and Rockwell Automation recommend the customer still utilize VLANs and follow proper design techniques.

Physical segmentation of the network via the ControlLogix backplane can also create a clear demarcation line of network ownership. This demarcation line enables network responsibilities to be divided between an information technology network engineer for the plant-wide/site-wide network and an industrial automation control system engineer for the Cell/Area Zone or machine/process skid network.

The disadvantage of this topology is that CIP capable Level 0 IACS device use is required in order to communicate to the devices at Level 0 (end devices) from the information network. This means non-CIP Ethernet traffic will not be able to reach all points of the network. For non-CIP devices, maintenance personnel will need to plug directly into the side of the network where they need to get connectivity to (e.g. plug into the information network for the HMI troubleshooting and plug into the Level 0 control network for the I/O diagnostics). For example, most IACS devices have an embedded HTTP or HTTPS server for diagnostics and configuration that will not be available from one centralized location in this topology. In Level 0 there will be no access to web pages, flash firmware, or programing of the switch.

The approach of security by obscurity, or isolation, is no longer enough today- this topology alone does not provide the defense-in-depth security approach which is required for an IACS. For example, the CIP Bridge acts as an application layer bridge, allowing all CIP traffic to be "forwarded" from the Level 2 information network to the Level 0 I/O network. Segmentation of Level 2 information traffic across the CIP Bridge to the Level 0 I/O traffic can be achieved by implementing a Deep Packet Inspection (DPI) capable firewall. For additional information on defense-in-depth refer to publication ENET-WP005, Securing Manufacturing Computing and Controller Assets.

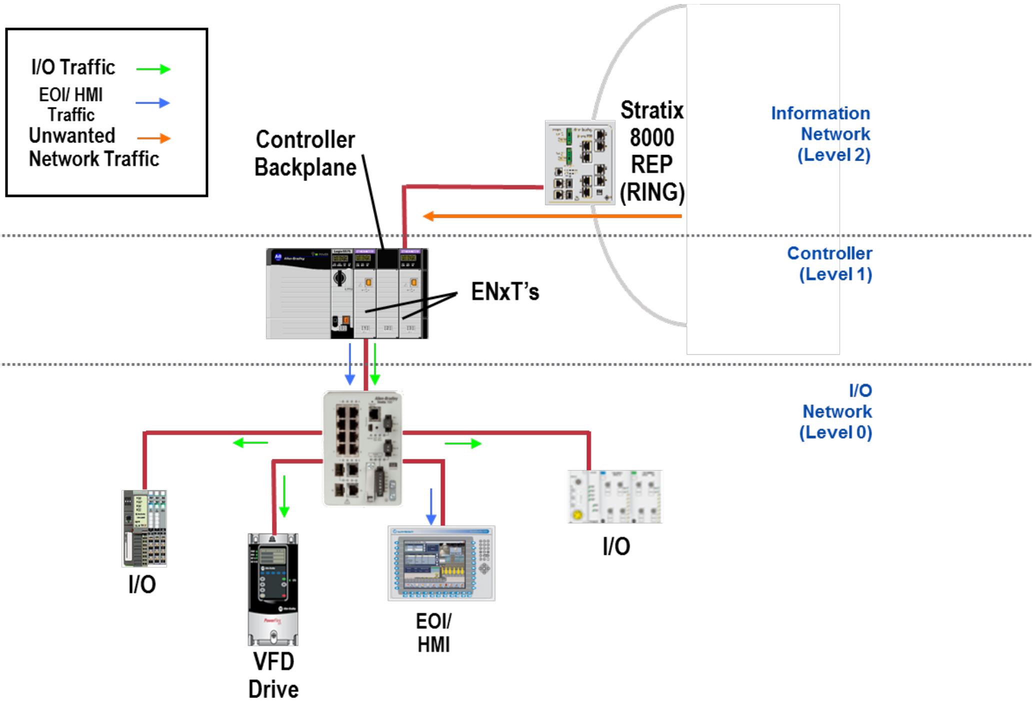


Figure 3: Segmenting the CPwE Cell/Area Zone #1 Using 2- ENxT(R)s

Advantages:

- Segmented network ownership demarcation lines between industrial automation and IT.
- Minimized network traffic loading by segmenting the multiple Cell/Area Zones from each other
- Minimized network traffic loading by preventing unwanted network traffic (i.e. streaming video, VoIP, rogue PCs, etc.) from entering the Cell/Area Zone via the ControlLogix backplane
- Minimal impact on ENxT(R)s CPU Utilization with traffic segmented amongst multiple cards

Disadvantages:

- Limited visibility to other IACSnetwork devices for asset management
- Limited scalability due to limited number of ENxT(R)s
- Limited future-ready information enabled capabilities

Converged Plantwide Ethernet Cell/Area Zone #2 - Using Multiple 1756-ENxT(R) Modules for Scalability

If a bandwidth limitation on the 1756-ENxT(R) card is of concern, the user may want to consider segmenting I/O traffic from information traffic. This can be accomplished using two or more ENxT(R) modules in the ControlLogix chassis. Figure 4a shows an example of I/O traffic being physically segmented from information traffic within the ControlLogix chassis to the same Stratix 8000 switch, on the same subnet and VLAN using two ENxT(R) modules in a Star topology.

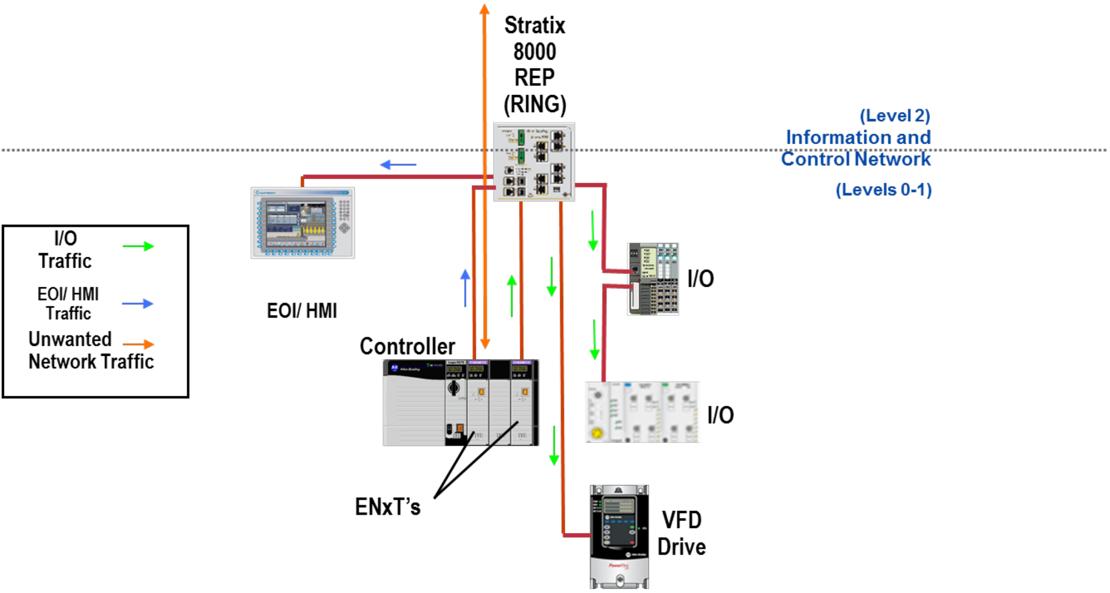


Figure 4a: Segregating I/O traffic from Information Traffic in the CPwE Cell/Area Zone #2 using twoENxT(R)s

Advantages:

- Minimal impact on ENxT(R)s CPU Utilization with traffic is segmented among multiple cards
- Visibility to all IACS network devices for asset management
- Provides future-ready information enabled capabilities

Disadvantages:

- Blurred network ownership demarcation line
- Unwanted traffic (i.e. streaming video, VoIP, rogue PCs, etc.) could pass into control network (Levels 0-1) – this can be minimized with managed switch technologies, including VLANs
- Unwanted control traffic (i.e. multicast and broadcast traffic) could pass into information network–this can be minimized with managed switch technologies, including VLANs

Converged Plantwide Ethernet Cell/Area Zone #2 - Logical Segmentation UsingVLANs

A converged, scalable, robust and future-ready network architecture can be achieved by using switching technology configured with multiple VLANs to logically segment the information network (Level 2) from the control network (Levels 0-1). However, this segmentation methodology has its own design considerations.

The first is the potential to blur the demarcation line of network ownership between the control network (Levels 0-1) and the information network (Level 2). The CIP Bridge example shown in Figure 3 provided the capability for a clear demarcation line of network ownership between the control network (Levels 0-1) and the information network (Level 2). Example, the control network could be managed by an industrial automation control system engineer while the information network could be managed by an information technology network engineer. The demarcation line of network ownership is not so clear for the converged examples shown in Figures 4a and 4b. Depending on a company's organizational structure, this converged network might be owned by a control system engineer, an IT network engineer or combination of the two. Regardless, a collaboration of industrial automation and information technology domains is essential for successful design and deployment of converged network architectures.

The second is the potential for network traffic from Levels 2 and 3 mixing with and impacting the control traffic in Levels 0 and 1. Figure 4a shows a converged but non-segmented example. There is the possibility of non-control traffic (i.e. streaming video, VoIP, and unwanted PCs) feeding in from the information network (Levels 2-3). The reverse may also be true - control traffic (multicast and broadcast traffic) traversing onto the information network (Levels 2-3), as there would be no technical controls to segment the traffic. Figure 4b shows the addition of VLANs to the previous example to logically segment the control traffic from the information traffic. This example provides for the convergence of traffic onto a common infrastructure (switch) while still segmenting the different traffic types.

As noted earlier, the choice of methodology to segment IACS traffic is dependent on multiple factors. Examples could be:

- Plant-wide/site-wide IACS application requirements
- OEM convergence-ready IACS applications – e.g. machine builders and process skid builders
- Company policies and procedures
- Company organizational and support structure – e.g. lines of responsibilities for control system engineers and IT network engineers

Figure 4b shows an example of segmenting the information traffic (VLAN 50, Subnet 10.50.10.0/24), from the control traffic (VLAN 20, Subnet 10.20.10.0/24) by configuring VLANs in the Stratix 8000 switch. This topology allows the ability to choose what traffic traverses the two VLANs with the help from the Catalyst 3750 switch stack Layer 3 routing capabilities (refer to Figure 2). Once again, segmenting Cell/Area Zones from each other will help create smaller Layer 2 domains, reduce overall network loading and create smaller domains of trust.

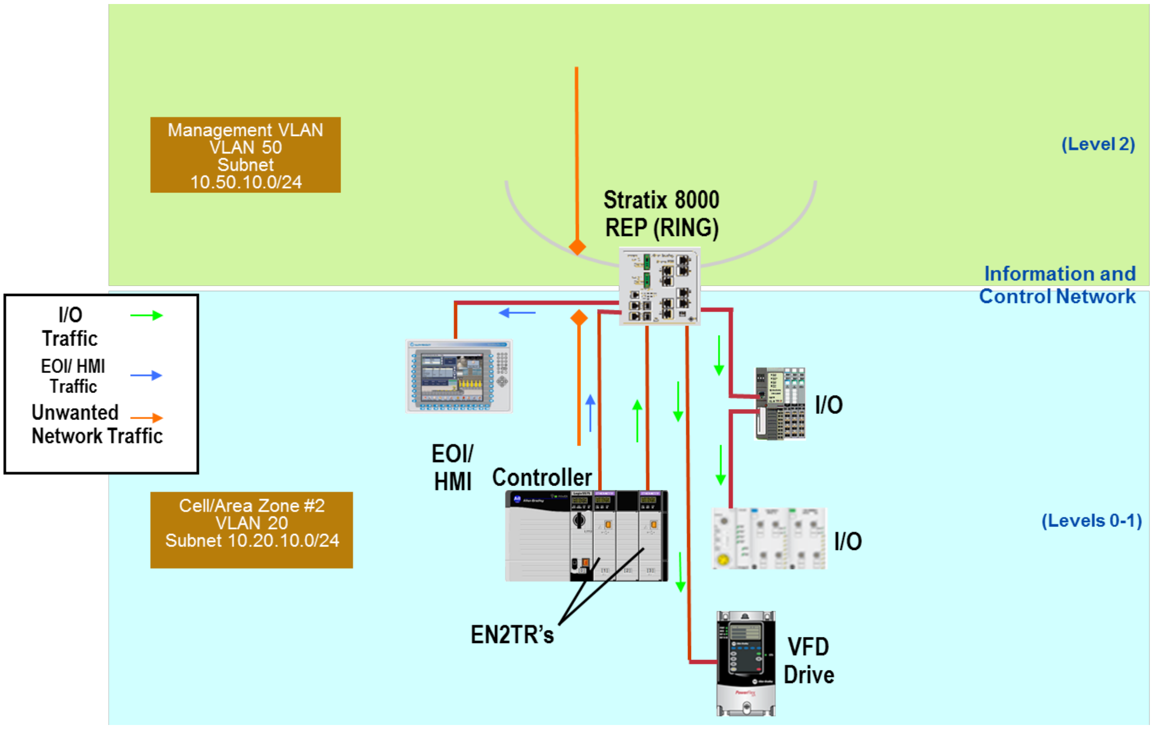


Figure 4b: Segmenting the CPwE Cell/Area Zone #2 Using VLANs

Advantages:

- Segmented network ownership demarcation lines between industrial automation and IT
- Minimized network traffic loading by segmenting the multiple Cell/Area Zones from each other
- Minimized network traffic loading by preventing unwanted network traffic (i.e. streaming video, VoIP, rogue PCs, etc.) from entering the Cell/Area Zone via the VLAN configuration
- Minimized impact to information network by preventing unwanted control traffic (i.e. multicast and broadcast traffic) from exiting the Cell/Area Zone via VLAN configuration
- Minimal impact on ENxT's CPU utilization due to segmentation of I/O and information traffic between two different ENxTs
- Visibility to other IACS network devices for asset management
- Provides future-ready information enabled capabilities

Disadvantages:

- Requires more advanced configuration abilities

Converged Plantwide Ethernet Cell/Area Zone #3 – Linear Device-Level Topology, Embedded Switch Technology (No Segmentation)

Figure 5a shows an example of a small IACS, in a linear device-level topology, where both I/O and information traffic is forwarded through one ENxT(R) module. Note that the ENxT(R) modules, as well as other devices in the Cell/Area Zone, have a two port embedded technology, enabling the linear device-level topology. The ENxT(R) module is designed to handle both of these types of traffic simultaneously; however the ENxT(R)'s CPU limitations must be considered.

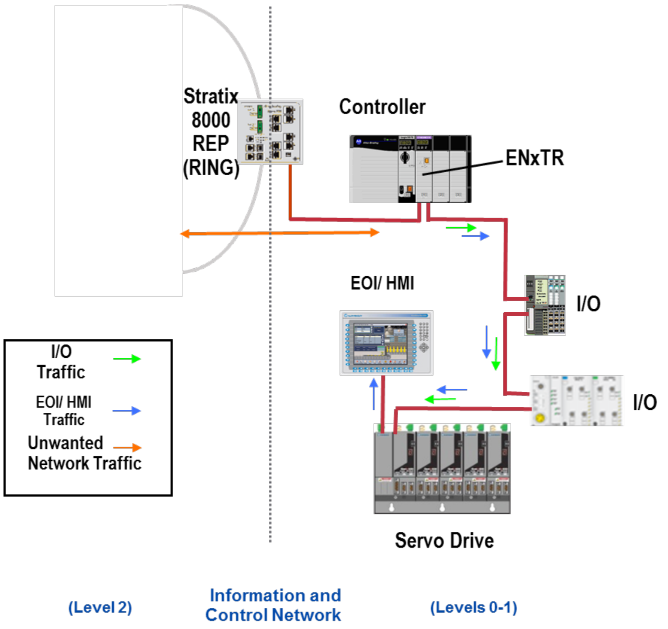


Figure 5a: Segmenting the CPwE Cell/Area Zone #3 Using OneENxT(R)

Advantages:

- Embedded switch enabled IACS devices enable simple connectivity of devices to form a linear device-level topology
- Visibility to other control network devices for asset management
- Provides future-ready information enabled capabilities

Disadvantages:

- Blurred network ownership demarcation line
- May impact the ENxT(R)'s CPU Utilization due to I/O and information traffic being routed through oneENxT(R)
- Unwanted information traffic (i.e. streaming video, VoIP, rogue PCs, etc.) could pass into the control network –this the could be minimized with managed switch technologies, including VLANs
- Unwanted control traffic (broadcast and multicast), could pass into the information network–this could be minimized with managed switch technologies, including VLANs
- A single fault within the linear device-level topology would interrupt communications to downstream IACS devices

Converged Plantwide Ethernet Cell/Area Zone #3 – Linear Device-Level Topology, Embedded Switch Technology (Segmentation Using VLANs)

As in Cell/Area Zone #2 example, a VLAN could be implemented in Cell/Area Zone #3 to help prevent unwanted traffic from traversing from Level 2 to Levels 0 and 1, and vice versa, with a software configuration within the Stratix 8000 switch. Traffic can be forwarded between VLANs (inter-VLAN routing) in a controlled manner using the management features found in a Layer 3 switch, such as the Catalyst 3750 StackWise™ switch stack.

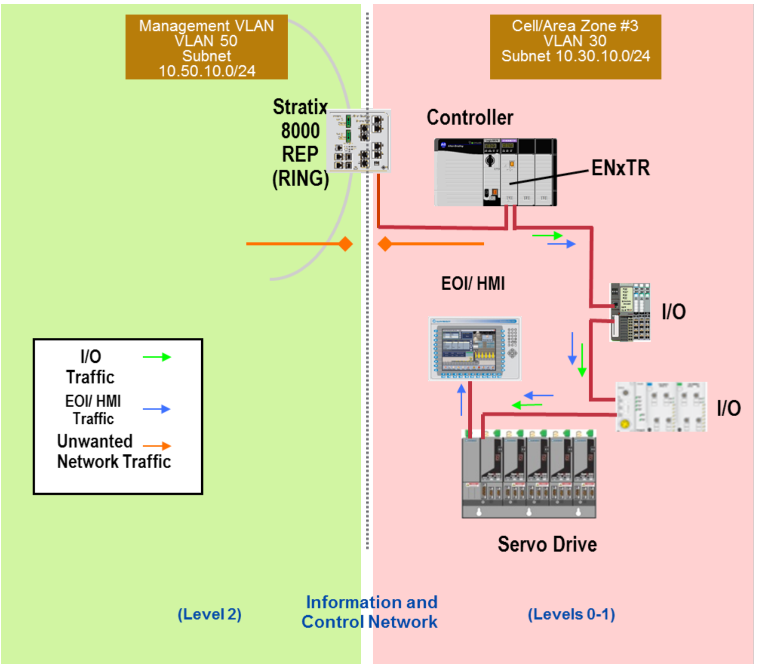


Figure 5b: Segmenting the CPwE Cell/Area Zone #3 Using One ENxT(R) and VLANs

Advantages:

- Embedded switch technology IACS devices enable easy connectivity of devices to form a linear device-level topology
- Unwanted information traffic (i.e. streaming video, VoIP, rogue PCs, etc.) can be restricted from the control network
- Visibility to other control network devices for asset management
- Unwanted control traffic (broadcast and multicast) can be restricted from the information network
- Provides future-ready information enabled capabilities

Disadvantages:

- May impact the ENxT(R)'s CPU Utilization due to I/O and information traffic being forwarded through one ENxT(R)
- A single fault within the linear device-level topology would stop communications to downstream nodes
- Requires more advanced configuration abilities

Converged Plantwide Ethernet Cell/Area Zone #4 – Ring Device-Level Topology, Embedded Switch Technology (No Segmentation)

If this were a larger system with ten to 20 distributed I/O racks and eight to ten HMI stations, consider deploying more than one ENxT(R) in the system to address bandwidth limitation. When the IACS gets so large that the ENxT(R)'s CPU utilization exceeds 60%, it is time to add a second ENxT(R) into the chassis and split the network traffic (ex. the first ENxT(R) gets 30% of the traffic and the second ENxT(R) gets the other 30%).

Figure 6a shows a larger IACS in a ring device-level topology. This topology provides one level of media resiliency in the event of a cable break. The topology choice here has little to do with segmentation best practices, and was chosen purely for demonstration.

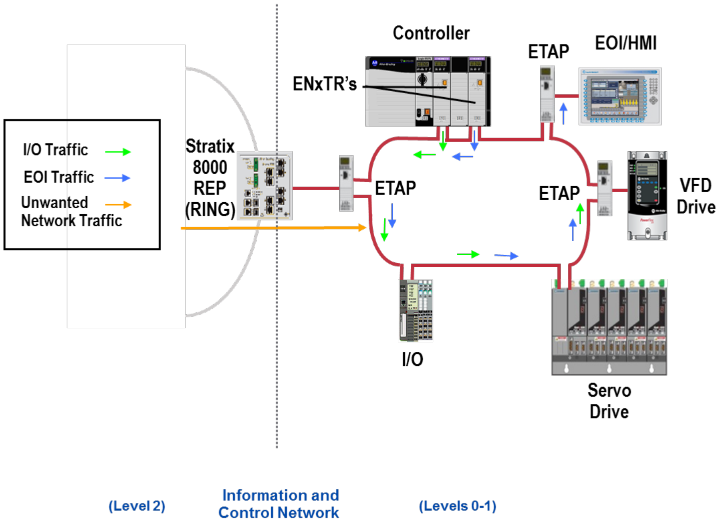


Figure 6a: Separating the network traffic within the CPwE Cell/Area Zone #4 using two ENxT(R)s

Advantages:

- Minimal impact on ENxT(R)'s CPU Utilization due to I/O and information traffic segmented between two different ENxT(R)s
- Separate Ethernet cards used for segmentation of traffic
- Converged network minimizes utilization of each ENxT(R) card
- Embedded switch technology IACS devices allow easy connectivity of devices to form either a linear or ring device-level topology
- Device Level Ring (DLR) resiliency protocol provides a single fault tolerant network within the device-level ring redundant pathtopology
- Visibility to other control network devices for asset management
- Provides future-ready information enabled capabilities

Disadvantages:

- Blurred network ownership demarcation line
- Unwanted information traffic (i.e. streaming video, VoIP, rogue PCs, etc.) could pass into control network–this can be minimized with managed switch technologies, including VLANs
- Unwanted control traffic (broadcast and multicast) could pass into information network

Converged Plantwide Ethernet Cell/Area Zone #4 – Device level Ring Topology, Embedded Switch Technology (Segmentation Using VLANs)

As in Cell/Area Zones #2 and #3, unwanted traffic can be contained by implementing VLANs in the Stratix 8000 switch.

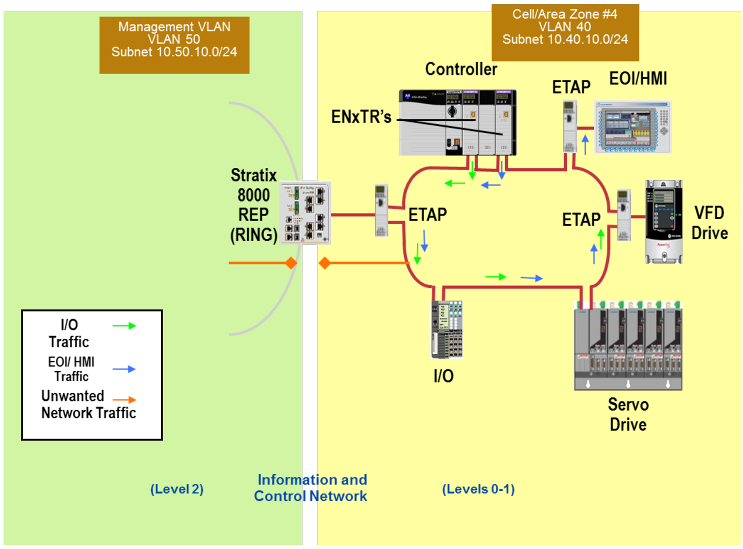


Figure 6b: Separating the network traffic within the CPwE Cell/Area Zone #4 using two ENxT(R)'s and from outside the CPwE Cell/Area Zone VLANs

Advantages:

- Minimal impact on ENxT(R)'s CPU Utilization due to I/O and information traffic segmentation between two different ENxT(R)s
- Separate Ethernet cards used for segmentation of types of traffic
- Converged network that minimizes utilization of each ENxT(R) card
- Unwanted information traffic (i.e. streaming video, VoIP, rogue PCs, etc.) can be restricted from the control network
- Visibility to other control network devices for asset management
- Unwanted control traffic (broadcast and multicast) can be restricted from the information network
- Clear network ownership demarcation line (i.e. responsibility for certain section of the network) accomplished with VLANs
- Embedded switch technology IACS devices allow easy connectivity of devices to form either a linear or ring device-level topology
- Device Level Ring (DLR) resiliency protocol provides a single fault tolerant network within the device-level ring redundant path topology toprovide visibility to other control network devices for asset management
- Provides future-ready information enabled capabilities

Disadvantages:

- Requires more advanced configuration abilities
- Requires the use of multiple ENxT(R) cards to separate types of traffic

Plant-wide/Site-wide ControlLogix Architectures utilizing Network Address Translation Appliances

NAT can be used in plant-wide/site-wide architectures to enable re-use of IP subnets. NAT can be applied using:

- NAT Appliances (9300-ENA)
- Switch based NAT (Stratix 5700)
- Unified Threat Management Security Appliances (Stratix 5900)

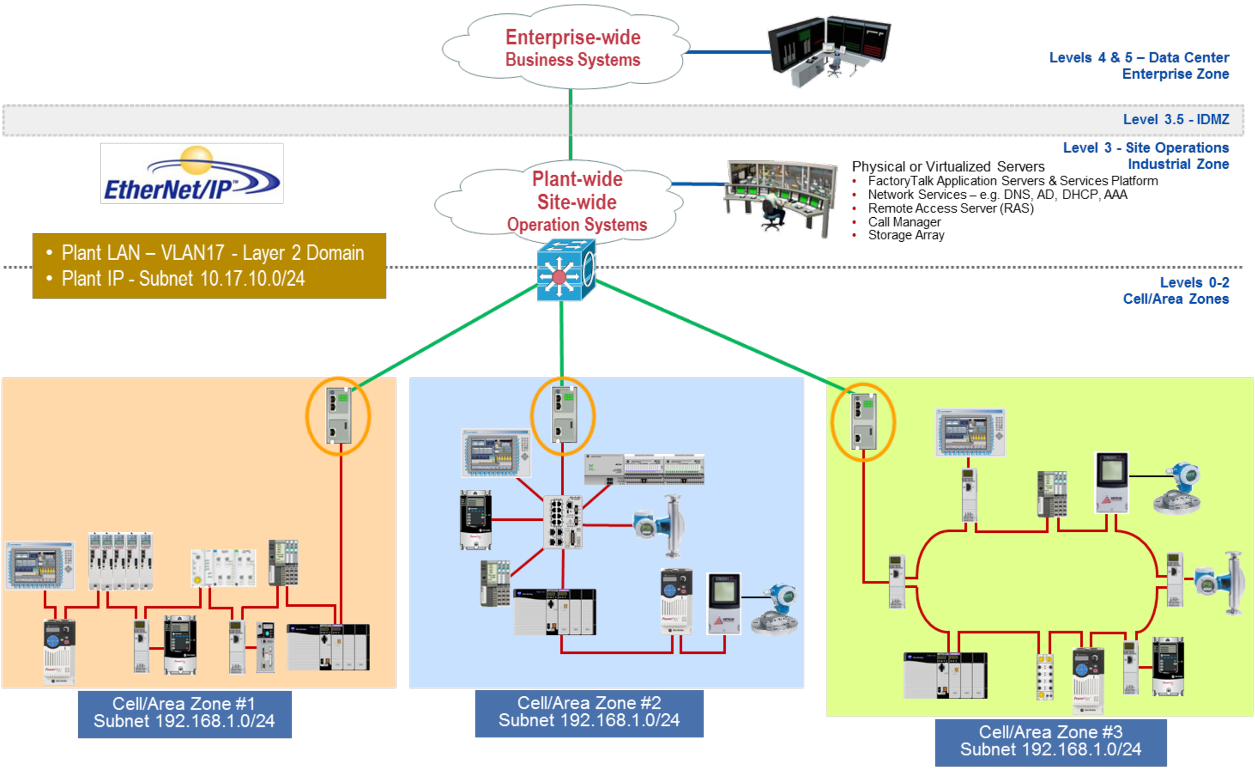


Figure 7: Repeating IP subnets between CPwE Cell/Area Zones. Translating IP Addresses using network address translation appliances

- IP Schema – separate from plant/site, all nodes within the machine/process skid must have a unique IP address, IP addresses can be reused across process skids
- In this example a device is placed between each Cell/Area Zone to provide Network Address Translation (NAT)
- From Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP addresses can be re-used
- Each NAT appliance must be programmed to translate from the 192.168.1.0/24 IP subnet to the plant-wide IP subnet
- Although the NAT appliance does breakup the Layer 2 network, it does not provide true logical segmentation between Cell/Area Zones- VLANs must be implemented to achieve this

Plant-wide/Site-wide ControlLogix Architectures utilizing Network Address Translation Enabled Switches and VLAN's

NAT can be used in plant-wide architectures to allow re-use of IP subnets. NAT can be applied using:

- NAT Appliances (9300-ENA)
- Switch based NAT (Stratix 5700)
- Unified Threat Management Security Appliances (Stratix 5900)

NAT can be combined with VLAN's to provide repeatable subnets, which is beneficial to machine/process skid builders. It will provide the additional benefit of smaller Layer 2 building blocks, allowing control over traffic traversing between subnets.

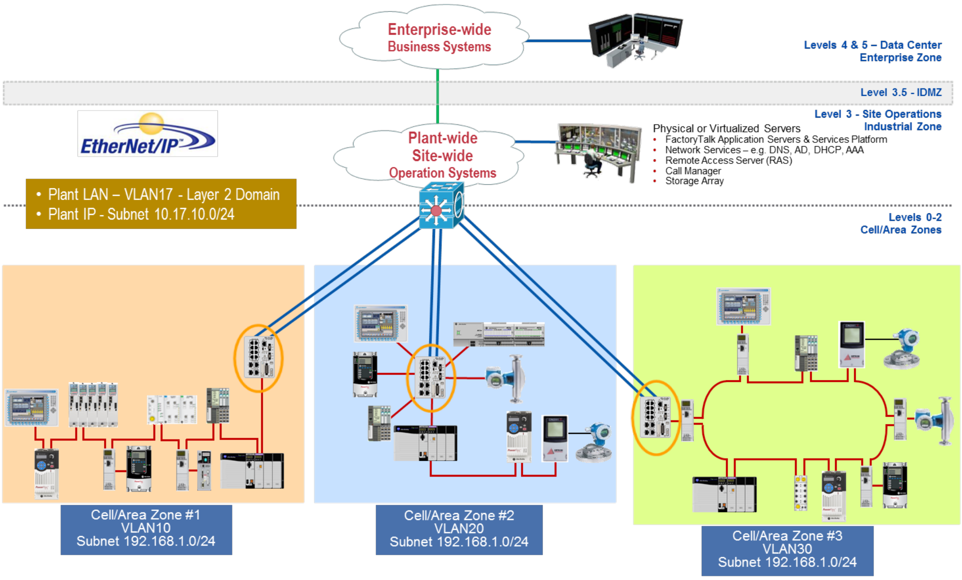


Figure 8: Repeating IP subnets between CPwE Cell/Area Zones. Translating IP addresses using Stratix 5700 series switches. VLAN's implemented to logically segment CPwECell/Area Zones.

- IP Schema – separate from plant/site, all nodes within the process skid must have a unique IP address, IP addresses can be re-used across machines/process skids
- In this example a device is placed between each Cell/Area Zone to provide Network Address Translation
- From the Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP addresses can be re-used
- Each NAT appliance must be programmed to translate from the 192.168.1.0/24 subnet to the plant-wide/site-wide subnet
- Cell/Area Zones are segmented from each other by logically implementing VLANs

Plant-wide/Site-wide ControlLogix Architectures utilizing Network Address Translation via Unified Threat Management Security Appliance

NAT can be used in plant-wide/site-wide architectures to allow re-use of subnets. NAT can be applied using:

- NAT Appliances (9300-ENA)
- Switch based NAT (Stratix 5700)
- Unified Threat Management Security Appliances (Stratix 5900)

NAT can provide repeatable IP subnets, which is beneficial to machine/process skid builders. It will provide the additional benefit of smaller Layer 2 building blocks, allowing control over traffic traversing between IP subnets.

NAT can be implemented via a unified threat management security appliance such as the Stratix 5900. Each UTM security appliance would act similar to the stand alone NAT appliance in that it would be programmed to translate from the 192.168.1.0/24 IP subnet to the plant-wide/site-wide IP subnet. The UTM security appliance supports an additional level of enhanced security to further segment Cell/Area Zones from the plant-wide/ site-wide network and other Cell/Area Zones.

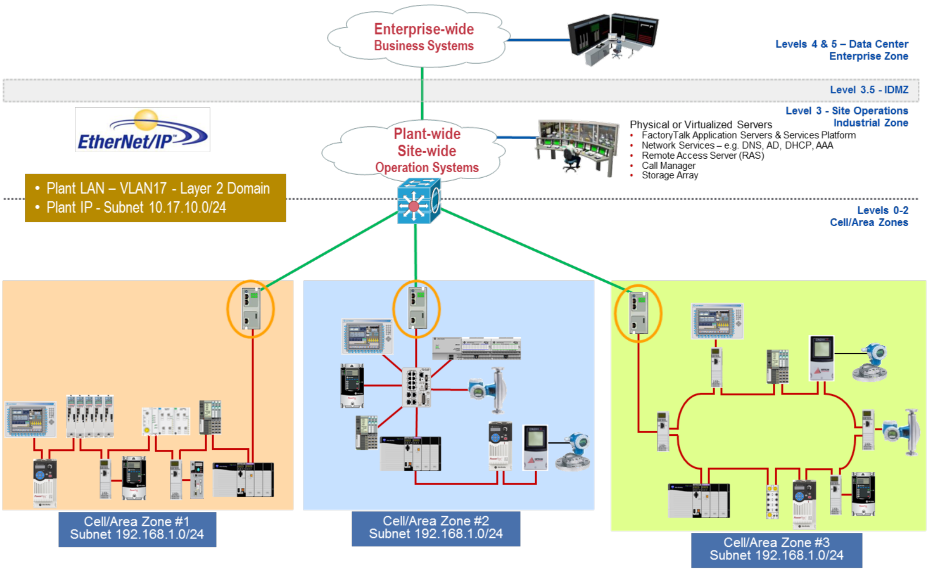


Figure9: Repeating IP subnets between CPwE Cell/Area Zones. Translating IP Addresses using Stratix 5900 Unified Threat Management Security Appliance.

- IP Schema – separate from plant/site, all nodes within the machine/process skid must have a unique IP address, IP addresses can be reused across machines/process skids
- In this example a UTM Appliance is placed between each Cell/Area Zone to provide Network Address Translation
- From the Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP addresses can be re-used
- Each UTM security appliance must be programmed to translate from the 192.168.1.0/24 IP subnet to the plant-wide/site-wide IP subnet

Part 2: Converged Plantwide Ethernet Cell/Area Zone Segmentation Methods – CompactLogix Platform

Summary of Design Considerations – CompactLogix Platform

CIP Bridge

1. CompactLogix 5370 platforms do not support multiple NICs like the ControlLogix platform. For this reason, the CIP Bridge is not an option for network segmentation within the CompactLogix 5370 platform.

NAT

1. Network Address Translation can be implemented with one of three Rockwell Automation available devices:

   a. NAT Appliances (9300-ENA)

   b. Switch based NAT (Stratix 5700)

   c. Unified Threat Management Security Appliances (Stratix 5900)

2. NAT can be combined with VLANs to not only provide repeatable IP subnets, which enables repeatable machine or process skid applications, but also Layer 2 segmentation.

VLANs

1. It is recommended to segment networks by configuring one VLAN and one IP subnet per Cell/Area Zone for similar traffic types

2. In some cases it may be advantageous to divide individual Cell/Area Zones into smaller VLANs (Layer 2) to separate traffic types (i.e. voice/video within the Cell/Area Zone)

3. Networks utilizing multiple Virtual LANs (VLANs) require a Layer 3 capable switch to route traffic between the VLANs

4. Always utilize Inter-VLAN routing vs. VLAN trunking between Cell/Area Zones to maintain smaller Layer 2 networks

5. The native VLAN should be a dedicated VLAN (other than VLAN 1) that does not carry any user traffic

CompactLogix 5370 Platform Based Segmentation Note

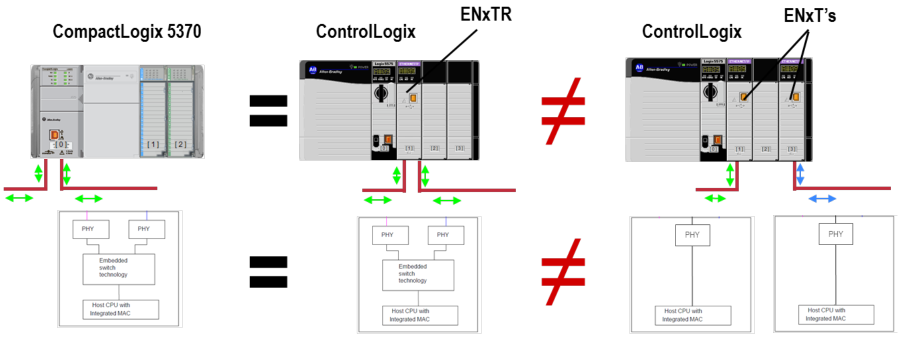


Figure10: PACs with multiple NICs vs. 2 port embedded switch technology

Note that the ControlLogix and CompactLogix L4x platforms can support multiple network interface cards (NICs) to segment network traffic. However, the CompactLogix 5370 platform is not capable of this method of network segmentation. The two ports of the CompactLogix 5370 PAC are part of an embedded switch, not a dual NIC.

Converged Plant-wide/Site-wide Network of CompactLogix-based Converged Plantwide Ethernet Cell/Area Zones

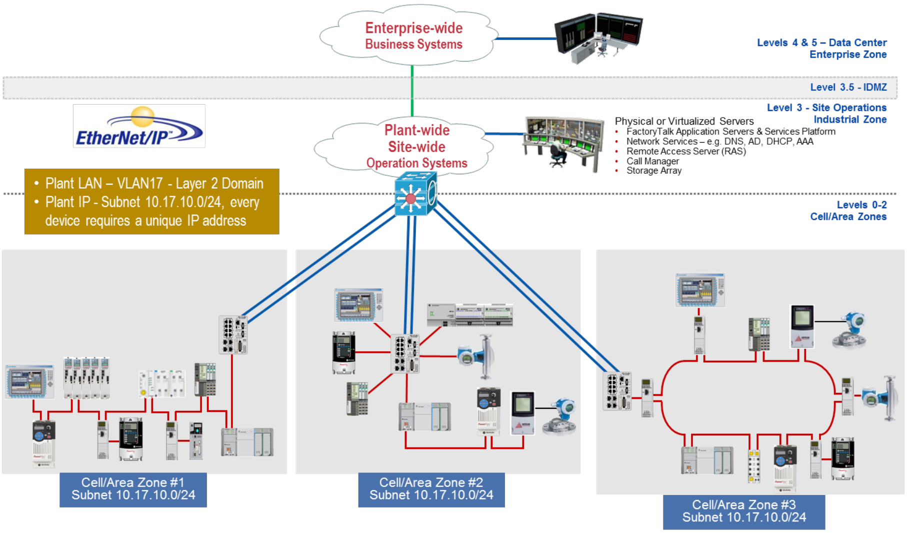

Enterprise-wide
Business Systems
Levels 4 & 5 – Data Center
Enterprise Zone
Level 3.5 - IDMZ
Level 3 - Site Operations
Industrial Zone
EtherNet/IP
Plant-wide
Site-wide
Operation Systems
Physical or Virtualized Servers
FactoryTalk Application Servers & Services Platform
Network Services – e.g. DNS, AD, DHCP, AAA
Remote Access Server (RAS)
Call Manager
Storage Array
Plant LAN – VLAN17 - Layer 2 Domain
Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address
Levels 0-2
Cell/Area Zones
Cell/Area Zone #1
Subnet 10.17.10.0/24
Cell/Area Zone #2
Subnet 10.17.10.0/24
Cell/Area Zone #3
Subnet 10.17.10.0/24

Figure 11: No network segmentation (not recommended) - common Layer 2 domain with each device requiring a unique IP address

In this system there are three Cell/Area Zones, each with different hardware and potentially from three unique OEMs who would like to protect their Intellectual Property (IP). Let's examine different techniques to accomplish the following:

1. Protect intellectual property of machine/process skid builders
2. Provide small Layer 2 domains of trust and broadcast domains
3. Provide logical Layer 2 building blocks to ensure a future-ready network
4. Enable Network Address Translation on a plant-wide/site-wide network to provide IP subnet repeatability at the Cell/Area Zone level, providing faster commissioning time for machine/process skid builders

Plant-wide/Site-wide Network with ControlLogix Converged Plantwide Ethernet Cell/Area Controller Providing Physical Segmentation

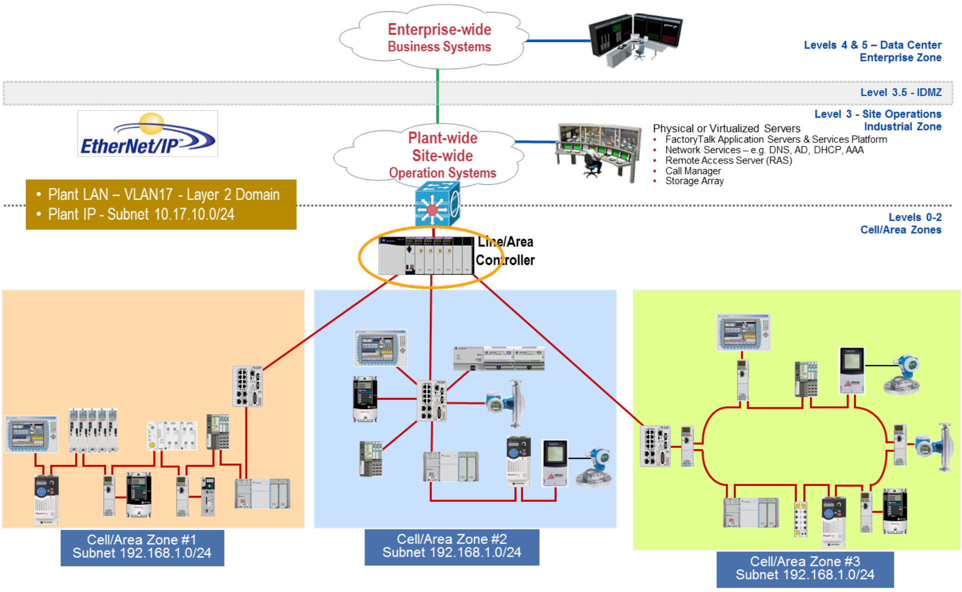


Figure 12: Repeating IP subnets between CPwE Cell/Area Zones. ControlLogix with multiple NICs providing logical segmentation for both Layer 2 domains and IP subnetting

In this example, a ControlLogix platform has been added to provide physical segmentation CIP Bridge between the plant-wide/site-wide network and the Cell/Area Zones

- The plant/site network is on a separate IP subnet than the Cell/Area Zones
- The Cell/Area Zones are able to re-use IP subnets, as they are physically segmented from each other via the ControlLogix backplane
- CIP traffic can still traverse the ControlLogix backplane, so other methods should be applied by OEMs to protect their intellectual property
- This is not a converged architecture, nor a scalable future-ready network-each time a new Cell/Area Zone is added, reconfiguration of the Line/Area controller will need to take place

Plant-wide/Site-wide Network with Network Address Translation Providing IP Subnet Repeatability

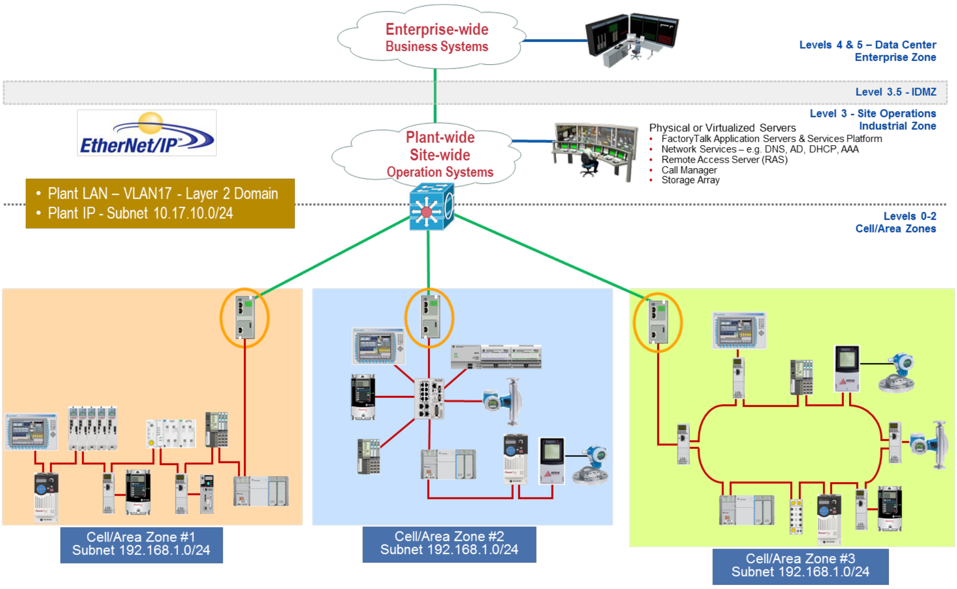


Figure 13: Repeating IP subnets between CPwE Cell/Area Zones. Translating IP addresses using network address translation appliances

In this example, all nodes within the Cell/Area Zones must have a unique IP address. IP addresses can be reused across Cell/Area Zones, allowing OEMs to repeat IP subnets while still allowing for a converged network.

- In this example a NAT appliance is placed between each Cell/Area Zone to provide Network Address Translation (ex. 9300-ENA)
- From the Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP addresses can be re-used
- Each NAT appliance must be programmed to translate from the 192.168.1.0/24 IP subnet to the plant-wide/site-wide IP subnet. If the entire Cell/Area Zone needs to communicate with the plant-wide/site-wide network, then all devices must have their addresses manually translated
- This architecture complicates the plant-wide/site-wide side of the architecture to provide simplicity to the Cell/Area Zones and OEMs

Plant-wide/Site-wide CompactLogix Architectures utilizing Network Address Translation via Unified Threat Management Security Appliance

Machine/process skid builders can benefit from the repeatable IP subnets provided from NAT. It can also provide the benefit of smaller Layer 2 building blocks, allowing control over traffic traversing between IP subnets.

NAT can be implemented via a unified threat management security appliance such as the Stratix 5900. Each UTM appliance would be programmed to translate from the 192.168.1.0/24 IP subnet, to the plant-wide/site-wide IP subnet, similar to the stand alone NAT appliance. The UTM security appliance can provide an additional level of enhanced security to further segment Cell/Area Zones from the plant-wide/site-wide network and other Cell/Area Zones.

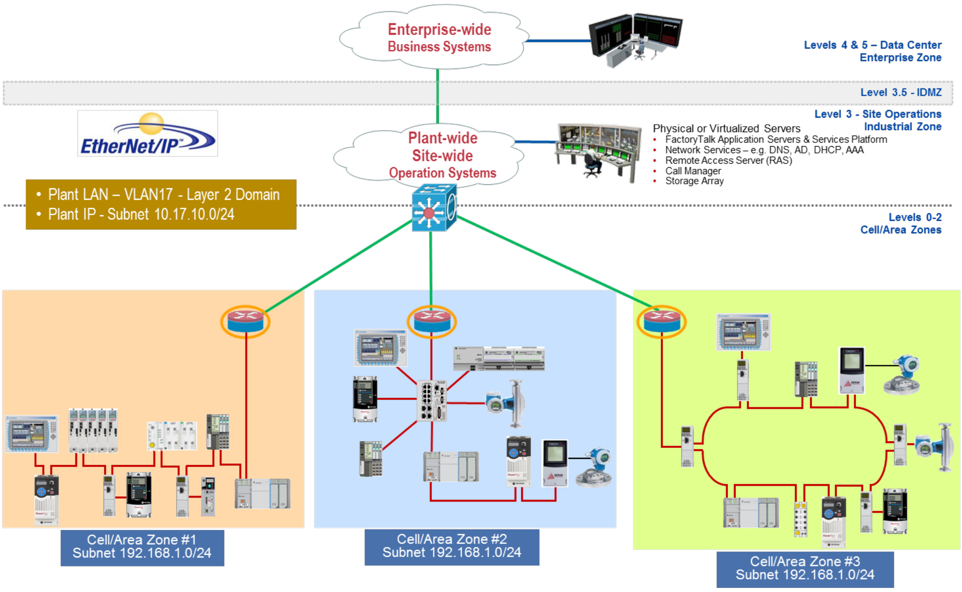


Figure 14: Repeating IP subnets between CPwE Cell/Area Zones. Translating IP addresses using Stratix 5900 Unified Threat Management Security Appliance.

- IP Schema – separate from plant/site, all nodes within the machine/process skid must have a unique IP address, IP addresses can be reused across machines/process skids
- In this example a UTM security appliance is placed between each Cell/Area Zone to provide Network Address Translation
- From the Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP Addresses can be re-used
- Each UTM security appliance must be programmed to translate from the 192.168.1.0/24 IP subnet to the plant-wide/site-wide IP subnet
- This architecture complicates the plant-wide/site-wide side of the architecture to provide simplicity to the Cell/Area Zones and machine/process skid builders

Plant-wide/Site-wide Network Segmentation using VLANs and Unique IP Subnets

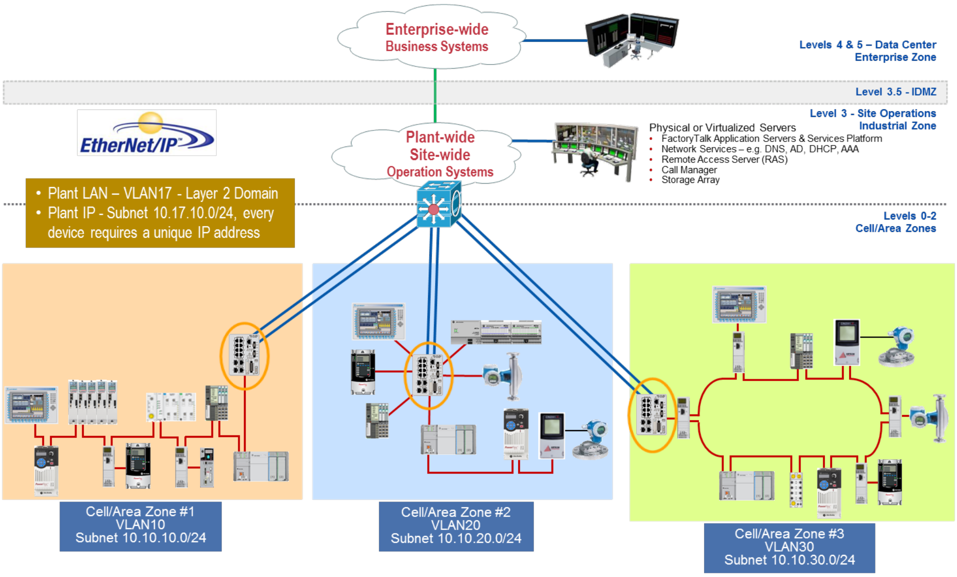

Enterprise-wide
Business Systems
Levels 4 & 5 – Data Center
Enterprise Zone
Level 3.5 - IDMZ
Level 3 - Site Operations
Industrial Zone
EtherNet/IP
Plant-wide
Site-wide
Operation Systems
Physical or Virtualized Servers
• FactoryTalk Application Servers & Services Platform
• Network Services – e.g. DNS, AD, DHCP, AAA
• Remote Access Server (RAS)
• Call Manager
• Storage Array
• Plant LAN – VLAN17 - Layer 2 Domain
• Plant IP - Subnet 10.17.10.0/24, every device requires a unique IP address
Levels 0-2
Cell/Area Zones
Cell/Area Zone #1
VLAN10
Subnet 10.10.10.0/24
Cell/Area Zone #2
VLAN20
Subnet 10.10.20.0/24
Cell/Area Zone #3
VLAN30
Subnet 10.10.30.0/24

Figure 15: Non repeating IP subnets (with each device requiring a unique IP address) between CPwE Cell/Area Zones. Stratix 5700 series switches - VLANs implemented to logically segment CPwE Cell/Area Zones.

In this example, all nodes within the Industrial Zones must have a unique IP address. IP addresses cannot be reused across machines/process skids or anywhere else within the Industrial Zone.

- Each Cell/Area Zone is segmented via a unique VLAN and IP subnet
- Note that CPwE VLAN best practices dictates that each Cell/Area Zone must have a unique IP subnet
- If Cell/Area Zones need to communicate between each other, they must communicate through a Layer 3 switch that can provide inter-VLAN routing
- This architecture provides small layer 2 domains of trust, fault domains and broadcast domains
- This architecture can help limit access between Cell/Area Zones to help provide restrictive access to machine/process skid builders' intellectual property
- Machine/process skid builders must adhere to addressing schema of plant-wide/site-wide network, potentially adding complication and time to commissioning

Plant-wide/Site-wide Network Segmentation using VLANs and Network Address Translation

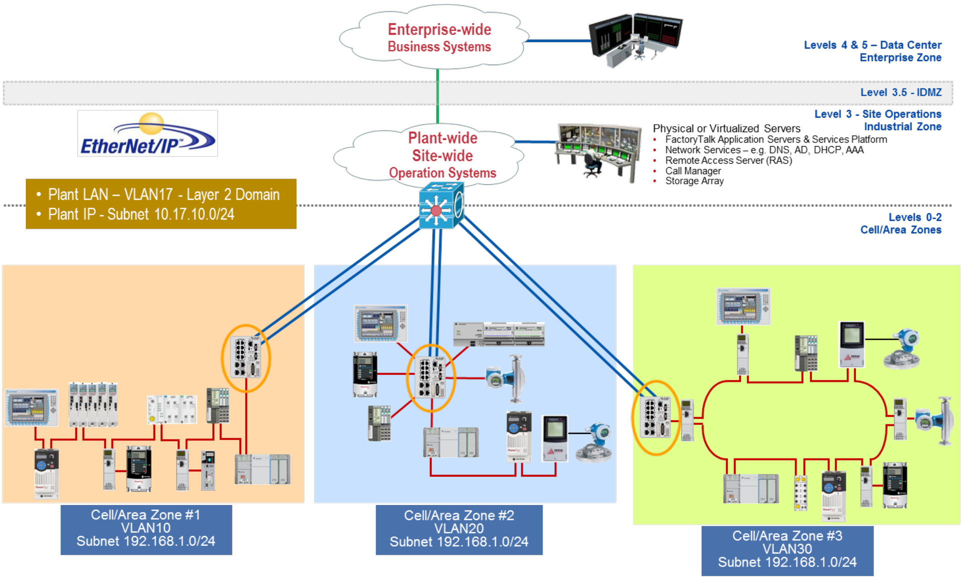


Figure 16: Repeating IP subnets between CPwE Cell/Area Zones. Translating IP addresses using Stratix 5700 series switches. VLANs implemented to logically segment CPwE Cell/Area Zones.

In this example all nodes within the Cell/Area Zones must have a unique IP address. IP addresses can be reused across Cells/Areas. The Cell/Area Zones repeat IP subnets and are segmented from each other by utilizing VLANs.

- Each Cell/Area Zone is segmented via a unique VLAN
- If Cell/Area Zones need to communicate between each other, they must communicate through a Layer 3 switch that can provide inter-VLAN routing
- This architecture provides small layer 2 domains of trust, fault domains and broadcast domains
- This architecture can help limit access between Cell/Area Zones to help provide restrictive access to machine/process skid builders' intellectual property
- This architecture utilizes Network Address Translation provided by the Stratix 5700 switches
- From Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP Addresses can be re-used
- Each NAT appliance must be programmed to translate from the 192.168.1.0/24 IP subnet to the plant-wide/site-wide IP subnet. If the entire Cell/Area Zone needs to communicate with the plant-wide/site-wide network, then all devices must have their addresses manually translated
- This architecture complicates the plant-wide/site-wide side of the architecture to provide simplicity to the Cell/Area Zones and machine/process skid builders

Conclusions

A continuing trend in industrial networking is the convergence of technology, specifically industrial automation technology with information technology. This network technology convergence enables a plant-wide/site-wide EtherNet/IP network, utilizing a single industrial network technology over a common network infrastructure for multiple control and information disciplines. This network technology convergence requires an industrial network design methodology utilizing network structure and hierarchy to help maintain real-time network performance. A key objective is to create smaller Layer 2 networks to create scalable and future-ready network infrastructures, minimize broadcast and fault domains, create smaller domains of trust and reduce overall network sprawl (undisciplined network growth).

The purpose of this application guide was to highlight the design considerations of various network segmentation methodologies for ControlLogix and CompactLogix 5370 to enable:

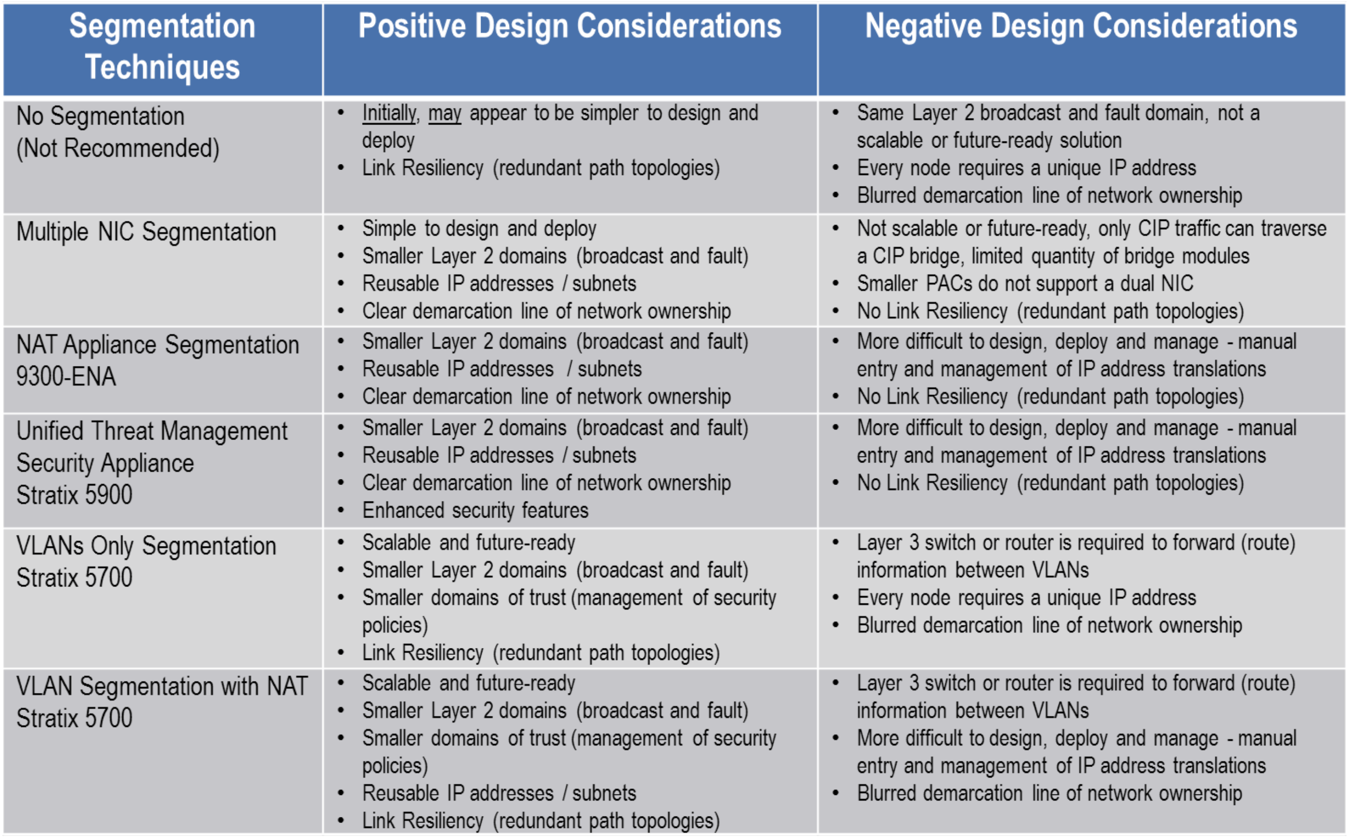
- Plant/site engineers to segment their industrial automation and control system (IACS) plant-wide/site-wide network infrastructure to help manage IACS traffic flow and segment policies – e.g. data prioritization and security
- OEMs (machine builders/process skid builders) to develop convergence-ready solutions to help simplify integration into their customer's plant-wide/site-wide network infrastructure

The choice of methodology to segment IACS traffic is dependent on multiple factors. Examples could be:

- Plant-wide/site-wide IACS application requirements
- OEM convergence-ready IACS applications – e.g. machine builders and process skid builders
- Company policies and procedures
- Applicable industry and regulatory standards
- Company organizational and support structure – e.g. lines of responsibilities for control system engineers and IT network engineers

The customer should understand these factors as well as the design considerations presented in this application guide when making design and deployment decisions during the process of choosing the appropriate segmentation methodology. Table 1 provides a general summary of design considerations for the various segmentation methodologies covered in this application guide.

Depending on a company's organizational structure, IACS networks might be owned by a plant-wide/site-wide control system engineer, an IT network engineer or combination of the two. Regardless, a collaboration of industrial automation and information technology domains is essential for successful design and deployment of IACS network architectures.



Segmentation Techniques	Positive Design Considerations	Negative Design Considerations
No Segmentation (Not Recommended)	• Initially, may appear to be simpler to design and deploy • Link Resiliency (redundant path topologies)	• Same Layer 2 broadcast and fault domain, not a scalable or future-ready solution • Every node requires a unique IP address • Blurred demarcation line of network ownership
Multiple NIC Segmentation	• Simple to design and deploy • Smaller Layer 2 domains (broadcast and fault) • Reusable IP addresses / subnets • Clear demarcation line of network ownership	• Not scalable or future-ready, only CIP traffic can traverse a CIP bridge, limited quantity of bridge modules • Smaller PACs do not support a dual NIC • No Link Resiliency (redundant path topologies)
NAT Appliance Segmentation 9300-ENA	• Smaller Layer 2 domains (broadcast and fault) • Reusable IP addresses / subnets • Clear demarcation line of network ownership	• More difficult to design, deploy and manage - manual entry and management of IP address translations • No Link Resiliency (redundant path topologies)
Unified Threat Management Security Appliance Stratix 5900	• Smaller Layer 2 domains (broadcast and fault) • Reusable IP addresses / subnets • Clear demarcation line of network ownership • Enhanced security features	• More difficult to design, deploy and manage - manual entry and management of IP address translations • No Link Resiliency (redundant path topologies)
VLANs Only Segmentation Stratix 5700	• Scalable and future-ready • Smaller Layer 2 domains (broadcast and fault) • Smaller domains of trust (management of security policies) • Link Resiliency (redundant path topologies)	• Layer 3 switch or router is required to forward (route) information between VLANs • Every node requires a unique IP address • Blurred demarcation line of network ownership
VLAN Segmentation with NAT Stratix 5700	• Scalable and future-ready • Smaller Layer 2 domains (broadcast and fault) • Smaller domains of trust (management of security policies) • Reusable IP addresses / subnets • Link Resiliency (redundant path topologies)	• Layer 3 switch or router is required to forward (route) information between VLANs • More difficult to design, deploy and manage - manual entry and management of IP address translations • Blurred demarcation line of network ownership

Table 1: General summary of design considerations for the various segmentation methodologies

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

Americas: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel: (1) 414.382.2000, Fax: (1) 414.382.4444
Europe/Middle East/Africa: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Belgium, Tel: (32) 2 663 0600, Fax: (32) 2 663 0640
Asia Pacific: Rockwell Automation, Level 14, Core F, Cyberport 3, 100 Cyberport Road, Hong Kong, Tel: (852) 2887 4788, Fax: (852) 2508 1846

Publication ENET-AT004B-EN-E – June 2013