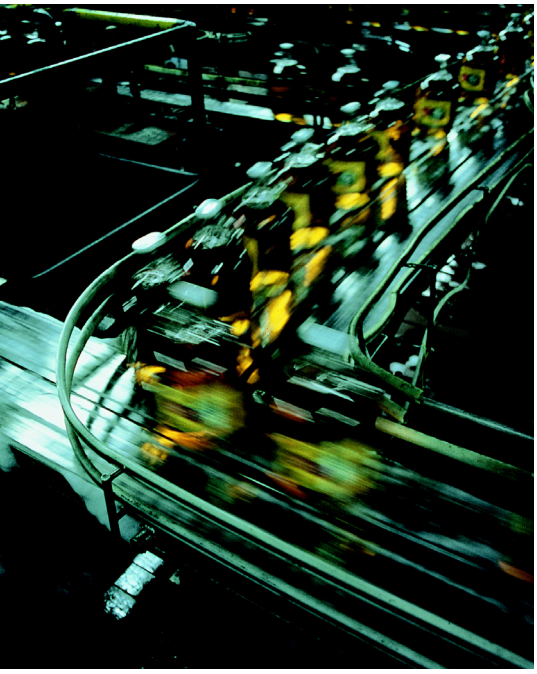


Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture

White Paper

May 2015

Rockwell Automation and Cisco Four Key Initiatives:

- Common Technology View:
  A single system architecture, using open, industry standard networking technologies, such as Ethernet and IP, is paramount for achieving the flexibility, visibility and efficiency required in a competitive manufacturing environment.
- Converged Plantwide Ethernet Architectures:
  These manufacturing focused reference architectures, comprised of the Rockwell Automation Integrated Architecture® and Cisco's Ethernet to the Factory, provide users with the foundation for success to deploy the latest technology by addressing topics relevant to both engineering and IT professionals.
- Joint Product and Solution Collaboration:
  Stratix 5700™ and Stratix 8000™ Industrial Ethernet switches incorporating the best of Cisco and the best of Rockwell Automation.
- People and Process Optimization:
  Education and services to facilitate Operational Technology (OT) and Information Technology (IT) convergence and allow successful architecture deployment and efficient operations allowing critical resources to focus on increasing innovation and productivity.

374629

Document Reference Number: ENET-WP036A-EN-P

Deploying Network Address Translation within a Converged Plantwide Ethernet Architecture

Whether you are an end user, OEM or system integrator, Internet Protocol (IP) addresses within your Industrial Automation and Control System (IACS) application may need to be reused. Network Address Translation (NAT) enables the reuse of IP addressing without introducing a duplicate IP address error into your IACS application architecture.

Technology and business aspects drive the decision to use NAT:

- From a business perspective, OEMs use NAT to enable the replication of skids and machines, including IP addressing. This helps to reduce development and commissioning costs.
- From a technology perspective, end users use NAT when the IP address space within the plant-wide network infrastructure is limited and not every device needs to communicate outside the skid or machine-level network.

Converged Plantwide Ethernet (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 provides design and implementation guidance to achieve the real-time communication, reliability, scalability and resiliency requirements of the IACS.

CPwE NAT for IACS applications is brought to market through a strategic alliance between Cisco Systems® and Rockwell Automation. The scalable CPwE NAT architecture details design and implementation considerations of NAT that meet the performance requirements of IACS applications.

Converged Plantwide Ethernet NAT

NAT 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. Plant-wide architectures require unique IP addressing. NAT can be configured to translate only specific IP addresses from inside the IACS application to the outside plant-wide architecture. Doing so provides the added benefit of effectively hiding the inside IP addressing schema of the IACS application.

NAT translations have two forms: one-to-one (1:1) and one-to-many (1: n). The CPwE NAT tested and validated use cases use one-to-one NAT, implemented in a Layer 2 access switch.

The CPwE NAT Cisco Validated Design (CVD) provides design and implementation guidance for a successful deployment of IACS NAT networking within plant-wide architectures. The CPwE NAT CVD includes a review of NAT technology that is based upon Layer 2 industrial Ethernet switches (IES): Allen-Bradley Stratix 5700 and Cisco IE 2000 Series switches. The CPwE NAT CVD presents steps and guidance for the implementation and configuration of NAT in conjunction with IACS applications. Guidance for maintaining and troubleshooting a CPwE NAT implementation are also provided.

Note The CPwE NAT architecture focuses on EtherNet/IP™, which is driven by the ODVA Common Industrial Protocol (CIP).

CPwE NAT IACS Use Cases

The CPwE NAT architecture is tailored to address a scalable application of NAT within the Cell/Area Zone of the CPwE architecture. Several NAT use cases have been individually tested and validated, allowing architectural selection that is practical to a small (machine/skid) or large-scale (Cell/Area Zone) plant-wide deployment.

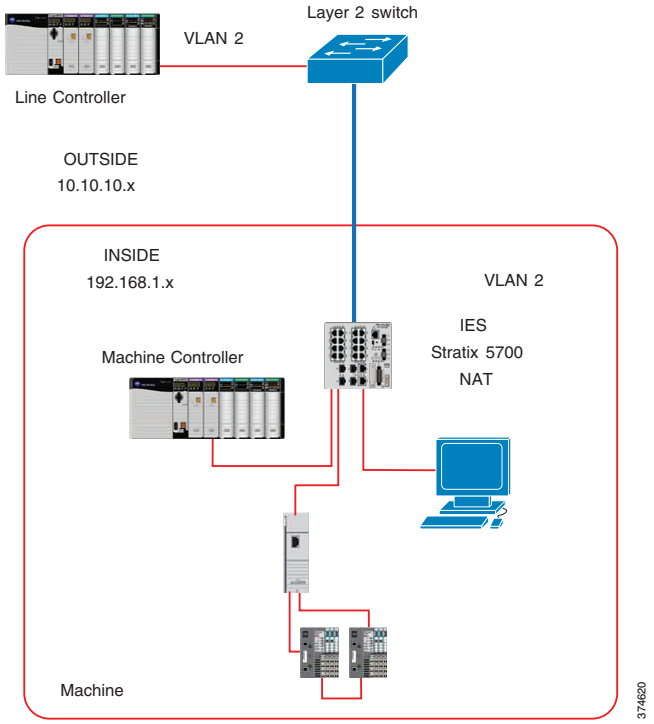
Single Skid/Machine Aggregated by One NAT Switch, Single VLAN

A common use case, as depicted in Figure 1, is the coordination of control functions of an OEM skid or machine by a line controller. In this use case, a single Layer 2 virtual LAN (VLAN 2) exists; however, the skid or machine IACS devices have a different IP address range (inside) than the line controller (outside). The machine IES translates the inside IP address (192.168.1.x) of the machine controller to an outside IP address (10.10.10.x) on VLAN 2.

This scalable use case enables the integration of multiple skids or machines with duplicated IP addressing into the same line controller VLAN. Each skid or machine IES would have to translate the duplicated inside IP addresses to unique outside IP addresses to avoid a duplicate IP error within the VLAN.

For this use case, a NAT-capable Layer 2 IES is required for each skid or machine. A Layer 3 switch is not required since a single VLAN is used.

Figure 1 Single Skid/Machine Aggregated by One NAT Switch, Single VLAN



Single Skid/Machine Aggregated by One NAT Switch, Multiple VLANs

A variation of the previous use case, as depicted in Figure 2, uses multiple VLANs—VLAN 10 for skid or machine 1, VLAN 20 for skid or machine 2 and VLAN 30 for the line controller. As in the previous use case, the IP addresses are duplicated for the IACS devices within each skid or machine.

The machine 1 IES translates the inside IP address (192.168.1.x) of the machine controller to an outside IP address (10.10.10.x) on VLAN 10. The IES switch also translates the outside IP address of the default gateway (Layer 3 switch) to an inside IP address.

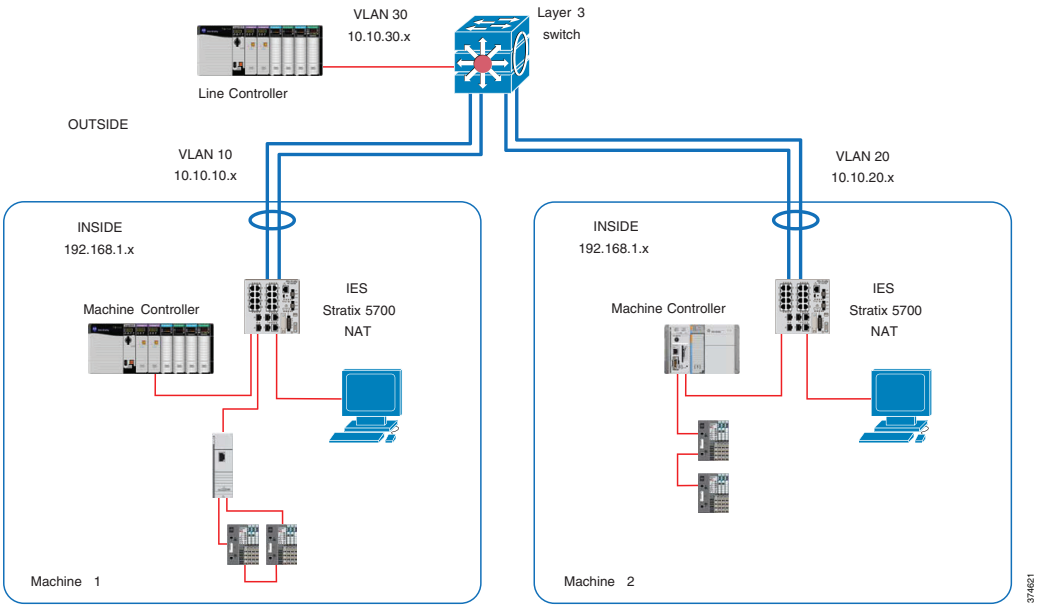
The machine 2 IES translates the inside IP address (192.168.1.x) of the machine controller to an outside IP address (10.10.20.x) on VLAN 20. Likewise, the machine 2 IES switch also translates the outside IP address of the default gateway to an inside IP address.

Each machine controller has a unique outside IP address and default gateway IP address on its own respective VLAN. The Layer 3 switch routes the outside IP address of each machine controller either to the line controller (vertical interlocking) on VLAN 30, or to the other machine VLAN (horizontal interlocking).

This scalable use case enables the integration of multiple skids or machines with duplicated IP addressing into the same line controller VLAN. Each skid or machine IES would have to translate the duplicated inside IP addresses to unique outside IP addresses to avoid a duplicate IP error within the VLAN.

For this use case, a NAT-capable Layer 2 IES is required for each skid or machine. A Layer 3 switch is required to enable routing between the VLANs.

Figure 2 Single Skid/Machine Aggregated by One NAT Switch, Multiple VLANs



Multiple Skids/Machines Aggregated by One NAT Switch, Multiple VLANs

A variation of the previous two use cases, as depicted in Figure 3, uses a single NAT-capable IES to translate IP addresses from multiple skids or machines. In this use case, the NAT IES supports multiple instances of NAT, on a per-VLAN basis. As in the previous use cases, the IP addresses are duplicated for the IACS devices within each skid or machine.

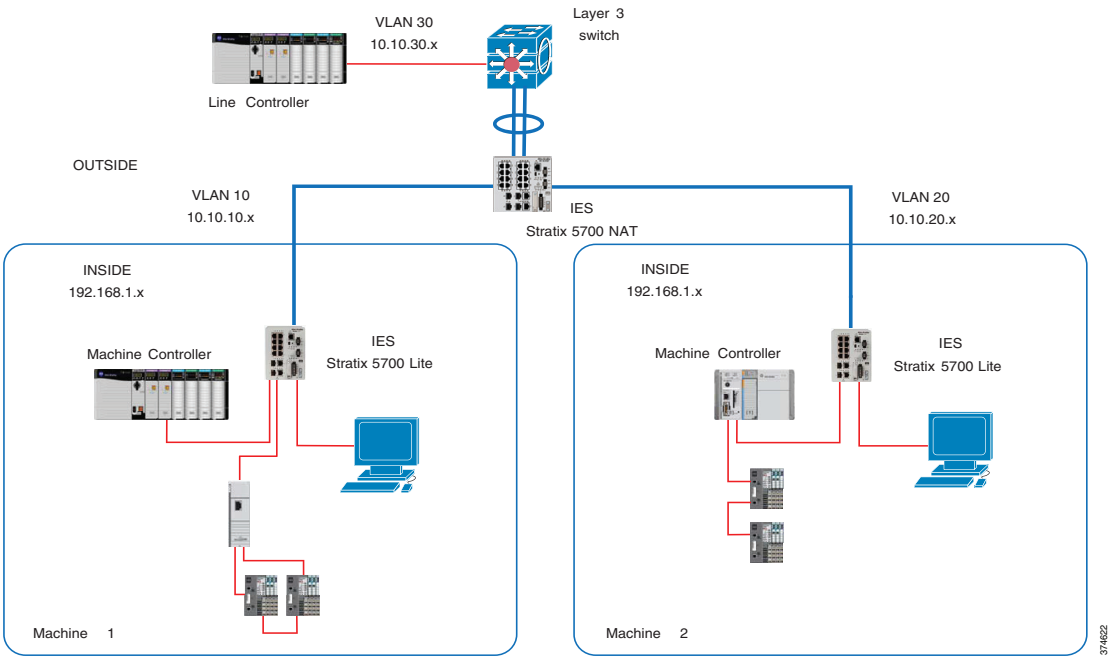
Each machine IES aggregates the IACS devices onto its VLAN. The single NAT IES translates the inside IP addresses (192.168.1.x) within each VLAN to its outside IP addresses—VLAN 10 (10.10.10.x) and VLAN 20 (10.10.20.x)—using a separate instance of the NAT table for each VLAN. Each machine controller has a unique outside IP address on its own respective VLAN. The single NAT IES also translates the IP addresses of the default gateway, which is a Layer 3 switch.

The Layer 3 switch routes the outside IP addresses of each machine controller either to the line controller (vertical interlocking) on VLAN 30, or to the other machine VLANs (horizontal interlocking).

This scalable use case enables the integration of multiple skids or machines with duplicated IP addressing into the same line controller VLAN. Each skid or machine has unique outside IP addresses within their respective VLANs to avoid a duplicate IP error.

For this use case, a single NAT-capable Layer 2 IES can be used to aggregate the two machines, while a non-NAT IES is used within each machine. A Layer 3 switch is required to enable routing between the VLANs.

Figure 3 Multiple Skids/Machines Aggregated by One NAT Switch, Multiple VLANs



Summary

Cisco Systems and Rockwell Automation have produced the CPwE NAT architecture that is based upon industry standards. Network Address Translation (NAT) allows for the reuse of IP addressing without introducing a duplicate IP address error into your IACS application architecture. The need for NAT is driven by both technology and business aspects. Design considerations allow end users to overcome common challenges where skid and machine builders use the same range of IP addresses for all machines produced. CPwE NAT aids both end users and OEMs in deploying a NAT-capable network through planning and design guidance, allowing for a network architecture optimized for IACS application needs.

Publication ENET-WP036A-EN-P - May 2015