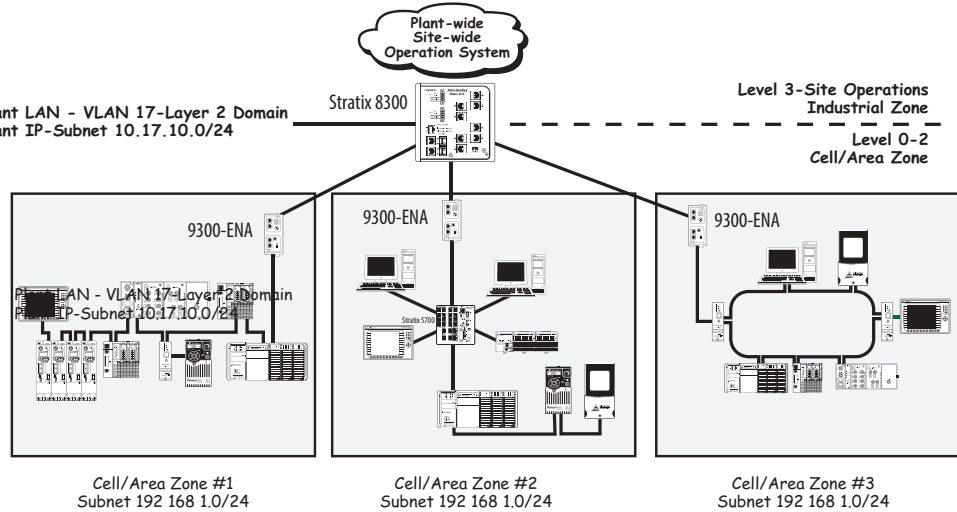


# Rockwell Automation and EtherNet/IP Provide Multiple Options to Connect to Your Plant Network Using Standard Ethernet Technology

## Plant-wide/Site-wide Network using Stratix 9300-ENAs with NAT Providing IP Subnet Repeatability

## Plant-wide/Site-wide Network using Stratix 5700's with VLANs and NAT

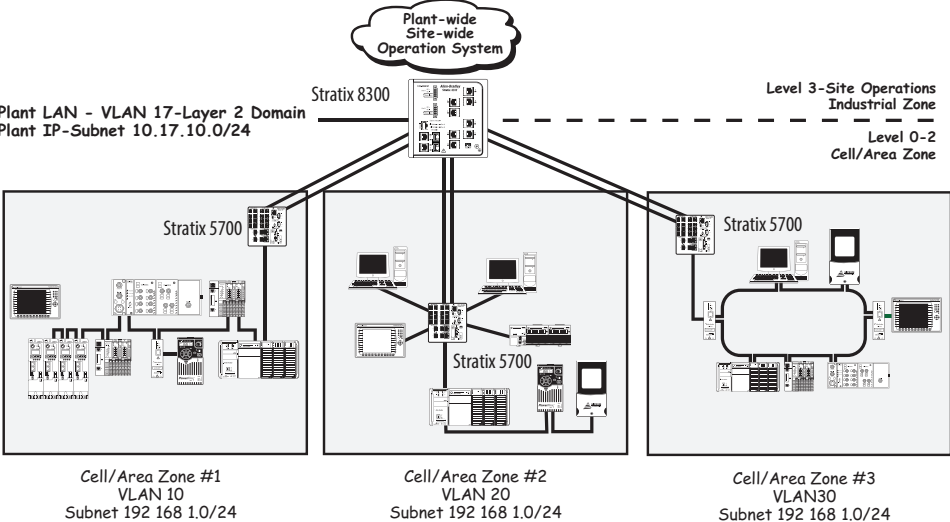
## Plant-wide/Site-wide Network using Stratix 5900's with NAT Providing IP Subnet Repeatability



### Repeating IP subnets between CPwE Cell/Area Zones. Translating IP addresses using 9300-ENA network address translation appliances

In this example, IP addresses can be reused across Cell/Area Zones, allowing OEMs to repeat IP subnets while still allowing for a converged network.

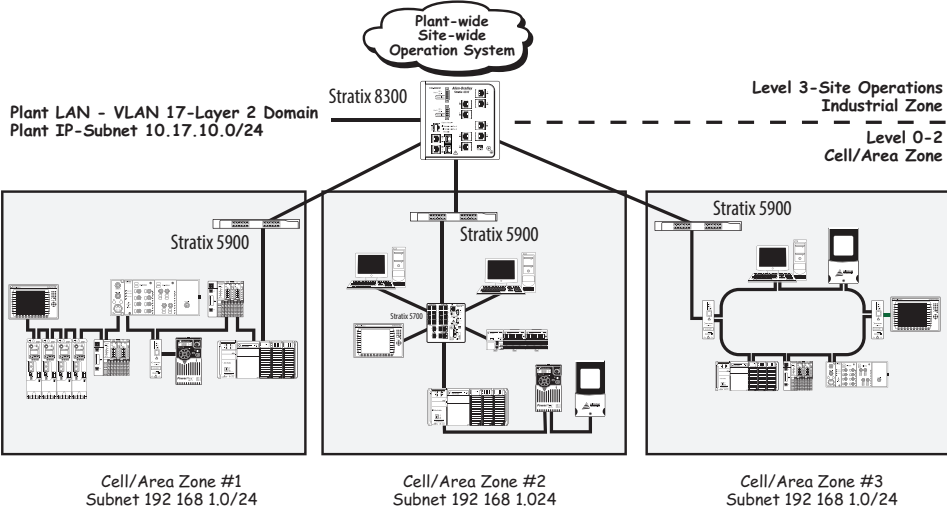
- A 9300-ENA appliance is placed between each Cell/Area Zone to provide Network Address Translation .
- From the Level 3, the site operations are able to access all devices
- Between each individual Cell/Area Zone, IP addresses can be re-used
- Each 9300-ENA must be programmed to translate from the 192.168.1.0/24 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



### 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, IP addresses can be reused across Cell/Area Zones, allowing OEMs to repeat IP subnets while still allowing for a converged network. 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 such as the Stratix 8300 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
- 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 Stratix 5700 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



### Repeating IP subnets between CPwE Cell/Area Zones. Translating IP addresses using Stratix 5900 Unified Threat Management Security Appliance with NAT

In this example, IP addresses can be reused across Cell/Area Zones, allowing OEMs to repeat IP subnets while still allowing for a converged network. NAT also provides the benefit of smaller Layer 2 building blocks, allowing control over traffic traversing between IP subnets.

NAT can be implemented via the Stratix 5900 unified threat management security 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.

- 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

Note: Information presented here is for illustrative purposes only

**Rockwell Automation**

Segmentation Via Network Address Translation

# Summary of Considerations for Segmentation Methodologies

Segmentation Techniques	Positive Design Considerations	Negative Design Considerations
No Segmentation (Not Recommended)	<ul style="list-style-type: none"><li>Initially, may appear to be simple to design anddeploy</li><li>Link Resiliency (redundant path topologies)</li></ul>	<ul style="list-style-type: none"><li>Same Layer 2 broadcast and fault domain, not a scalable or future ready solution.</li><li>Every node requires a unique IP address</li><li>Blurred demarcation line of network ownership</li></ul>
Multiple NIC Segmentation (ControlLogix Only)	<ul style="list-style-type: none"><li>Simple to design and deploy</li><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Reusable IP addresses/subnets</li><li>Clear demarcation of network ownership</li></ul>	<ul style="list-style-type: none"><li>Not scalable or future ready, only CIP traffic can traverse a CIP bridge, limited quantity of bridge modules.</li><li>Smaller PACs do not support a dual NIC.</li><li>No Link Resiliency (redundant path topologies)</li></ul>
NAT Appliance Segmentation 9300-ENA	<ul style="list-style-type: none"><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Reusable IP addresses/subnets</li><li>Clear demarcation of network ownership</li></ul>	<ul style="list-style-type: none"><li>More difficult to design, deploy, and manage-manual entry and management of IP address translations</li><li>No Link resiliency (redundant path topologies)</li></ul>
Unified Threat Management Security Appliance with NAT Stratix 5900	<ul style="list-style-type: none"><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Reusable IP addresses/subnets</li><li>Clear demarcation of network ownership</li><li>Enhanced security features</li></ul>	<ul style="list-style-type: none"><li>More difficult to design, deploy, and manage-manual entry and management of IP address translations</li><li>No Link resiliency (redundant path topologies)</li></ul>
VLANs Only Segmentation Stratix 5700	<ul style="list-style-type: none"><li>Scalable and future ready</li><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Smaller domains of trust (management of security policies)</li><li>Link Resiliency (redundant path configuration)</li></ul>	<ul style="list-style-type: none"><li>Layer 3 switch or router is required to forward (route) information between VLANs</li><li>Every node requires a unique IP address</li><li>Blurred demarcation line of network ownership</li></ul>
VLAN Segmentation with NAT Stratix 5700	<ul style="list-style-type: none"><li>Scalable and future ready</li><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Smaller domains of trust (management of security policies)</li><li>Reusable IP addresses/subnets</li><li>Link Resiliency (redundant path configuration)</li></ul>	<ul style="list-style-type: none"><li>Layer 3 switch or router is required to forward (route) information between VLANs</li><li>More difficult to design, deploy, and manage-manual entry and management of IP address translations</li><li>Blurred demarcation line of network ownership</li></ul>

## Bill of Material

Qty	Catalog #	Description System: Communication Hardware
1	1783-BMS10CL	Stratix 5700 Layer 2 Managed Switch, 10 Ports Lite
1	1783-BMS10CGN	Stratix 5700 Layer 2 Managed Switch, 10 Ports,Full with CIP Synch and NAT
1	1783-RMS10T	Stratix 8300 Layer 3 Managed Switch, 10 Ports
1	1783-MS10T	Stratix 8000 Layer 2 Managed Switch, 10 Ports
1	1783-SR	Stratix 5900 Security Appliance
1	9300-ENA	Network Address Translation Appliance

# About the Products

## Stratix 5700

- Scalable Layer 2 managed industrial switch
- Default configurations for industrial autom ation and EtherNet/IP devices (Global and Smartports)
- Studio 5000 for configuration via Add on Profiles/Predefined Logix tags for diagnostics
- FactoryTalk View Faceplates for status monitoring and alarming
- Best of Cisco - Catalyst® switch architecture/ feature set

## Stratix 8300

- Full Layer 3 industrial switch that supports routing between Subnets and VLANs.
- Default configurations for industrial automation and EtherNet/IP devices (Global and Smartports)
- Studio 5000 for configuration via Add on Profiles/Predefined Logix tags for diagnostics
- FactoryTalk View Faceplates for status monitoring and alarming
- Best of Cisco - Catalyst® switch architecture/ feature set

## Stratix 5900

- Combines a number of modern security functions into a single appliance
- Managed router that also provides a number of managed switching features
- A single device to implement VPN, Firewall, NAT, and many other services
- Best of Cisco - Fully integrated with Cisco IOS

## 9300-ENA

- NAT Appliance allowing identical machines to be placed on Ethernet networks

# About this Configuration

This system consists of three Cell/Area Zones, each with different hardware and potentially from three unique OEMs who would like to protect their Intellectual Property (IP). It illustrates different techniques to accomplish the following:

- Protect intellectual property of machine/process skid builders
- Provide small Layer 2 domains of trust and broadcast domains
- Provide logical Layer 2 building blocks to ensure a future-ready network
- 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

## Product Reference Table

Product	Managed Layer 2 Switch	NAT Mapping	Full Layer 3 Routing
Stratix 5700	X	X	
Stratix 5900		X	X
Stratix 8000	X		
Stratix 8300	X		X
9300-ENA		X	

Reference Architecture Web Page  
<http://www.rockwellautomation.com/rockwellautomation/products-technologies/network-technology/architectures.page>

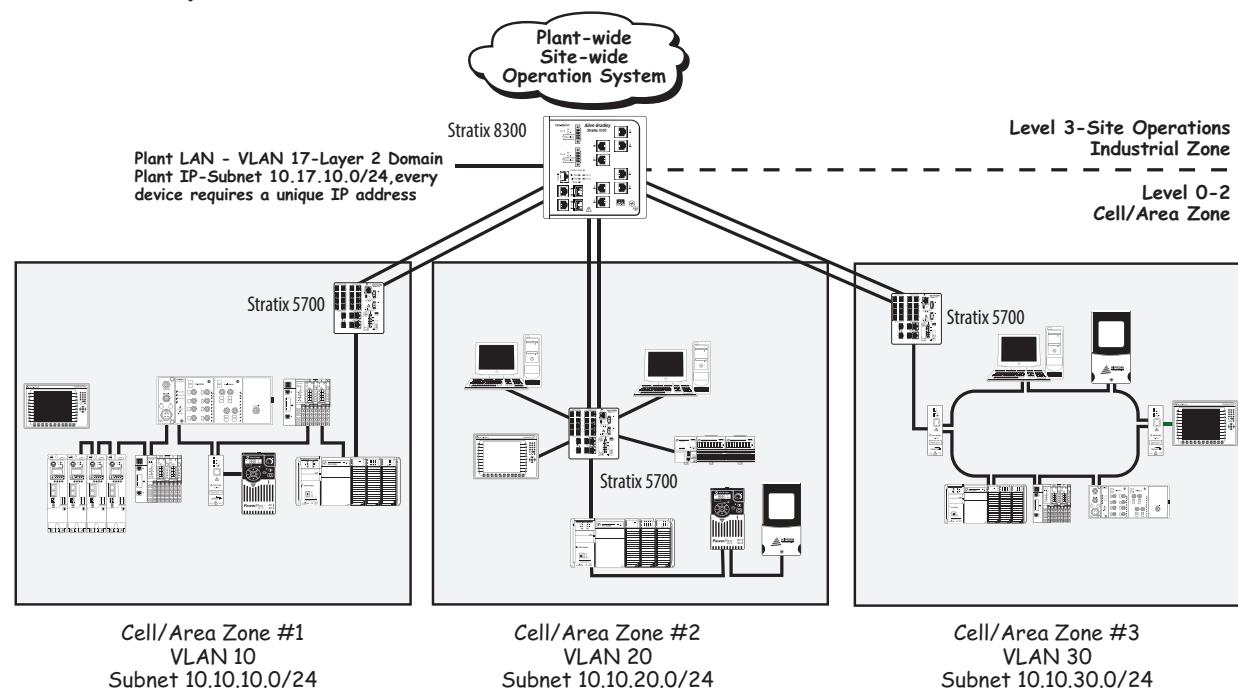
## Additional Resources

ENET-PP005C-EN-E	Stratix 5700 Industrial Ethernet Switch Product Profile
ENET-PP002B-EN-P	Stratix 8000 and 8300 Industrial Ethernet Switches Product Profile
ENET-PP006A-EN-P	Stratix 5900 Services Router Product Profile
ENET-AT004B-EN-E	Segmentation Methods within the Cell / Area Zone
IASIMP-QS038A-EN-P	Stratix 5700 NAT Quick Start
ENET-WP032A-EN-E	Stratix 5700 NAT Whitepaper
ENET-QR001-EN-E	Stratix Switch Reference Chart
ENET-QR002-EN-E	Stratix 5700 Reference Chart
GMSP-PP001-EN-E	9300-ENA Network Address Translation Device Product Profile
IASIMP-QR029A-EN-P	Stratix/Infrastructure Product Family Quick Reference Drawing
ENET-TD001-EN-P	Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (DIG)



# Rockwell Automation and EtherNet/IP Provide Multiple Options to Connect to Your Plant Network Using Standard Ethernet Technology

## Plant-wide/Site-wide Network using Stratix 5700's with VLANs and Unique IP Subnets

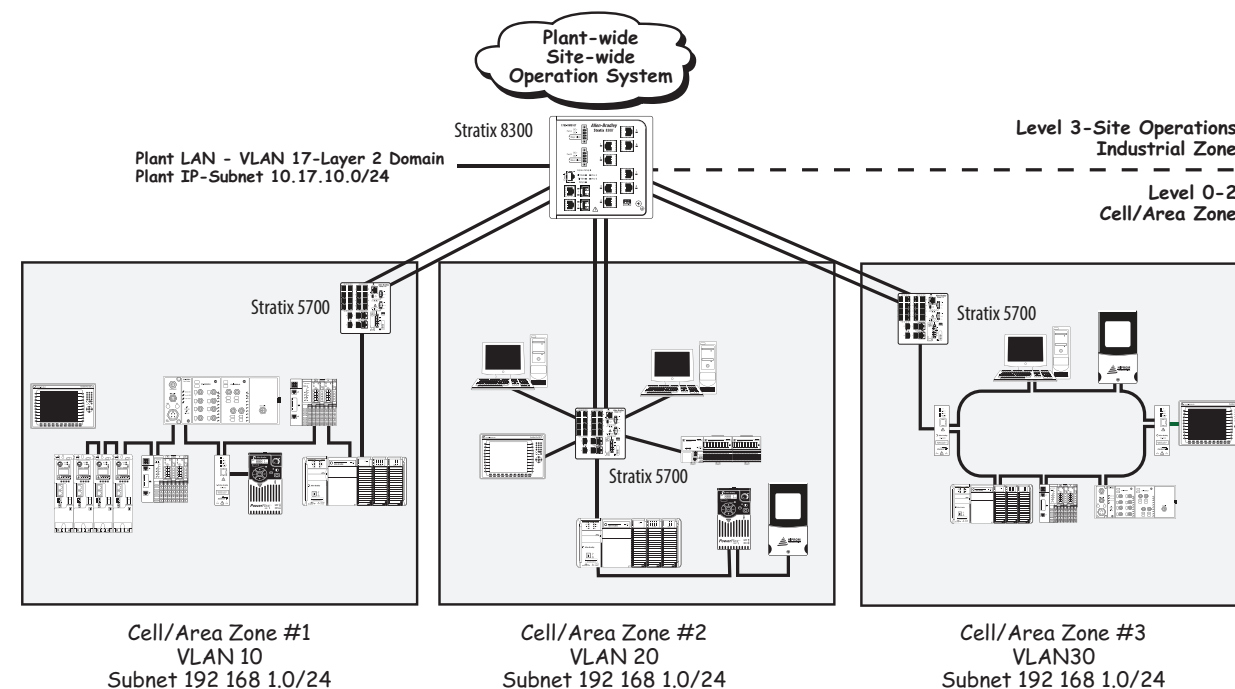


**Non repeating IP subnets (with each device requiring a unique IP address) between CPwE Cell/Area Zones. Stratix 5700 series switches - VLANs implemented to logically segment CPwE Cell/Area Zones.**

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 such as the Stratix 8300 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 using Stratix 5700's with VLANs and NAT



**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, IP addresses can be reused across Cell/Area Zones, allowing OEMs to repeat IP subnets while still allowing for a converged network. 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 such as a Stratix 8300 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 Stratix 5700 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

# Summary of Considerations for Segmentation Methodologies

Segmentation Techniques	Positive Design Considerations	Negative Design Considerations
No Segmentation (Not Recommended)	<ul style="list-style-type: none"><li>Initially, may appear to be simple to design anddeploy</li><li>Link Resiliency (redundant path topologies)</li></ul>	<ul style="list-style-type: none"><li>Same Layer 2 broadcast and fault domain, not a scalable or future ready solution.</li><li>Every node requires a unique IP address</li><li>Blurred demarcation line of network ownership</li></ul>
Multiple NIC Segmentation (ControlLogix Only)	<ul style="list-style-type: none"><li>Simple to design and deploy</li><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Reusable IP addresses/subnets</li><li>Clear demarcation of network ownership</li></ul>	<ul style="list-style-type: none"><li>Not scalable or future ready, only CIP traffic can traverse a CIP bridge, limited quantity of bridge modules.</li><li>Smaller PACs do not support a dual NIC.</li><li>No Link Resiliency (redundant path topologies)</li></ul>
NAT Appliance Segmentation 9300-ENA	<ul style="list-style-type: none"><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Reusable IP addresses/subnets</li><li>Clear demarcation of network ownership</li></ul>	<ul style="list-style-type: none"><li>More difficult to design, deploy, and manage-manual entry and management of IP address translations</li><li>No Link resiliency (redundant path topologies)</li></ul>
Unified Threat Management Security Appliance with NAT Stratix 5900	<ul style="list-style-type: none"><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Reusable IP addresses/subnets</li><li>Clear demarcation of network ownership</li><li>Enhanced security features</li></ul>	<ul style="list-style-type: none"><li>More difficult to design, deploy, and manage-manual entry and management of IP address translations</li><li>No Link resiliency (redundant path topologies)</li></ul>
VLANs Only Segmentation Stratix 5700	<ul style="list-style-type: none"><li>Scalable and future ready</li><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Smaller domains of trust (management of security policies)</li><li>Link Resiliency (redundant path configuration)</li></ul>	<ul style="list-style-type: none"><li>Layer 3 switch or router is required to forward (route) information between VLANs</li><li>Every node requires a unique IP address</li><li>Blurred demarcation line of network ownership</li></ul>
VLAN Segmentation with NAT Stratix 5700	<ul style="list-style-type: none"><li>Scalable and future ready</li><li>Smaller Layer 2 domains (broadcast and fault)</li><li>Smaller domains of trust (management of security policies)</li><li>Reusable IP addresses/subnets</li><li>Link Resiliency (redundant path configuration)</li></ul>	<ul style="list-style-type: none"><li>Layer 3 switch or router is required to forward (route) information between VLANs</li><li>More difficult to design, deploy, and manage-manual entry and management of IP address translations</li><li>Blurred demarcation line of network ownership</li></ul>

## Bill of Material

Qty	Catalog #	Description System: Communication Hardware
1	1783-BMS10CL	Stratix 5700 Layer 2 Managed Switch, 10 Ports Lite
1	1783-BMS10CGN	Stratix 5700 Layer 2 Managed Switch, 10 Ports,Full with CIP Synch and NAT
1	1783-RMS10T	Stratix 8300 Layer 3 Managed Switch, 10 Ports
1	1783-MS10T	Stratix 8000 Layer 2 Managed Switch, 10 Ports
1	1783-SR	Stratix 5900 Security Appliance
1	9300-ENA	Network Address Translation Appliance

# About the Products

## Stratix 5700

- Scalable Layer 2 managed industrial switch
- Default configurations for industrial autom ation and EtherNet/IP devices (Global and Smartports)
- Studio 5000 for configuration via Add on Profiles/Predefined Logix tags for diagnostics
- FactoryTalk View Faceplates for status monitoring and alarming
- Best of Cisco - Catalyst® switch architecture/ feature set

## Stratix 8300

- Full Layer 3 industrial switch that supports routing between Subnets and VLANs.
- Default configurations for industrial automation and EtherNet/IP devices (Global and Smartports)
- Studio 5000 for configuration via Add on Profiles/Predefined Logix tags for diagnostics
- FactoryTalk View Faceplates for status monitoring and alarming
- Best of Cisco - Catalyst® switch architecture/ feature set

## Stratix 5900

- Combines a number of modern security functions into a single appliance
- Managed router that also provides a number of managed switching features
- A single device to implement VPN, Firewall, NAT, and many other services
- Best of Cisco - Fully integrated with Cisco IOS

## 9300-ENA

- NAT Appliance allowing identical machines to be placed on Ethernet networks

# About this Configuration

This system consists of three Cell/Area Zones, each with different hardware and potentially from three unique OEMs who would like to protect their Intellectual Property (IP). It illustrates different techniques to accomplish the following:

- Protect intellectual property of machine/process skid builders
- Provide small Layer 2 domains of trust and broadcast domains
- Provide logical Layer 2 building blocks to ensure a future-ready network
- 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

## Product Reference Table

Product	Managed Layer 2 Switch	NAT Mapping	Full Layer 3 Routing
Stratix 5700	X	X	
Stratix 5900		X	X
Stratix 8000	X		
Stratix 8300	X		X
9300-ENA		X	

## Additional Resources

ENET-PP005C-EN-E	Stratix 5700 Industrial Ethernet Switch Product Profile
ENET-PP002B-EN-P	Stratix 8000 and 8300 Industrial Ethernet Switches Product Profile
ENET-PP006A-EN-P	Stratix 5900 Services Router Product Profile
ENET-AT004B-EN-E	Segmentation Methods within the Cell / Area Zone
IASIMP-QS038A-EN-P	Stratix 5700 NAT Quick Start
ENET-WP032A-EN-E	Stratix 5700 NAT Whitepaper
ENET-QR001-EN-E	Stratix Switch Reference Chart
ENET-QR002-EN-E	Stratix 5700 Reference Chart
GMSP-PP001-EN-E	9300-ENA Network Address Translation Device Product Profile
IASIMP-QR029A-EN-P	Stratix/Infrastructure Product Family Quick Reference Drawing
ENET-TD001-EN-P	Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (DIG)