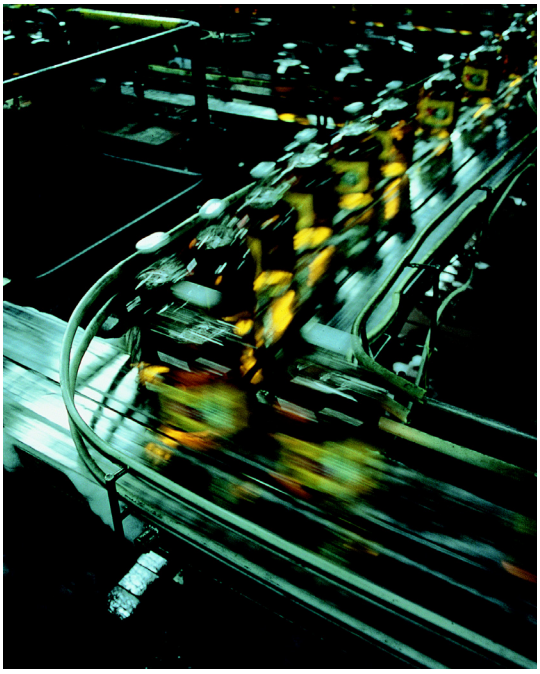


Migrating Legacy IACS Networks to a Converged Plantwide Ethernet Architecture

Design and Implementation Guide

January 2016

Cisco Validated Design

Document Reference Number: ENET-TD011A-EN-P

Preface

This *Migrating Legacy IACS Networks to a Converged Plantwide Ethernet (CPwE) Cisco Validated Design (CVD)*, which is documented in a Design and Implementation Guide (DIG), outlines two application use cases for migrating a traditional Industrial Automation and Control System (IACS) network architecture to standard Ethernet and IP networking technologies to support the Industrial Internet of Things (IoT). This DIG highlights the key IACS application requirements, technology and supporting design considerations to help with the successful design and deployment of these specific use cases within the framework of CPwE.

Note In the traditional CPwE campus model, all routing is done at the Layer 3 distribution switch. This CVD deviates from that model in order to address the specific requirements of the application use cases documented within this DIG.

Note This release of the CPwE architecture focuses on EtherNet/IP, which utilizes the ODVA Common Industrial Protocol (CIP™), and is ready for the Industrial IoT. For more information on EtherNet/IP, see odva.org at the following URL:

- http://www.odva.org/Technology-Standards/EtherNet-IP/Overview

Document Organization

The *Migrating Legacy IACS Networks to a Converged Plantwide Ethernet Architecture DIG* contains the following chapters and appendices:

Chapter or Appendix	Description
"Migrating Legacy IACS Networks to a Converged Plantwide Ethernet Architecture"	Provides an overview of the IACS application use cases and introduces the standard networking technologies used to address the use cases.
"System Design Considerations"	Provides an architectural framework and design considerations for the application use cases.
"Configuring the Infrastructure"	Describes how to configure and implement the design considerations of the previous chapters.
"Troubleshooting Tips"	Describes how to assess and verify the status of the Connected Routing and Layer 2 NAT.
"Migrating Legacy IACS Networks to a CPwE Architecture Test Results"	Provides latency results from scaled testing of the application use cases.
"CPwE References"	List of references for CPwE, Connected Routing, and Layer 2 NAT concepts discussed in this document.

Chapter or Appendix	Description
"Test Hardware and Software"	List of hardware and software components used in validation of this CVD.
"Acronyms and Initialisms"	List of acronyms and initialisms used in this document.

For More Information

More information on CPwE Design and Implementation Guides can be found at the following URLs:

Rockwell Automation site:

- http://www.rockwellautomation.com/global/products-technologies/network-technology/architectures.page?

Cisco site:

- http://www.cisco.com/c/en/us/solutions/enterprise/design-zone-manufacturing/landing_ettf.html

CHAPTER 1

Migrating Legacy IACS Networks to a Converged Plantwide Ethernet Architecture

This chapter includes the following major topics:

The prevailing trend in IACS networking is the convergence of technology, specifically IACS Operational Technology (OT) with Information Technology (IT). CPwE helps enable network technology convergence through the use of standard Ethernet and Internet Protocol (IP) technology. A converged IACS network technology enables the Industrial Internet of Things and helps to facilitate:

- Multi-discipline application convergence, including discrete, continuous process, batch, drive, safety, motion, power, time synchronization, supervisory information, asset configuration/diagnostics and energy management
- Standard IT technology that is future-ready, with increased sustainability and minimized risk of deployment
- Better asset utilization through a common network infrastructure that can also help support lean initiatives
- Common toolsets and required skills/training, including assets for design, deployment and troubleshooting, as well as human assets
- Standard and established IT security technology, best practices, policies and procedures
- Seamless plant-wide/site-wide information sharing due to IP pervasiveness-routability and portability across data links (such as Ethernet and Wi-Fi)

Although technology has been the enabler behind OT and IT convergence, business aspects have also sustained a continual trend:

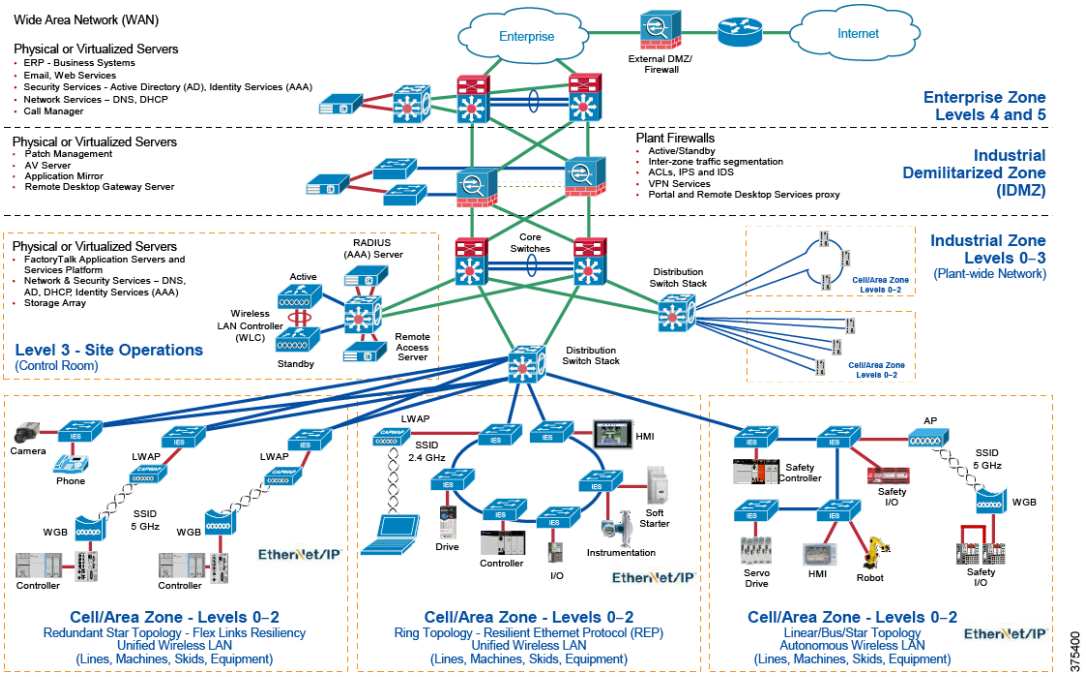
- **Integration**—Converging business systems with plant-wide/site-wide systems for more Key Performance Indicators (KPIs), regulatory compliance (such as genealogy and track and trace) and supply chain management
- **Connectivity**—More IACS devices connected for better IACS asset utilization, optimization and management
- **Applications**—Expanded application support (such as energy management and sustainability initiatives)

- **Collaboration**—OT and IT groups, who previously had little interaction, are now collaborating to share standards, best practices, innovations and security policies, procedures and technology

This *Migrating Legacy IACS Networks to CPwE DIG* outlines two application use cases for migrating a traditional IACS network architecture to standard Ethernet and IP network technologies. CPwE is the underlying architecture that provides standard network services for control and information disciplines, devices and equipment found in modern IACS applications. The CPwE architecture (Figure 1-1) provides design and implementation guidance that can help to achieve the real-time communication, reliability, scalability, security and resiliency requirements of the IACS.

This *Migrating Legacy IACS Networks to CPwE CVD*, which is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation, highlights the key IACS application requirements, technology and supporting design considerations to help with the successful design and deployment of migration use cases within the framework of CPwE.

Figure 1-1 CPwE Architectures



IACS Migration Use Case Requirements

An IACS is deployed in a wide variety of discrete and process manufacturing industries such as automotive, pharmaceuticals, consumer goods, pulp and paper, oil and gas, mining and energy. IACS applications are made up of multiple control and information disciplines such as continuous process, batch, discrete and hybrid combinations.

Manufacturers traditionally deployed multiple disparate network technologies (Figure 1-2) for their IACS applications to address multiple control and information disciplines. One of the challenges facing manufacturers is the complexities of migrating traditional IACS network technologies to standard Ethernet and IP networking technologies (Figure 1-3) to take advantage of the business benefits associated with the Industrial IoT.

Figure 1-2 Disparate IACS Network Technologies

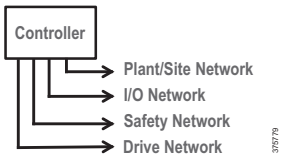
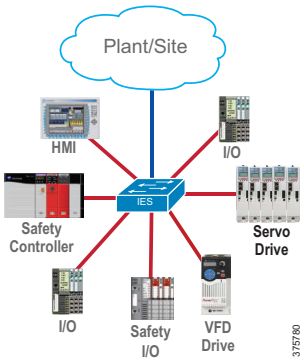


Figure 1-3 Single IACS Network Technology

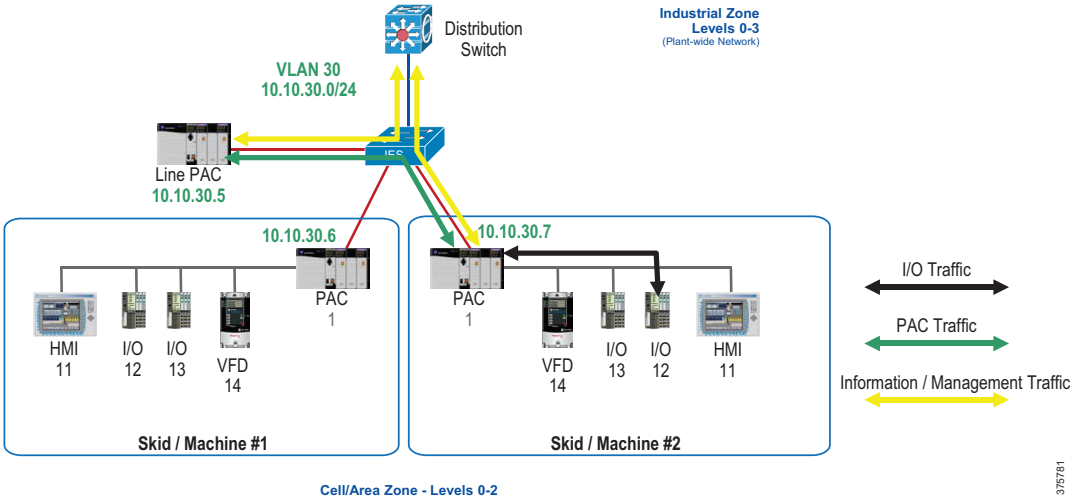


This *Migrating Legacy IACS Networks to CPwE DIG* outlines the concepts, requirements and technology solutions for two specific application use cases that were tested, validated and documented by Cisco and Rockwell Automation to migrate a traditional IACS network architecture (Figure 1-4) to a converged EtherNet/IP™ architecture (Figure 1-5). It is up to the reader to determine how this could be applied to their specific IACS migration application use cases.

As shown in Figure 1-4, use case requirements include:

- Maintain existing Programmable Automation Controllers (PACs) and replace Network Interface Cards (NICs)
- Maintain existing PAC subnet and IP addressing schema
- Maintain existing plant-wide virtual LAN (VLAN) structure for inter-PAC communications
- Maintain existing IACS input/output (I/O) platform and replace NICs and/or I/O adapter modules:
  - Migrate legacy IACS I/O network (non IP) to EtherNet/IP
- Maintain existing IACS devices, replace NICs such as Variable Frequency Drives (VFDs), instrumentation and Human Machine Interface (HMI):
  - Migrate legacy IACS device network (non IP) to EtherNet/IP
- For maintenance simplification, maintaining identical IP addressing for I/O and IACS devices across each skid/machine such as I/O, VFD, instrumentation and HMI
- For maintenance simplification, support by IACS OT personnel such as plant engineer, control system engineer and maintenance engineer
- Keep IACS I/O traffic local
- Keep IACS PAC traffic local
- Support plant-wide data acquisition
- Support plant-wide IACS asset management
- Support plant-wide network management

Figure 1-4 Use Case—Legacy IACS Network Architecture

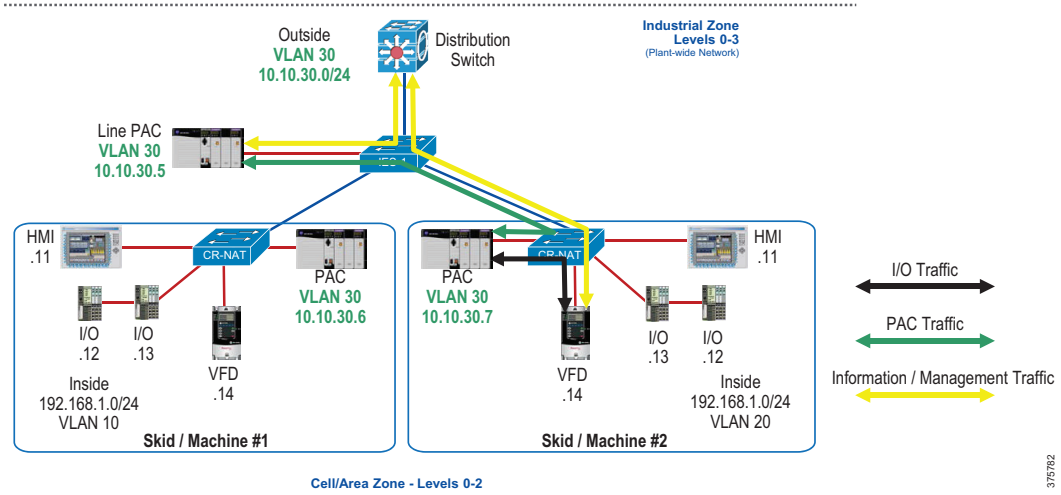


IACS Migration Technology

A variety of standard Ethernet and IP networking technology was applied to the *Migrating Legacy IACS Networks to CPwE CVD* to accomplish the requirements of specific application use cases (Figure 1-5):

- EtherNet/IP—Single IACS Network Technology
- Layer 2 Industrial Ethernet Switches (IES)
- Network Address Translation (NAT) within the Layer 2 IES
- Routing enabled within the Layer 2 IES—Connected and Static

Figure 1-5 Use Case—Converged EtherNet/IP Network Architecture



The *Migrating Legacy IACS Networks to CPwE CVD* builds atop the *Deploying Network Address Translation in a Converged Plantwide Ethernet Architecture DIG.* NAT within CPwE enables the reuse of IP addressing without introducing a duplicate IP address error into the IACS architecture. NAT translations have two forms:

one-to-one (1:1) and one-to-many (1:n). The *Migrating Legacy IACS Networks to CPwE CVD* includes tested and validated use cases utilizing 1:1 NAT, implemented from the Allen-Bradley® Stratix 5700™ or Cisco IE 2000 Layer 2 IES.

NAT within the Layer 2 IES helps to address the use case requirements:

- For maintenance simplification, NAT must maintain identical IP addressing for I/O and IACS devices across each skid/machine such as I/O, VFD, instrumentation and HMI.
- For maintenance simplification, NAT must be capable of being supported by IACS OT personnel such as plant engineer, control system engineer and maintenance engineer.

The *Migrating Legacy IACS Networks to CPwE CVD* introduces routing, specifically connected and static routing, within the Layer 2 IES to help keep control and information traffic closer to the edge of the IACS application. Routing helps to:

- Forward IACS control and information traffic between IACS devices on different IP subnets
- Create smaller broadcast domains by connecting yet segmenting multiple Layer 2 VLANs

Connected Routing, when used in conjunction with NAT functionality, helps enable routing between several NAT-connected IACS applications (skids, machines and lines) within the Cell/Area Zone. Several use cases have been tested and validated, allowing for architectural selections to be made based upon small (skid/machine) to large-scale (Line or Cell/Area Zone) plant-wide deployments.

Layer 2 Industrial Ethernet Switches

The Allen-Bradley Stratix 5400™, 5700 and Cisco Industrial Ethernet 2000 and 4000 IES support routing (connected and static) and NAT today. IES that supports Layer 2 NAT spans nine models of the Allen-Bradley Stratix and Cisco IES, including:

- Select models of the Cisco IE 2000 and IE 4000 series IES
- Select models of the Allen-Bradley Stratix 5400 and Stratix 5700 series IES

Connected Routing and NAT are network switch functions that allow control system engineers to build IACS applications using reused IP (IPv4) addresses behind separate IES, while also allowing those IACS applications to integrate into the larger plant-wide architecture where unique IP addressing is required. With NAT, the IES is configured to translate only specific IP addresses from inside the IACS application to the public plant-wide architecture.

Connected Routing within the CPwE architecture also addresses two key challenges:

- Limiting Layer 2 broadcast domains by segmenting with VLANs within the Cell/Area Zone
- Keeping all control traffic local, by routing locally between the VLANs within the IACS application such as skid/machine or Cell/Area Zone
- Reusing IP addresses across multiple skids/machines while providing direct access from the plant-wide network by using NAT within the Layer 2 IES

CHAPTER 2

System Design Considerations

This chapter, which describes design considerations for migrating legacy IACS networks to a Converged Plantwide Ethernet, includes the following major topics:

Routing Technologies Overview

The *Migrating Legacy IACS to CPwE CVD* uses static and connected IP routing on the access switch to provide Layer 3 connectivity between subnets on IE 2000/Stratix 5700 and IE 4000/Stratix 5400 switches with the LAN Base (default on NAT-enabled versions) license installed. These features do not require purchasing additional licenses.

Enabling IP routing on the IES switch allows it to route directly between connected subnets, which is known as *Connected Routing*. The switch learns connected routes when an IP address is configured on the Switched Virtual Interface (SVI) for each routed VLAN. Additional routes can be manually entered into the switch using static routes. Static routes are used to send traffic to other Layer 3 switches in the network, but do not change in response to topology changes in the network.

Table 2-1 describes the different types of routing. Note that only connected and static routing are included in the *Migrating Legacy IACS Networks to CPwE CVD*.

Table 2-1 Routing Types

Type	Network Path	Routing Paths	Supported by
Connected	Network path is automatically populated into the routing table when subnets are manually assigned to the local interface ports of the IES.	Limited to routing between subnets directly connected to the IES.	Layer 2 and Layer 3 IES

Table 2-1 Routing Types (continued)

Type	Network Path	Routing Paths	Supported by
Static	Network path is manually entered into the routing table and remains static until manual updates are made.	Supports routing to local and remote subnets (not directly connected to the IES).	Layer 2 and Layer 3 IES
Dynamic	Dynamically learns remote network paths and automatically populates the paths into the routing table.	Routing protocol between Layer 3 switches and routers to determine optimal network topology/path to subnets, and forwarding packets along those paths - that is, OSPF (Open Shortest Path First) and EIGRP (Enhanced Interior Gateway Routing Protocol).	Layer 3 IES

Connected and static routing within a Layer 2 IES helps to provide a cost effective and simplified solution that addresses the use case requirements of:

- Maintaining existing PAC subnet and IP addressing schema
- Maintaining existing plant-wide VLAN structure for inter-PAC communications
- Keeping IACS I/O traffic local by placing it in its own VLAN
- Keeping IACS PAC traffic local by allowing direct communication (no need to route via the distribution/core layer)
- For maintenance simplification, must be capable of being supported by IACS OT personnel such as plant engineer, control system engineer and maintenance engineer
- Supporting plant-wide data acquisition
- Supporting plant-wide IACS asset management
- Supporting plant-wide network management

Layer 2 NAT Technology Overview

Layer 2 NAT (NAT within a Layer 2 IES) is a networking technology that enables control system engineers to build IACS applications reusing IP (IPv4) addresses, while allowing those IACS applications to integrate into the larger plant-wide architecture. However, the integration to the plant-wide network still requires unique IP addresses for the translated IACS devices. NAT can be configured to translate only specific IP addresses from inside the IACS application (private network) to the outside plant-wide architecture (public network).

Note NAT devices may use words such as *public* to identify larger (that is, plant-wide) networks with a unique IP addressing scheme, and *private* to describe smaller (that is, machine-level) networks with reusable IP addresses. These terms should not be confused with the terms public and private when describing IP addresses routable on the Internet versus IP addresses reserved to be used in the local network (such as 192.168.x.x, 10.x.x.x, 172.16.x.x).The IE 2000/Stratix 5700 and IE 4000/Stratix 5400 use public/private terminology in the Device Manager GUI.

NAT translations have two forms: One to One (1:1) and One to Many (1: n):

- **One-to-One (1:1) NAT**—A service that assigns a unique public IP address to an private device with an existing private IP address. The device can then communicate on both the private and public subnets. This service is configured within a NAT-enabled device and is the public translation of the IP address physically programmed on the private device. NAT translations are typically entered into a table in the NAT-enabled device.

- **One-to-Many (1:n) NAT**—Also known as Transmission Control Protocol (TCP) / User Datagram Protocol (UDP) Port Address Translation (PAT), this service allows multiple devices on the private network to share one IP address on the public network. TCP/UDP ports are translated in addition to the IP address to facilitate this service. The most common use of 1:n NAT is to connect users to Internet. The Internet edge router is typically NAT-enabled and allows all individual private devices to access the Internet via the same single public address.

Layer 2 NAT is hardware-based implementation of 1:1 NAT on a Layer 2 switch that provides wire speed performance.

Note

- The products and architectures that are described in this document use the 1:1 form of NAT.
- For Layer 2 NAT to be implemented with Connected Routing described in this CVD, the IES must be running version 15.2(4)EA or later.
- For more information on Layer 2 NAT designs, see the *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture CVD* at the following URLs:
  - Rockwell Automation site:

    http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
  - Cisco site:

    http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

Connected Routing with Layer 2 NAT Design Considerations

In order to facilitate migration of Legacy IACS networks to CPwE, while helping to minimize impact to the existing IACS application, the controllers and I/O are placed in separate VLANs and Connected Routing is used to route between them. All the existing controllers with the unique plant-wide IP addresses reside on one common VLAN, whereas the I/O blocks have the same private IP addresses per each machine. Layer 2 NAT is enabled for reuse of IP addressing without introducing a duplicate IP address error in the IACS application architecture.

The IES for each machine acts as a default gateway/router for the controllers and I/O directly connected to it. If traffic needs to be routed outside the Cell/Area Zone, static routing on the IES is required to forward (route) traffic to the distribution switch, which will then forward the traffic to its destination in the plant-wide network.

Layer 2 NAT is performed only on the devices with private IP addresses such as I/O. NAT is NOT performed on devices with public IP addresses such as engineering workstations or FactoryTalk® application servers. The following points summarize the data flow between the devices:

- Traffic between the PAC and I/O is routed using Connected Routing between two SVIs on the IES.
- Traffic between the devices in the same VLAN is switched.
- Traffic between the I/O and devices in the plant-wide network (engineering workstations or the FactoryTalk application servers) is routed by the IES using connected and static routes. Layer 2 NAT is applied by the same switch.

In summary, Connected Routing, in conjunction with Layer 2 NAT, allows plant-wide reachability for controllers and I/O while keeping the controller to I/O traffic local to the Layer 2 access switch.

Note The Layer 2 NAT configuration for the Connected Routing architecture defined in this CVD differs from standard Layer 2 NAT, due to the routing that occurs directly behind the NAT boundary.

The end user, OEM, or system integrator should consider asking whether Connected Routing with Layer 2 NAT is the right technology for the IACS application. Connected Routing, in conjunction with Layer 2 NAT, brings the following advantages:

- Helps to limit Layer 2 broadcast domain by segmenting VLANs in the Cell/Area Zone.
- Keeps all control traffic local by routing locally between the VLANs within the IACS application such as skid/machine or Cell/Area Zone. The control traffic does not have to traverse through the distribution switch which helps to optimize the traffic flow.
- Enables reuse of IP addressing without introducing duplicate IP address error.
- Helps to reduce commissioning cost by enabling replication of skids and machines due to Layer 2 NAT within the IES.
- Enables plant-wide connections (such as engineering workstation and FactoryTalk Application Servers) to I/O in the Cell/Area Zone, which helps to minimize operational cost due to improved troubleshooting as well as direct analysis and monitoring.
- Reduces hardware cost by not requiring an additional controller NIC.

Connected Routing, in combination with Layer 2 NAT, has advantages, but it can also add complexity to the plant-wide network design if it is not implemented correctly or without real need. Some of the examples where Connected Routing with Layer 2 NAT that may NOT be a good solution are:

- In networks where routing functionality in access switches should not be enabled due to increased complexity in configuring, managing and troubleshooting
- In networks where resilient topologies, such as redundant star or ring topology, are needed
- Multiple skid or machine networks with significant variations in layout, design and control programs
- Multiple skids or machines with large number of translated addresses and large amount of interlocking traffic between areas
- If NAT is used as a segmentation method in a large network without implementing VLANs and Layer 3 hierarchical network design

It is important to consider the cost and difficulties of creating and managing Connected Routing with Layer 2 NAT configuration. For example, a Connected Routing with NAT switch may be part of the OEM machine, but it is typically an end user who is responsible for managing IP address translations across the plant.

Connected Routing with Layer 2 NAT Use Cases

When Connected Routing with Layer 2 NAT design is the right solution for the application, this section describes two specific use cases that were tested:

- Single Private Network VLAN per machine
- Two Private Network VLANs per machine

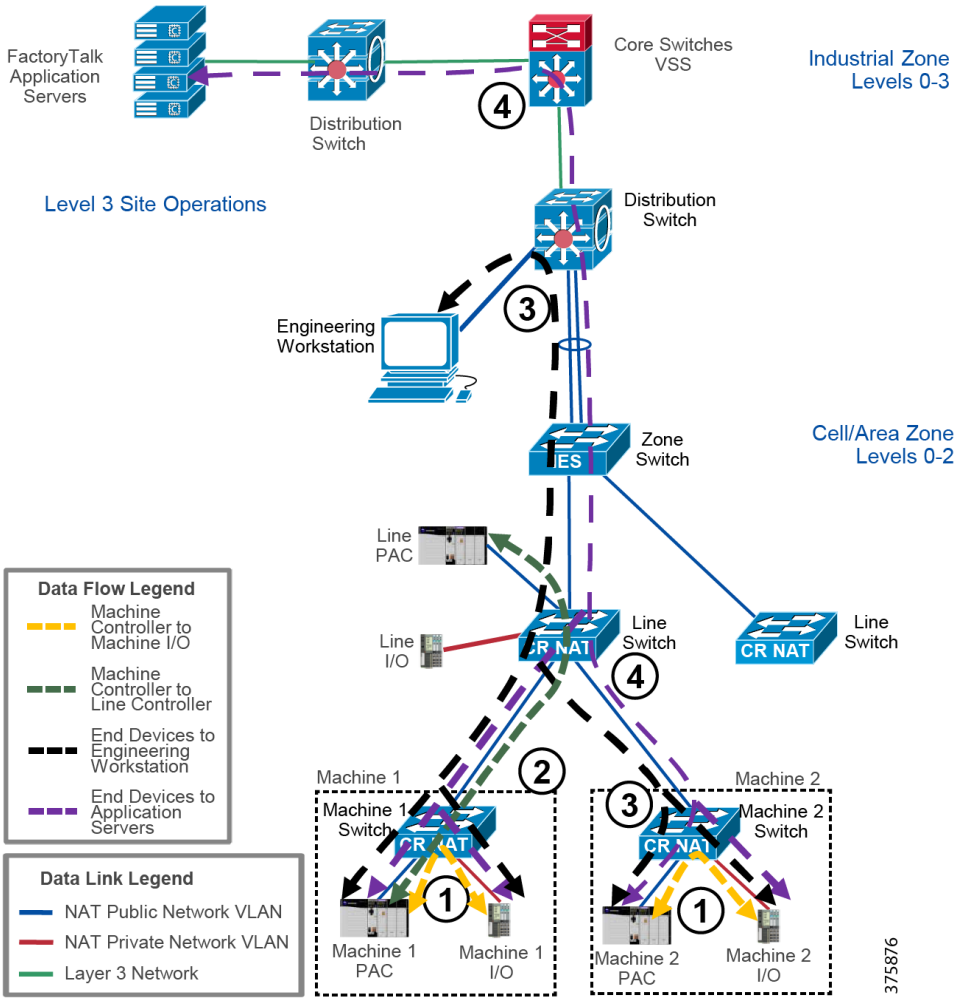
Single Private Network VLAN per Machine

This use case is based on Connected Routing with Layer 2 NAT design explained earlier. In this design, the controller and the I/O are placed in separate VLANs. Connected Routing is enabled on the IES to route between the two subnets. By keeping the two device types in separate VLANs, no changes are needed for controller communication, and the I/O device addition to the network has minimal or no impact. Layer 2 NAT is enabled for reuse of the I/O subnet IP addressing without introducing a duplicate IP address error in the IACS application architecture. Connected Routing when used in conjunction with Layer 2 NAT allows controllers and I/O reachability from devices (for example, engineering workstation or FactoryTalk Application Servers) in the plant-wide network, while keeping the controller to I/O traffic local to the IES.

This use case also assumes a star topology with hierarchical layering of IES within the Cell/Area Zone, which is typical when migrating toward the CPwE architecture from legacy IACS networks. Each IES sits at the machine, line or zone level and provides connectivity for all the switches below it in the hierarchy. Controller and I/O devices can be located at multiple layers and still communicate directly as needed. The topology can be scaled for multiple machines and lines, as long as the total number of end devices within the Cell/Area Zone does not exceed 250 (as per CPwE best practices).

Figure 2-1 provides a detailed view of the data flows between end devices using this design.

Figure 2-1 Single Private Network VLAN per Machine Architecture and Data Flows



As shown in Figure 2-1, the I/O devices connected to each machine IES are confined to a VLAN separate from the rest of the Cell/Area Zone. This design may also include a line-level controller and associated I/O devices that supervise multiple machines. The same design principles may be applied to this setup.

With this design, typical data flows through the network are enabled as follows (indicated by number in the figure):

1. Machine controller-to-machine I/O communication:
   - Traffic originating from the machine controller and destined to the machine I/O is routed from the controller VLAN to the I/O VLAN in both directions using Connected Routing.
2. Machine controller-to-line controller communication:
   - Machine controllers communicate to the line controller via the public VLAN. No routing or Layer 2 NAT translation is performed since the two controllers are present on the same VLAN.
3. Controllers and I/O devices to/from the Engineering Workstation:
   - Machine controllers communicate to the engineering workstation via the common VLAN. No routing or Layer 2 NAT translation is performed since the two controllers are present on the same VLAN.
   - For traffic from the engineering workstation destined for the I/O devices, the I/O devices are located on a separate private network VLAN so the IES must route the traffic across VLANs and perform NAT translations. First, the engineering workstation sends its data packet into the Cell/Area Zone with a destination address of the I/O device's public IP address. Second, as the packet arrives at the local IES, the destination address is translated to the private IP address of the I/O device. Third, the IES sees that the packet is destined for the private network VLAN subnet so it routes the packet into the private network VLAN. The packet can then be received by the appropriate I/O device on that VLAN.
   - For traffic from the I/O devices destined for the engineering workstation, the I/O devices are located on a separate private network VLAN and using an IP subnet that is duplicated across the machines. Therefore, the IES must route the traffic between VLANs and perform NAT translations for the I/O data. First, the I/O device sends its data packet to the IES with a destination IP address of the engineering workstation. This engineering workstation has a public IP address so the IES routes the packet from the I/O VLAN to the public VLAN. Second, the packet's source address is translated from its private subnet to a corresponding public address as it exits the IES uplink toward the distribution switch. Translation of the destination address is not necessary since it is already a public address on the plant-wide network. The packet can then be switched and/or routed through the network to the management system.
4. Controllers and I/O Devices to/from FactoryTalk Application Servers:
   - Machine and line controllers communicate to the application servers in the Site Operations area. The IES (the default gateway) performs the routing and forwards traffic to the distribution switch using the static route.
   - For traffic from the FactoryTalk Application Servers destined for the I/O devices: First, the server management system sends its data packet into the Cell/Area Zone with a destination address of the I/O device's public IP address. Second, as the packet arrives at the local IES, the destination address is translated to the private IP address of the I/O device. Third, the IES sees that the packet is destined for the private network VLAN subnet, so it routes the packet into the private network VLAN. The packet can then be received by the appropriate I/O device on that VLAN.
   - For traffic from the I/O devices destined for the FactoryTalk Application Servers: First, the I/O device sends its data packet to the IES with a destination IP address of the FactoryTalk Application Server. The IES routes the packet from the private I/O VLAN to the public VLAN and then forwards it towards the distribution switch using the static route. Second, the packet's source address is translated from its private subnet to a corresponding public subnet address as it exits the IES uplink

toward the distribution switch. Translation of the destination address is not necessary, since it is already a public address. The packet can then be switched and/or routed through the network to the server.

Two Private Network VLANs per Machine

This use case is based on the Connected Routing with Layer 2 NAT design explained earlier. This design allows for *drop in place* OEM equipment (including both controllers and I/O devices), with added functionality for the equipment vendor to segment their machine LAN into two VLANs.

In this design, the controller and I/O devices for a machine share the same private address space and are present in the same private network VLAN. This puts both the controllers and I/O for a machine in the same broadcast domain in the machine switch level, but allows connectivity to external IP devices in the plant-wide network and to other machine VLANs. This design can be used in scenarios where the OEM or end equipment user wants to keep both end devices for a machine in the same private IP address space, but needs connectivity to the devices above, while limiting the broadcast domain within the machine switch level.

Note The number of private network VLANs per machine could be more than two, depending on the application requirements. For this CVD, the two-VLAN case was selected and validated.

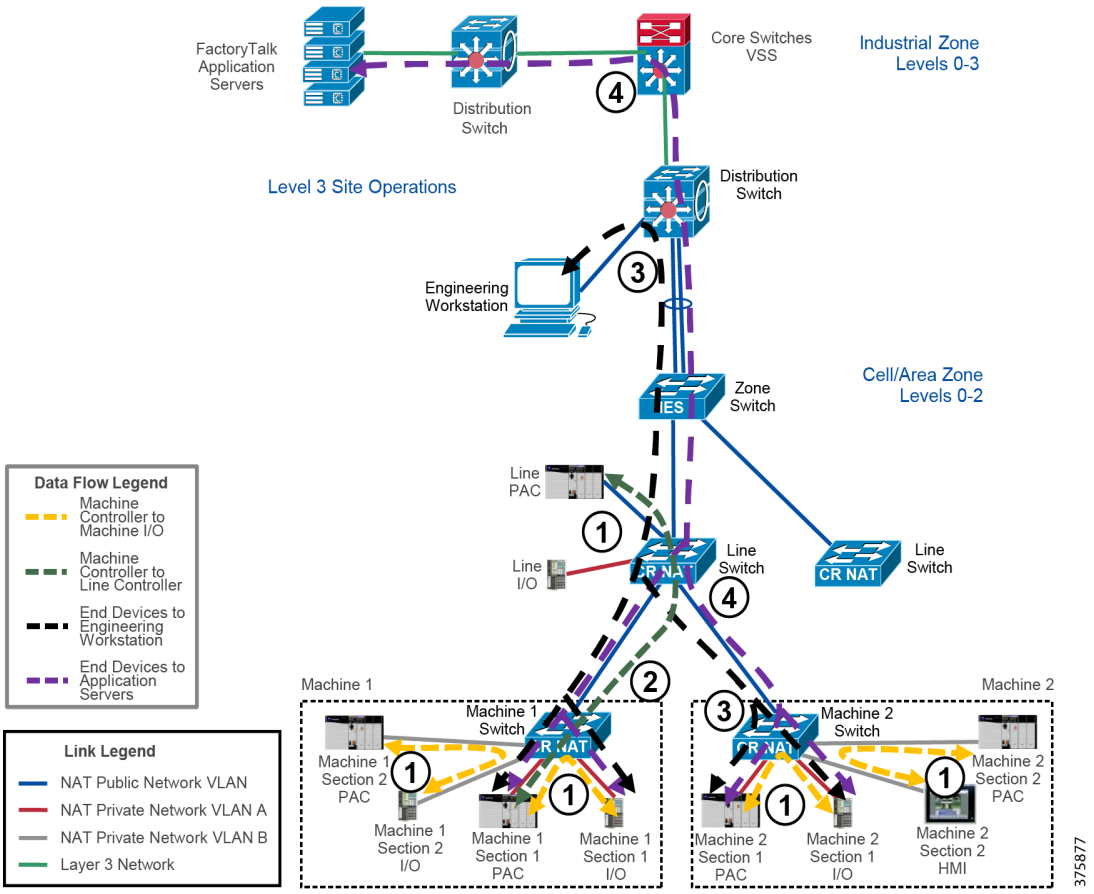
The local IES with Connected Routing provides connectivity between these VLANs, as well as to the other parts of the Cell/Area Zone. As with the other scenario, the devices also maintain reachability from either an engineering workstation located within the Cell/Area Zone or FactoryTalk applications hosted at Level 3 of the Industrial Zone. Here the controller and the I/O for a machine section will have the same default gateway configured to the IES since they are present in the same private network VLAN. Layer 2 NAT is enabled for reuse of IP addressing without introducing a duplicate IP address error in the IACS application architecture. Connected Routing, when used in conjunction with Layer 2 NAT, allows controllers and I/O reachability from devices (for example, engineering workstation or FactoryTalk Application servers) above in the network, while keeping the controller to end devices traffic local to the IES.

Note In this use case, the private IP address space cannot be reused across sections within the same machine and must be different.

As with the first use case, this use case also assumes a star topology with hierarchical layering of IES within the Cell/Area Zone, which is typical when migrating toward the CPwE architecture from legacy IACS networks. Each IES sits at the machine, line or zone level and provides connectivity for all the switches below it in the hierarchy. Controller and I/O devices can be located at multiple layers and still communicate directly as needed. The topology can be scaled for multiple machines and lines, as long as the total number of end devices within the Cell/Area Zone does not exceed 250 (as per CPwE best practices).

Figure 2-2 provides a detailed view of the data flows between end devices using this design.

Figure 2-2 Two Private Network VLANs per Machine Architecture and Data Flows



As shown in Figure 2-2, the controllers and I/O devices within Machine 1 are subdivided into sections that are each segmented in their own VLAN from the rest of the Cell/Area Zone. Layer 2 NAT must be enabled to allow use of repeated private subnets across machines, but not across sections within the same machine, as indicated by the public and private network VLAN designations.

Alternatively, traffic within a machine can be segmented based not just on location but also on the data type (for example, I/O versus HMI data). This can be useful in scenarios where existing HMI devices are already segmented on the machine, and legacy I/O is being migrated to EtherNet/IP. In this case, I/O devices could be on their own private network VLAN. This approach is illustrated in Figure 2-2 on Machine 2.

With this design, typical data flows through the network are enabled as follows (indicated by number in the figure):

1. Machine controller-to-machine I/O (or HMI) communication:
   - Traffic originating from the controller and destined for an I/O (or HMI) device within the same section is simply switched by the IES since both devices are present in the same VLAN.
   - For devices within different sections of the machine to communicate, the IES must route traffic from one section VLAN to the other.
2. Machine controller-to-line controller communication:
   - Since the machine and line controllers are located on separate VLANs, the IES must route the traffic between VLANs and perform Layer 2 NAT translations as the machine controller networks are using duplicate address space. First, the machine controller sends its data packet to the IES with a destination IP address of the line controller. This line controller has a public (plant-wide) IP address,

so the IES routes the packet from the machine section Controller and I/O VLAN to the public VLAN. Second, the packet's source address is translated from its private (machine-level) to a corresponding public address as it exits the IES uplink towards the line controller. Translation of the destination address is not necessary, since it is already a public address.

- For communication between controllers across two sections of the same machine, since each machine section is in separate VLAN, the traffic between them will be routed using connected routes. Here Layer 2 NAT translation is not needed as the traffic is local to the machine switch.

3. Controller, I/O, or HMI devices to/from Engineering Workstation:
   - For traffic from the engineering workstation destined for the controller, I/O, or HMI devices, the devices are located on a separate private network VLAN, so the IES must route the traffic across VLANs and perform NAT translations. First, the engineering workstation sends its data packet into the Cell/Area Zone with a destination address of the device's public IP address. Second, as the packet arrives at the local IES, the destination address is translated to the private IP address of the device. Third, the IES sees that the packet is destined for the private network VLAN subnet, so it routes the packet into the private network VLAN. The packet can then be received by the appropriate device on that VLAN.
   - For traffic from the controller, I/O, or HMI devices destined for the engineering workstation, since the controllers, I/O and engineering workstation are located on separate VLANs, the IES must route the traffic between VLANs and perform Layer 2 NAT translations as they are using duplicate address space. First, the device sends its data packet to the IES with a destination IP address of the engineering workstation. This workstation has a public (plant-wide) IP address, so the IES routes the packet from the device-level private network VLAN to the public VLAN. Second, the packet's source address is translated from its private to a corresponding public address as it exits the IES uplink. Translation of the destination address is not necessary, since it is already a public address. The packet can then be switched through the network to the engineering workstation.
4. Controller, I/O, or HMI Devices to/from FactoryTalk Application Servers:
   - Devices at the machine and line levels communicate to the application servers in the Site Operations area. The IES (the default gateway) performs the routing and forwards traffic to the distribution switch using the static route.
   - For traffic from the FactoryTalk Application Servers destined for the controller, I/O, or HMI devices: First, the server management system sends its data packet into the Cell/Area Zone with a destination address of the device's public IP address. Second, as the packet arrives at the local IES, the destination address is translated to the private IP address of the device. Third, the IES sees that the packet is destined for the private network VLAN subnet, so it routes the packet into the private network VLAN. The packet can then be received by the appropriate device on that VLAN.
   - For traffic from the controller, I/O, or HMI devices destined for the FactoryTalk Application Servers: First, the device sends its data packet to the IES with a destination IP address of the FactoryTalk Application Server. The IES routes the packet from the private I/O VLAN to the public VLAN and then forwards it towards the distribution switch using the static route. Second, the packet's source address is translated from its private subnet to a corresponding public subnet address as it exits the IES uplink toward the distribution switch. Translation of the destination address is not necessary, since it is already a public address. The packet can then be switched and/or routed through the network to the server.

CHAPTER 3

Configuring the Infrastructure

This chapter, which provides an overview of key concepts and general configuration information as they pertain to the IE 2000/Stratix 5700 in the Connected Routing and Layer 2 NAT architecture, includes the following major topics:

Configuring IP Routing

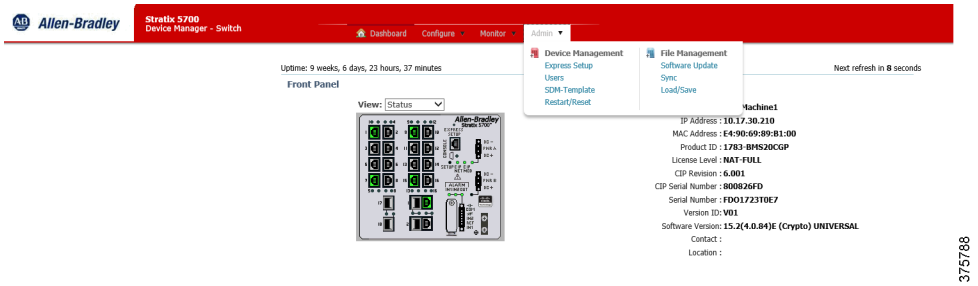
This section describes configuration for SDM templates, routing, and VLAN interfaces.

Switch Database Management Template Configuration

To enable IP routing, the Connected Routing-capable switch must be running the Lanbase Routing Switch Database Management (SDM) template rather than the Default. Complete the following steps to enable this template:

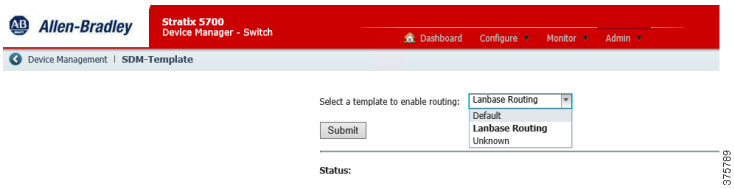
Step 1 In Device Manager, navigate to **Admin > SDM-Template** (see Figure 3-1).

Figure 3-1 Device Management—SDM Template



Step 2 In the **Select a template to enable routing** drop-down menu, select **Lanbase Routing** (see Figure 3-2).

Figure 3-2 SDM Template Selection



Step 3 Click **Submit** and then **OK** to reboot.

Note The SDM template will not be applied until the switch has been rebooted.

The equivalent CLI configuration for Steps 1-3 is shown below:

```
sdm prefer lanbase-routing
exit
copy running-config startup-config
reload
```

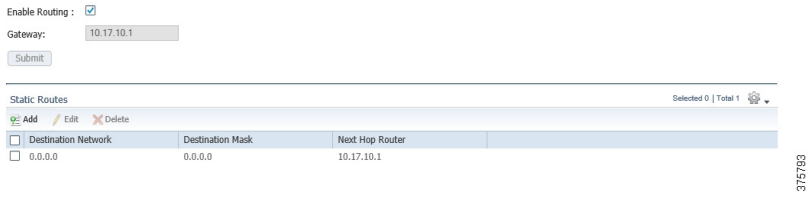
Routing Configuration

Once the proper SDM template is loaded on the switch, complete the following steps to enable IP routing:

Step 1 In Device Manager, navigate to **Configure > Routing**.

Step 2 Check the **Enable Routing** check box and enter the gateway IP address (typically the Layer 3 distribution switch for the Cell/Area Zone) in the **Gateway** field (see Figure 3-3).

Figure 3-3 Routing Configuration



Step 3 Click **Submit**. A static route, directing all traffic destined for remote networks to the gateway address, will be configured on the switch (but will not appear in the lower part of the window).

The equivalent CLI configuration for Steps 1-3 is shown below:

```
ip routing
ip route 0.0.0.0 0.0.0.0 10.17.30.1
```

VLAN Interface Configuration

The switch must have SVIs configured for both the public (outside) and private (inside) VLANs that are used in the Cell/Area Zone network. This will allow the switch to route traffic between the VLANs. Complete the following steps to create these interfaces:

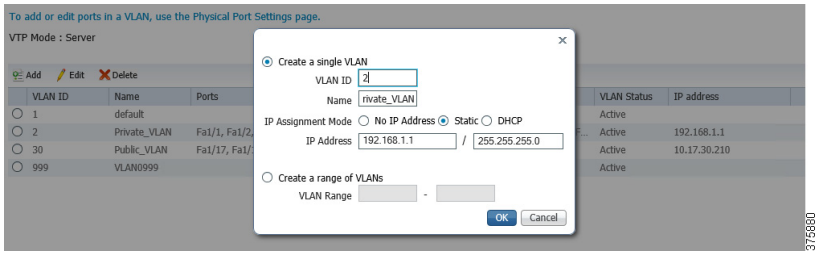
Step 1 In Device Manager, navigate to **Configure > VLAN Management**.

Step 2 Click **Add to add a VLAN** (see Figure 3-4).

Figure 3-4 VLAN Addition

Step 3 Enter the VLAN ID in the **VLAN ID** field and (optionally) a name in the **Name** field. For IP Assignment Mode, select the **Static** option and then enter an IP address and subnet mask in the respective fields (see Figure 3-5).

Figure 3-5 VLAN Interface Configuration



Step 4 Click **OK**.

Step 5 Repeat Steps 1-4 for any additional VLANs that are needed.

The equivalent CLI configuration for Steps 1-5 is shown below (VLAN 2 represents the private network VLAN, VLAN 30 represents the public Cell/Area Zone VLAN):

```
vlan 2
 name Private_VLAN
vlan 30
 name Public_VLAN
interface Vlan2
 ip address 192.168.1.1 255.255.255.0
interface Vlan30
 ip address 10.17.30.210 255.255.255.0
```

Note Any IACS equipment that needs a translation must be configured with a default gateway address. This will be the IP address of the local IES's SVI.

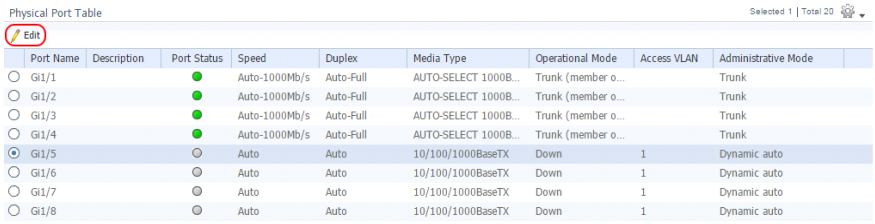
Applying VLAN to Interfaces

Once the VLANs and SVIs have been created, the VLANs must be associated with the appropriate interfaces (for example, **Private_VLAN** for the I/O interface and **Public_VLAN** for the uplink interface). Complete the following steps to create these associations:

Step 1 In Device Manager, navigate to **Configure > Port Settings**.

Step 2 Click the radio button next to the port that needs to be configured and then click **Edit** (see figure below).

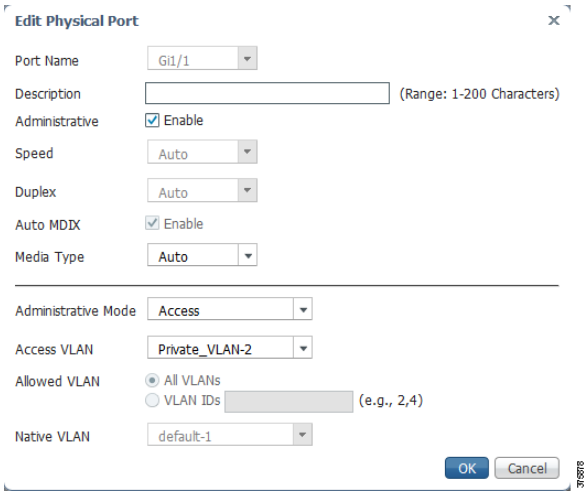
Figure 3-6 Device Manager Port Table



Step 3 In the **Administrative** mode drop-down menu, choose the **Access** option.

Step 4 Choose the desired VLAN to be applied to the port from the **Access VLAN** drop-down menu.

Figure 3-7 Device Manager Port Settings



Step 5 Click **OK** to save.

The equivalent CLI configuration for Steps 1-5 is shown below (VLAN 2 represents the private network VLAN, VLAN 30 represents the public Cell/Area Zone VLAN):

```
interface FastEthernet1/1
 description I/O Interface
 switchport mode access
 switchport access vlan 2
interface GigabitEthernet1/1
 description Uplink Interface
 switchport mode access
 switchport access vlan 30
```

Configuring Layer 2 NAT

The configurations shown in this section are specific to the Migrating Legacy IACS Networks to a Converged Plantwide Ethernet design and have significant differences from normal Layer 2 NAT configurations. For examples of standard Layer 2 NAT configurations, please refer to the *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture CVD* at the following URLs:

- Rockwell Automation site:
  - http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
- Cisco site:
  - http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

NAT Instance Configuration

Layer 2 NAT can be configured in two ways: host-based and network-based translation. This section describes how to configure the Layer 2 NAT instance on the switch based on these two translation methods.

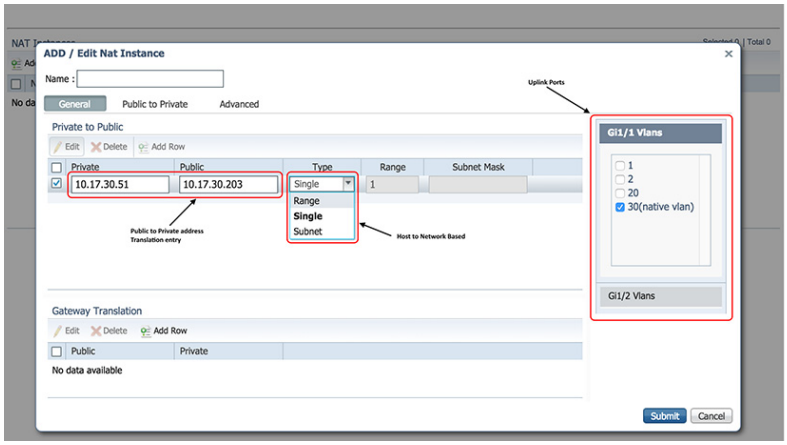
Host-based Translation

To configure the Layer 2 NAT instance with host-based translations, complete the following steps:

Step 1 In Device Manager, navigate to **Configure > NAT**.

Step 2 Enter a name for the instance in the **Name** field (see Figure 3-8).

Figure 3-8 NAT Instance Configuration



Step 3 In the Private to Public table under the General tab, click **Add Row** and enter the private IP address of the machine device, along with the public address that it should be translated to, in the respective fields. Under the **Type** drop-down menu, choose **Single** for host-based. Repeat this process for any other machine devices that require translation.

Note If **Range** is selected for Type instead of Single, a range of consecutive host addresses may be defined for translation.

Step 4 On the right side of the window, select the public (native) VLAN under the uplink port where the NAT instance should be applied.

Step 5 Select the following settings under the **Advanced** tab: Multicast/IGMP set to **pass-through** and fix-ups for ARP and ICMP enabled.

Step 6 Click **Submit**.

The equivalent CLI configuration for Steps 1-6 is shown below:

```
l2nat instance CR
 permit all
 fixup arp
 fixup icmp
 inside from host 192.168.1.51 to 10.17.30.203
!
interface GigabitEthernet1/1
 l2nat CR <Public VLAN ID>
```

Note By setting IGMP and multicast to pass-through mode, both IGMP/multicast and other unmatched traffic will be permitted through the NAT boundary (as shown by *permit all* in the CLI). If any IGMP or multicast setting is set to blocking instead, then unmatched traffic will also be blocked.

Note Although it is permitted by the above configuration, multicast I/O traffic was not tested as a part of this solution, so it is not recommended to send multicast traffic through the NAT boundary.

Access List Configuration

Access lists filter network traffic by controlling whether packets are forwarded or blocked at the interfaces. A switch determines whether to forward or drop the packet on the basis of the criteria specified within the access lists. With Layer 2 NAT configured, it is possible that traffic sourced from the private IP address range could leak onto the public VLAN. To protect against this possibility, we recommend blocking the private IP address range on the *line switch* port connected to the machine switch to prevent the traffic not using NAT from reaching any other connected switches.

The CLI configuration (to be applied on the line switch on each port facing a machine switch) is shown below:

```
  ip access-list standard <name of the access list>
   deny 192.168.1.0 0.0.0.255
   permit ip any
!
interface GigabitEthernet 1/1
 ip access-group <name of the access list> in
```

CHAPTER 4

Troubleshooting Tips

This chapter, which describes how to assess and verify the status of the Connected Routing and Layer 2 NAT, includes the following major topics.

Troubleshooting IP Routing

The first step in diagnosing IP routing is to check reachability between the host and its destination by using the ping command. If the ping fails, check the routing table on the switch using the *show ip route* command to validate that the destination network (or a default route of 0.0.0.0) is present:

```
IES#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is 10.17.30.2 to network 0.0.0.0

S*    0.0.0.0/0 [1/0] via 10.17.30.2
      10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        10.17.30.0/24 is directly connected, Vlan30
L        10.17.30.220/32 is directly connected, Vlan30
      120.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C        120.137.129.0/24 is directly connected, Vlan3
L        120.137.129.1/32 is directly connected, Vlan3
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Vlan2
L        192.168.1.1/32 is directly connected, Vlan2
```

Troubleshooting Layer 2 NAT

To investigate problems with L2NAT, first confirm the configuration by running the *show l2nat instance* command on the switch:

```
IES#show l2nat instance
l2nat instance NAT1
 permit : all
 fixup  : all
 inside  from host    192.168.1.51 to 10.17.30.213
 inside  from host    192.168.1.50 to 10.17.30.212
```

The permit option must be set to *all* to allow traffic that does not match an entry in the NAT translation table from being dropped. If this type of traffic is being dropped at the switch, check this configuration setting.

Note The permit option is set to drop all unmatched traffic by default.

The fix up option must also be set to *all*, implying that ARP and ICMP packets will have all relevant fields in the packet translated as they pass through the NAT boundary. Without this setting, ARP requests and ICMP ping requests will not be able to properly traverse the NAT switch, so hosts on each side may have trouble communicating as a result.

Note The fix up option is set to fix up ARP and ICMP packets by default.

The remaining lines of output show the translation entries present in the table. If packets are not being translated properly, check this list to ensure that there are no errors.

For a more detailed view of how many packets have been translated and which addresses are being rewritten, run the *show l2nat statistics* command:

```
IES#show l2nat statistics

STATS FOR INSTANCE: NAT1 (IN PACKETS)

TRANSLATED STATS (IN PACKETS)
================================================================================
INTERFACE DIRECTION VLAN  BYPASSED    DISCARDED   TRANSLATED  TOTAL PACKETS
Gi1/1     EGRESS    0     0           0           1712898     1712898
Gi1/1     INGRESS   0     1532        0           1684837     1686369
--------------------------------------------------------------------------------

PROTOCOL FIXUP STATS (IN PACKETS)
================================================================================
INTERFACE DIRECTION VLAN  ARP         ICMP
Gi1/1     EGRESS    0     0           0
Gi1/1     INGRESS   0     0           0
--------------------------------------------------------------------------------

IGMP AND MULTICAST STATS (IN PACKETS)
================================================================================
INTERFACE DIRECTION VLAN  IGMP        MULTICAST   UNICAST
Gi1/1     EGRESS    0     0           0           1712898
Gi1/1     INGRESS   0     0           0           1686355
--------------------------------------------------------------------------------

PER TRANSLATION STATS (IN PACKETS)
================================================================================
TYPE    DIRECTION SA/DA ORIGINAL IP     TRANSLATED IP   COUNT     ACTIVE(90Sec)
```

```
INSIDE  EGRESS    SA    192.168.1.50    10.17.30.222    1544689    168192
INSIDE  INGRESS   DA    10.17.30.222    192.168.1.50    1513907    164852
INSIDE  EGRESS    SA    192.168.1.51    10.17.30.223    4403       480
INSIDE  INGRESS   DA    10.17.30.223    192.168.1.51    5137       560
--------------------------------------------------------------------------------
================================================================================

NUMBER OF ACTIVE TRANSLATIONS IN THE PAST 90 SECONDS OF CORE[0]: 4
TOTAL TRANSLATIONS ATTACHED TO CORE [0]: 4
TOTAL INSTANCES ATTACHED TO CORE    [0]: 1
================================================================================

GLOBAL NAT STATISTICS
================================================================================
Total Number of NAT Packets               = 3399267
Total Number of TRANSLATED NAT  Packets   = 3397735
Total Number of BYPASSED   NAT  Packets   = 1532
Total Number of DISCARDED  NAT  Packets   = 0
Total Number of ARP      FIX UP Packets   = 0
Total Number of ICMP     FIX UP Packets   = 0
Total Number of IPV4 MULTICAST  Packets   = 0
Total Number of IGMP            Packets   = 0
Total Number of IPV4 UNICAST    Packets   = 3399253
================================================================================
================================================================================
```

The statistics shown in this output are as follows:

- **Translated Stats**—Shows how many packets have had translation operations performed while arriving at (ingress) or departing (egress) the NAT-enabled interface on the switch, and whether they were translated, discarded, or bypassed (meaning no translation was performed)
- **Protocol Fixup Stats**—Shows how many ARP and ICMP packets have been fixed up by NAT
- **IGMP and Multicast Stats**—Shows how many packets have been translated based on whether they are multicast or unicast, as well as IGMP packets
- **Per Translation Stats**—Shows how many packets have been translated for each entry in the NAT table, as well as the exact translation that occurs for the source/destination IP address of the packet depending on its direction
- **Global NAT Statistics**—Shows a summary of all of the above statistics, independent of which direction the traffic passed through the NAT-enabled interface

CHAPTER 5

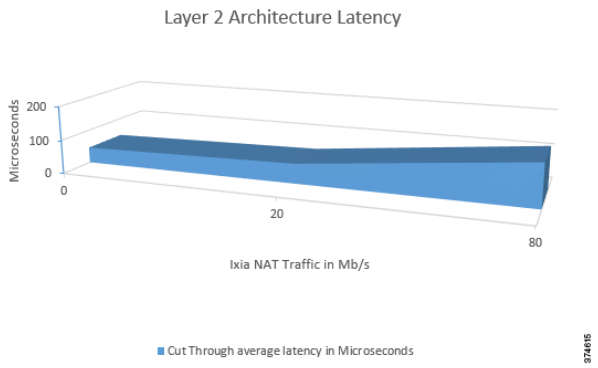
Migrating Legacy IACS Networks to a CPwE Architecture Test Results

This chapter, which describes test results for the Connected Routing with Layer 2 NAT use cases with the IE 2000/Stratix 5700, includes the following major topics:

In addition to functional validation of the configurations given in Configuring the Infrastructure, the architecture was scaled to validate performance under heavy traffic load conditions. The NAT table on the switch was configured to a total of 128 translation entries, which is the maximum supported. Ixia IxNetwork was used to generate traffic across the scaled switch at speeds varying from 20 to 80 Mbps over a six hour period, and average latency over that period as reported by Ixia was recorded.

To provide data points for comparison, Figure 5-1 shows the results obtained in previous testing with only Layer 2 NAT configured (see Chapter 4 of the *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture DIG*).

Figure 5-1 Average Latency for Layer 2 NAT Only Use Case



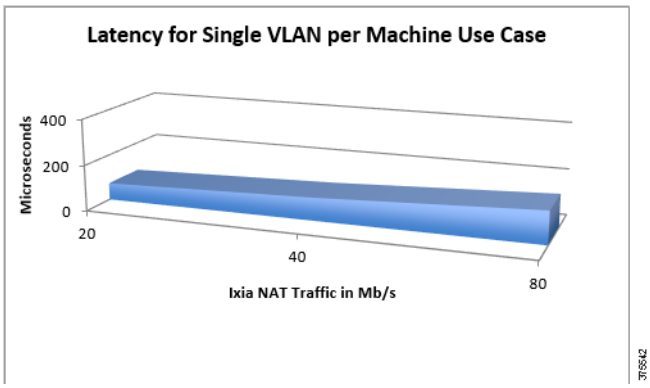
The average latency at 20 Mbps of traffic was about 50 microseconds; at 80 Mbps it reached 125 microseconds. These latency numbers take into account overall network latency through the architecture, which includes going through the IES. The results were consistent with the latency when NAT had not been enabled on the IES.

The following sections describe the results for each Connected Routing with the Layer 2 NAT use case.

Single Private Network VLAN per Machine

Figure 5-2 shows average latency times for varying NAT traffic loading in the single private network VLAN per machine use case.

Figure 5-2 Average Latency for Single Private Network VLAN per Machine Use Case

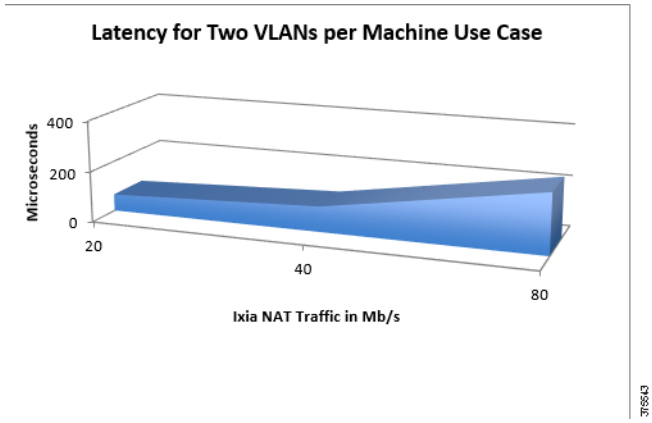


The average latency at 20 Mbps of traffic was about 70 microseconds; at 80 Mbps it reached 142 microseconds. These latency numbers take into account overall network latency through the architecture, which includes going through the IE 2000/Stratix 5700. The results were marginally larger than in previous testing, although still well within acceptable ranges for typical IACS traffic.

Two Private Network VLANs per Machine

Figure 5-3 shows average latency times for varying NAT traffic loading in the two private network VLAN per machine use case.

Figure 5-3 Latency for Two Private Network VLANs per Machine Use Case



The average latency at 20 Mbps of traffic was about 70 microseconds; at 80 Mbps it reached 237 microseconds. These latency numbers take into account overall network latency through the architecture, which includes going through the IE 2000/Stratix 5700. The results were marginally larger than in previous testing, although still well within acceptable ranges for typical IACS traffic.

APPENDIX A

CPwE References

This appendix lists the references that are pertinent to the *Migrating Legacy IACS Networks to a Converged Plantwide Network CVD*.

- *Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (CPwE)*
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td001_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/CPwE_DIG.html
- *Deploying the Resilient Ethernet Protocol (REP) in a Converged Plantwide Ethernet System (CPwE) Design Guide*
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td005_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/REP/CPwE_REP_DG.html
- *Deploying 802.11 Wireless LAN Technology within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td006_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/NovCVD/CPwE_WLAN_CVD.html
- *Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture Design and Implementation Guide*
  - Rockwell Automation site: http://literature.rockwellautomation.com/idc/groups/literature/documents/td/enet-td007_-en-p.pdf
  - Cisco site: http://www.cisco.com/c/en/us/td/docs/solutions/Verticals/CPwE/3-5-1/NAT/DIG/CPwE_NAT_CVD.html

APPENDIX B

Test Hardware and Software

Table B-1 lists the test hardware and software for the *Migrating Legacy IACS Networks to a Converged Plantwide Network CVD*.

Table B-1 Test Hardware and Software

Role	Product	SW Version	Notes
Distribution switch	Catalyst 3850	03.03.05.SE	--
Industrial Ethernet Switch – Layer 2 Access	IE 2000, Stratix 5700	15.2(4).EA	--
Rockwell Automation software	RSLinx® Classic	3.73.00	--
Rockwell Automation software	Studio 5000 Logix Designer®	26.01	--
Safety Programmable Automation Controller	1756 GuardLogix® Safety Controller	26.012	1756-L73S 1756-L7SP
EtherNet/IP Communication Module	ControlLogix® 2-port Ether-Net/IP module	5.028	1756-EN2T 1756-EN2TR
Programmable Automation Controller	1769 CompactLogix™ Controller	21.011	1769-L18ERM
EtherNet/IP Communication Module	2-Port EtherNet/IP I/O Adapter Module	3.011	1734-AENTR

APPENDIX C

Acronyms and Initialisms

Table C-1 lists acronyms and initialisms used in the *Migrating Legacy IACS Networks to a Converged Plantwide Network CVD*.

Table C-1 Acronyms and Initialisms

Term	Definition
CPwE	Converged Plantwide Ethernet
CVD	Cisco Validated Design
DIG	Design and Implementation Guide
EIGRP	Enhanced Interior Gateway Routing Protocol
HMI	Human Machine Interface
I/O	Input/Output
IACS	Industrial Automation and Control System
IES	Industrial Ethernet Switch
IoT	Internet of Things
IT	Information Technology
KPI	Key Performance Indicator
NAT	Network Address Translation
NIC	Network Interface Card
OSPF	Open Shortest Path First
OT	Operational Technology
PAC	Programmable Automation Controller
PAT	Port Address Translation
SDM	Switch Database Management
SVI	Switched Virtual Interface
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VFD	Variable Frequency Drive
VLAN	Virtual Local Area Network

Publication ENET-TD011A-EN-P January 2016