Allen-Bradley Stratix 5700™ Network Address Translation (NAT)

Mark Devonshire – Product Manager, Rockwell Automation
Mark Hantel – Senior Engineer, Rockwell Automation

Synopsis

Machine integration onto a plant's network architecture can be difficult as OEM IP-address assignments rarely match those of the end-user network and network IP addresses are generally unknown until the machine is being installed – adding cost and time to the commissioning of the equipment, and delays moving that equipment into production.

The Allen-Bradley Stratix 5700 with Network Address Translation (NAT) is a hardware Layer 2 implementation that provides "wire speed" 1:1 translations ideal for automation applications where performance is critical.

NAT allows for:

- High performance and simplified integration of IP-address mapping from a set of local, machine-level IP addresses to the end user's broader plant network
- OEMs to deliver standard machines to end users without programming unique IP addresses
- End users to more simply integrate the machines into the larger network
- Easier machine maintenance because machine configuration remains standard

The Stratix 5700 switch with NAT technology also allows users to have the flexibility to segment or isolate network traffic by determining which devices are exposed to the larger network. By limiting access to certain devices, they can be isolated from unneeded network traffic, which can help optimize network performance at the local level.

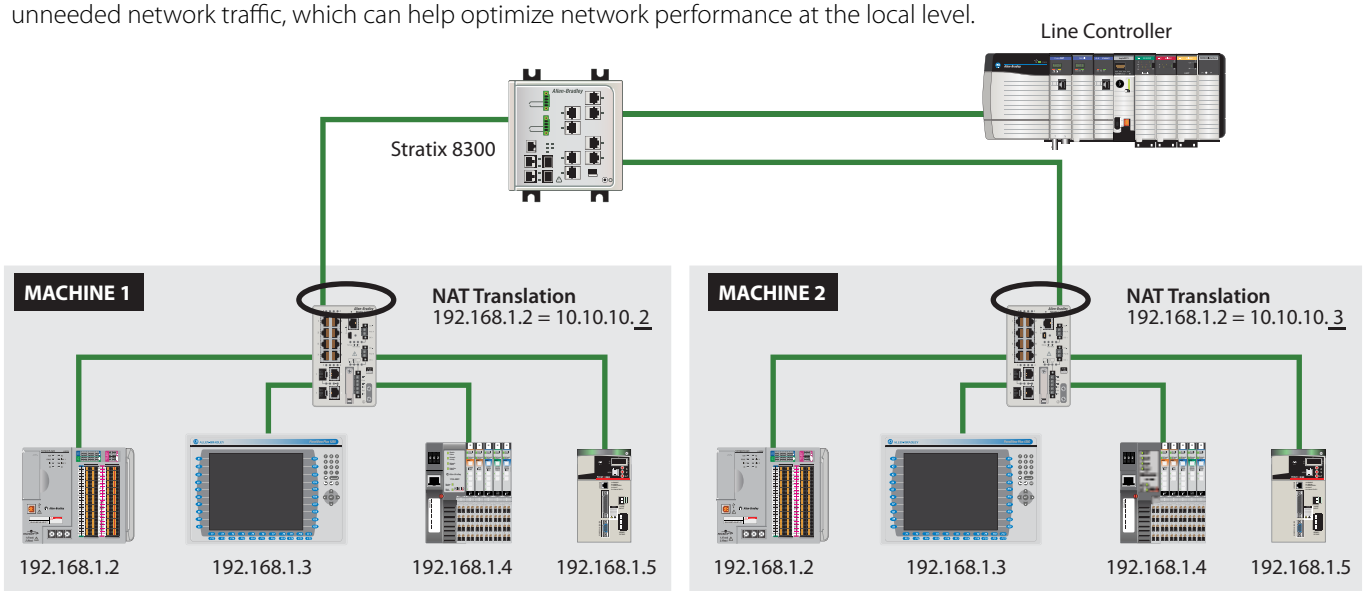

Figure 1 - Multiple Identical Machines On The Same Network

What Is NAT?

Network Address Translation is a service that can translate a packet from one IP address to another IP address. NAT can be found either on a Layer 2 device or on a Layer 3 device. NAT can be understood easiest with the introduction of the concept of a private network and a public network (Figure 2)*. These two networks are separated by a boundary; a device that implements NAT is this boundary. NAT can take on multiple forms including one-to-many NAT and one-to-one NAT (our implementation).

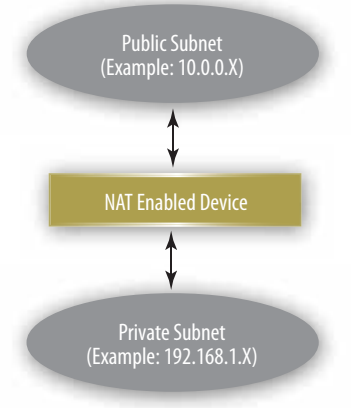

Figure 2 – Concept Of Public And Private Subnets With A NAT Device Separating

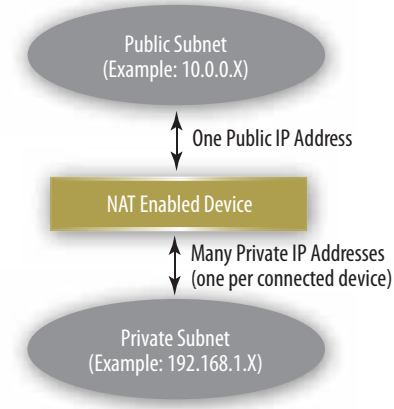

Figure 3 – One-To-Many NAT Example

One-to-many NAT is also known as Port Address Translation and allows one public IP address to be shared by many private IP addresses. This function is commonly found in consumer grade routers. A one-to-many NAT device contains a table that allows unique private host ports to be exposed on the single public IP address (Figure 3).

What is One-To-One NAT?

One-to-one (1:1) NAT is a service that allows the assignment of a unique public IP address to an existing private IP address (end device), allowing the end device to communicate on both subnets (Figure 4). This service is configured in a NAT enabled device and is the public "alias" of the IP address physically programmed on the end device. This is typically represented by a table in the NAT device.

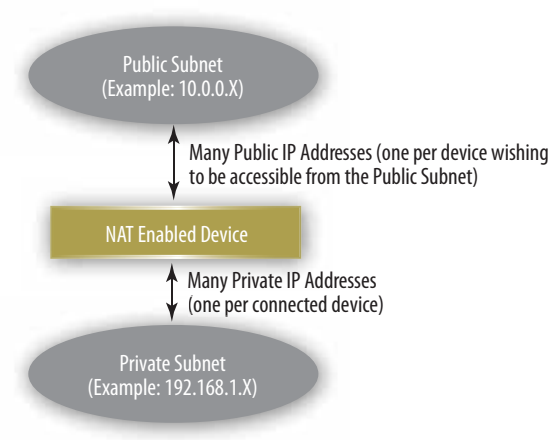

Figure 4 – 1:1 NAT Example

- *Note that we use the terms private and public to differentiate the two networks on either side of the NAT device. This does not infer that the public network must be Internet routable*

1:1 NAT allows a manufacturer to keep duplicate machines identical while providing a unique identity (alias) to the larger industrial network. The feature also gives a granular method of granting or restricting access to an end device (I/O blocks, drives, etc.) on the machine in one place.

1:1 NAT works by replacing the IP header on a packet and recalculating the packet checksums as it finds the appropriate match in the NAT table when it passes through the NAT device (Figure 5).

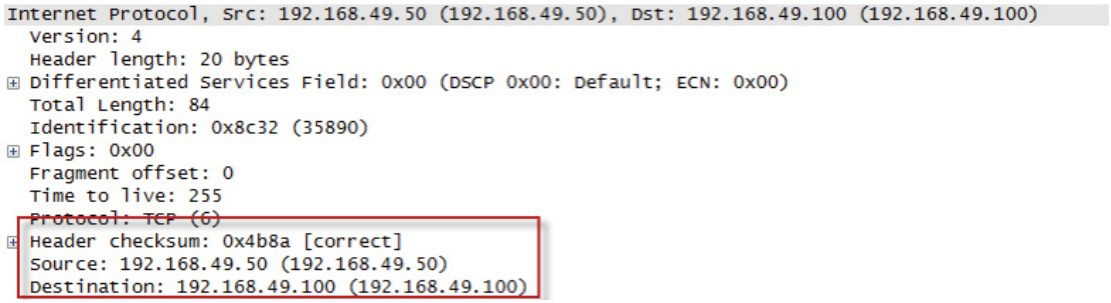

Figure 5 – NAT Specific Data in an Ethernet Packet

1:1 Layer 2 vs. Layer 3 NAT

Historically 1:1 NAT has been implemented in software on Layer 3, meaning the NAT enabled device acts as the default gateway (router) for all the devices on the private subnet. The NAT device will intercept traffic on behalf of its private subnet devices, perform the translation, and route traffic to the private subnet appropriately. As a software implementation, Layer 3 NAT translations typically are handled by the host CPU on the NAT device. Performance of a software NAT implementation is tied directly to the loading the host CPU can handle.

The Layer 2 1:1 NAT implementation differs in several areas. Rather than acting as the default gateway for the private subnet, Layer 2 NAT has two translation tables where private-to-public and public-to-private subnet translations can be defined. Layer 2 NAT is a hardware-based implementation that provides wire speed performance throughout switch loading. This implementation also supports multiple VLANs through the NAT boundary for enhanced network segmentation. Ring architecture support is built into Layer 2 NAT, allowing redundancy through the NAT boundary.

Stratix 5700 1:1 Layer 2 NAT Implementation

The Stratix 5700 integrates 1:1 NAT capability into the switch. This is a Layer 2 (MAC layer) implementation and is integrated with the hardware fabric of the switch (Figure 6). It allows for a scalable, high performance, single box solution.

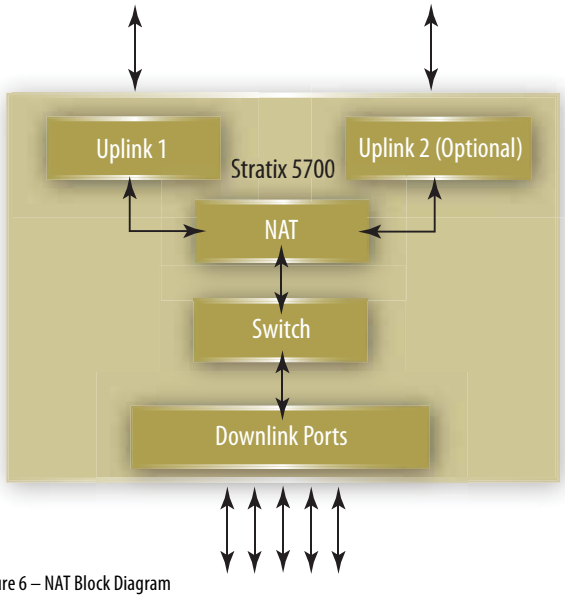

Figure 6 – NAT Block Diagram

The NAT feature is integrated in hardware between the uplink ports and the rest of the switch. It supports one or two uplinks which can be used in star, redundant star and ring topologies. One uplink would be used for a standard star topology. Two uplinks could be used for either a redundant star using spanning tree, or a ring topology using REP (Figure 7).

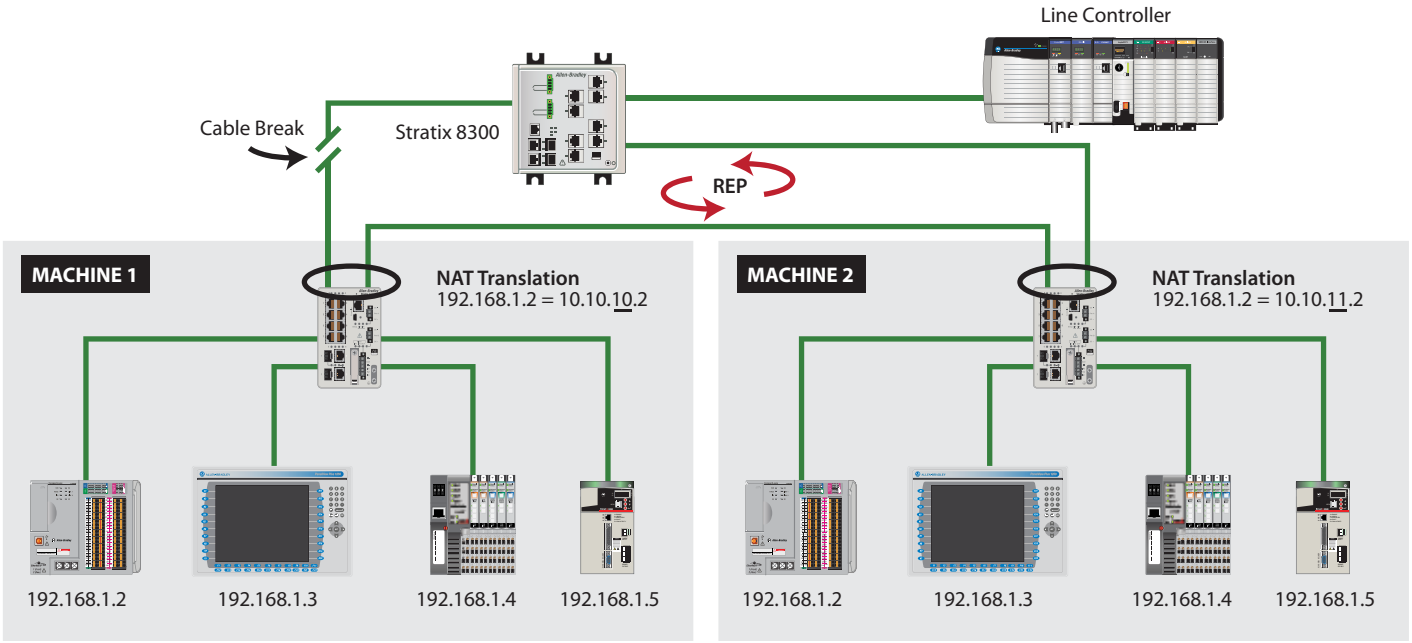

Figure 7 – REP Ring Topology

NAT Instances

The software interface for NAT has been implemented using the concept of instances (Figure 8). Each instance contains a name, "Private to Public" NAT table, "Public to Private" NAT table, VLAN and interface association, specific packet fix-ups, and specific types of traffic that can be blocked or passed through. Typically only one instance will be used; however, multiple instances can be supported to differentiate between different VLAN configurations. NAT can be attached to one or many VLANs, but will not translate traffic across VLANS (i.e. change a VLAN tag) or break other existing VLAN rules.

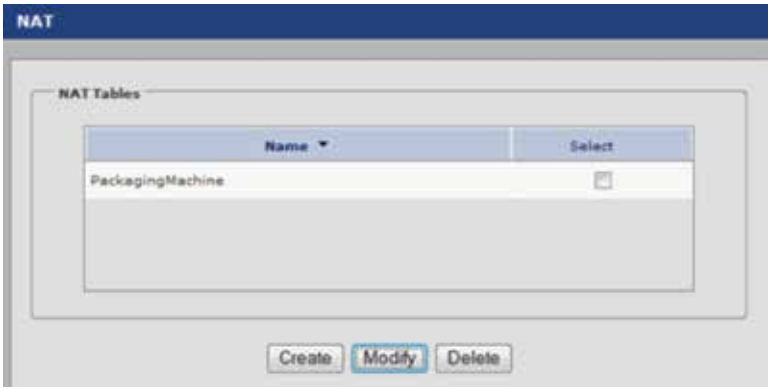

Figure 8 – NAT Instances

NAT Tables

An important concept of the Layer 2 NAT implementation is how NAT interacts with private and public subnets (Figure 9). Each NAT instance has two tables, a "Private to Public" table, and a "Public to Private" table. "Private" devices must be assigned a unique IP address in the "Private to Public" NAT table on the "public" subnet. Likewise "public" devices must be assigned unique IP addresses in the "Public to Private" NAT table on the "private" subnet. The implementer is responsible for defining these addresses. The addresses must be unique and unused on other attached devices and throughout the switch.

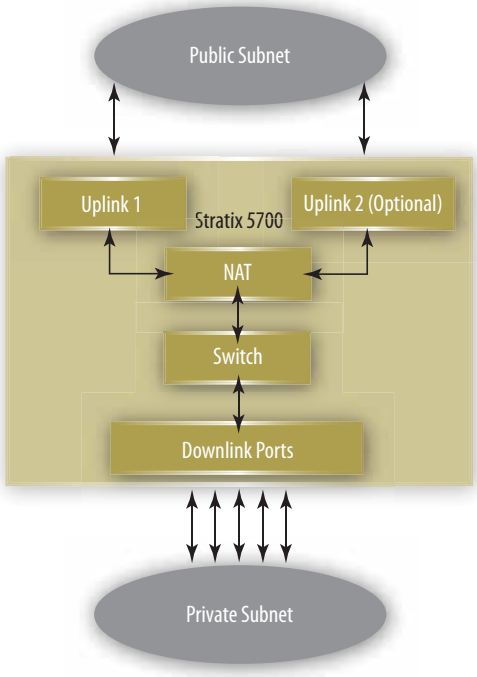

Figure 9 – Stratix 5700 NAT

Each private subnet device that is expected to talk on the public subnet must have a "Private to Public" translation. However, not all private subnet devices must have translations. They can be kept behind the NAT barrier to increase security, decrease traffic on the uplink port, and conserve public address space.

If the uplinks are connected to a Layer 3 switch or router, only one "Public to Private" translation must be used – the default gateway (Figure 10). If the uplinks are connected via a Layer 2 switch to other devices on the public subnet, each public subnet device must have a unique IP address in the "Public to Private" table.

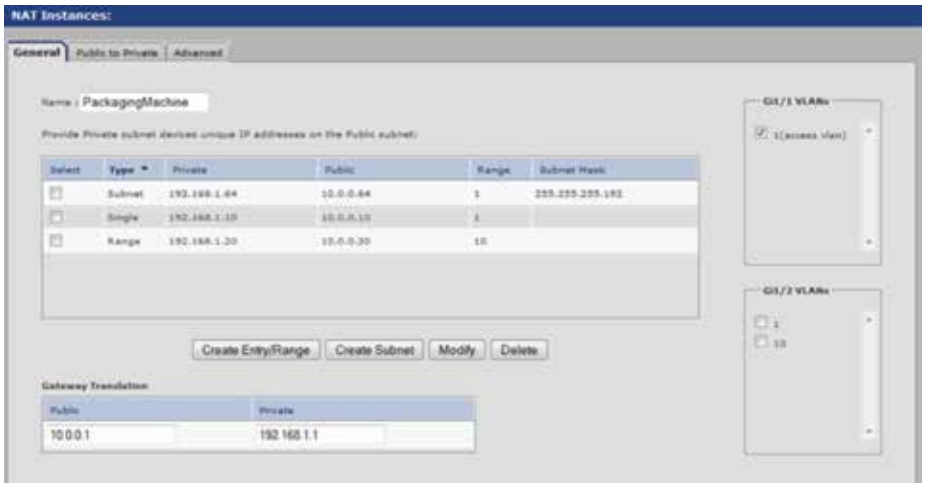

Figure 10 – NAT Private to Public Table (General Tab)

Types Of Translations

There are three types of translations that can be defined: single, range and subnet. A single translation will have one private address and one public address. A range will have a starting private address, a starting public address and a number of entries (Figure 11). A subnet translation allows the definition of a Class "B" subnet (mask: 255.255.0.0), Class "C" subnet (mask: 255.255.255.0) or a fraction of a Class "C" subnet (Figure 12). A maximum number of 128 NAT entries can be created per switch. These entries can be defined in one instance or up to 128 separate instances. These entries can be of any type and are defined by the rules below (Table 1). Subnet translations will have a starting private address and public address that must be aligned on proper subnet boundaries (Table 2).

Types of Translations	Number of Entries in NAT Table
Single	1
Range	Quantity of Range
Subnet	1

Table 1 – Number of NAT Table Entries Per Translation Type

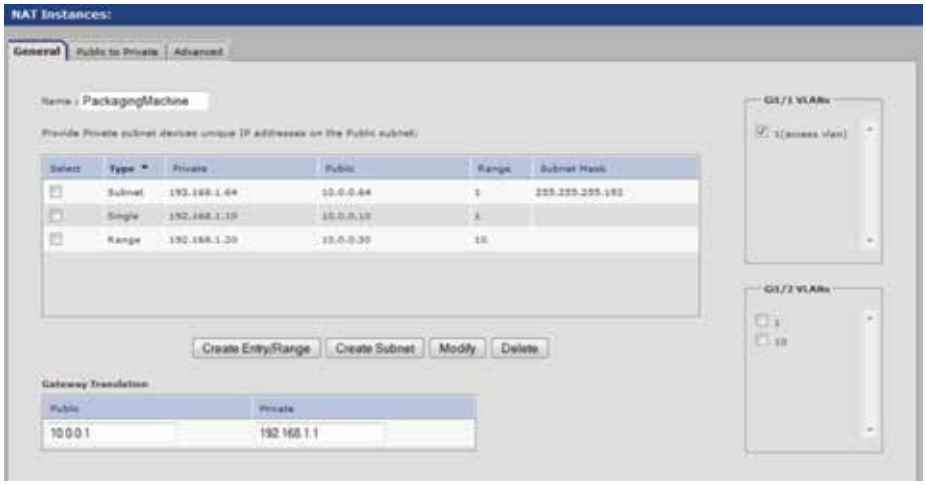

Figure 11 – Example of Translation Types

Figure 12 – Example of A Subnet Definition

Subnet Mask	Number of Translations
255.255.255.240	16
255.255.255.224	32
255.255.255.192	64
255.255.255.128	128
255.255.255.0	255
255.255.0.0	65535

Table 2 – Subnet Translation Detail

The use of a subnet translation will allow for many more than 128 IP addresses to be translated. For example the table shown in Figure 11 uses 12 NAT entries but provides 75 actual translations.

VLANs

When configuring NAT, you can assign one or more VLANs to a NAT instance (Figure 13). When you assign a VLAN to a NAT instance, the traffic associated with that VLAN is subject to the configuration parameters of the NAT instance. Configuration parameters include whether traffic is translated, fixed up, blocked or passed through.

Figure 13 – VLAN Selection

When assigning VLANs to a NAT instance, consider the following:

- NAT supports both trunk ports and access ports.
- NAT does not change VLAN tags – both your private and public subnets, while different, need to share the same VLAN to communicate.
- You can assign a maximum of 128 VLANs to one or more instances.
- You can assign the same VLAN to multiple instances as long as the VLAN is associated with different ports. For example, you can assign VLAN 1 to both instance A and instance B as long as VLAN 1 is associated with port Gi1/1 on instance A and port Gi1/2 on instance B.
- By default, each instance is assigned to all VLANs on port Gi1/1 and no instances on port Gi1/2. VLANs associated with a trunk port can or cannot be assigned to a NAT instance. It is recommended to only assign one VLAN per instance to simplify configuration.
- If a VLAN is assigned to a NAT instance, its traffic is subject to the configuration parameters of the NAT instance.
- If a VLAN is unassigned to a NAT instance, its traffic remains untranslated and is always permitted to pass through the trunk port.

Management Interface and VLANs

The management interface can be associated with a VLAN that is or is not assigned to a NAT instance:

- If its associated VLAN is assigned to a NAT instance, the management interface resides on the private subnet by default. To manage the switch from the private subnet, additional configuration is not required. To manage the switch from the public subnet, you must configure a private-to-public translation.
- If its associated VLAN is not assigned to a NAT instance, the management interface's traffic remains untranslated and is always permitted to pass through the port.

Traffic Permits and Fix-Ups

The Stratix 5700 NAT implementation allows certain types of traffic to either be blocked or passed through, these are called "traffic permits" (Figure 14). They can be assigned on a per-instance basis. Traffic on VLANs not attached to an instance will be unaffected by these rules. The types of traffic that can either be blocked or passed-through on an incoming or outgoing basis are: unicast, multicast and IGMP. Unicast traffic that is not translated can be passed through (with its original IP information) to the public or private network, or blocked. While multicast is not officially supported for NAT translation, we allow it to be passed through or blocked by the user when necessary. IGMP can also be passed through or blocked. Broadcast traffic will flow seamlessly through the NAT boundary if a public-to-private translation exists for the sending device.

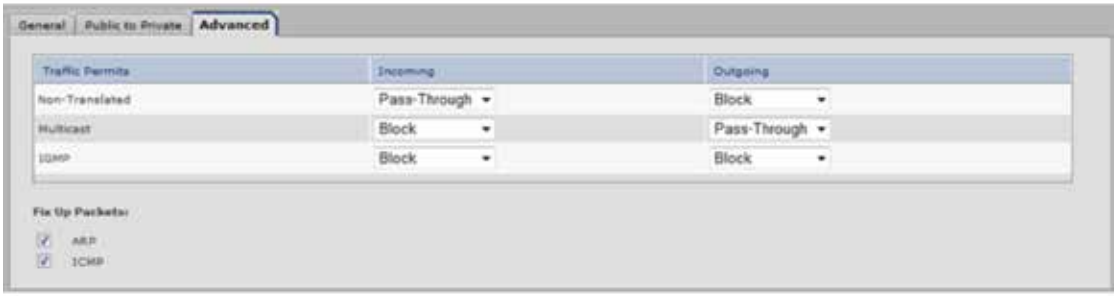

Figure 14 – Permit & Fix-Up User Interface Example

Certain types of traffic may have IP addresses embedded within the packet and may need to be "fixed-up" for them to work properly (Figure 14). Two types of traffic can be fixed-up – ARP and ICMP. Fix-ups can be assigned on a per-instance basis. These are typically enabled in all configurations.

Unsupported Traffic

The following is a list of traffic that is not supported across the NAT boundary due to its use of embedded IP addresses that are not fixed-up, encrypted IP addresses, or reliance on multicast traffic. This traffic is supported on either side of the NAT boundary. These limitations are typical for all NAT devices.

- Traffic encryption and integrity checking protocols generally incompatible with NAT (e.g. IPSec transport mode*)
- Applications that use dynamic session initiations, such as Netmeeting*
- FTP*
- Rockwell Automation 1791-ES safety module (IP address is in the safety signature and is not fixed-up) This is planned to be changed in V22.
- Microsoft DCOM (used in OPC communications)
- Multicast traffic and applications which use multicast including CIP Sync™ (IEEE-1588) and ControlLogix® redundancy

Source: www.tcpipguide.com

RSLinx Support

As of RSLinx® 3.51, IP addresses that are changed with NAT will be shown using the Ethernet Devices driver (Figure 15). You can tell your device is NAT'ed because the IP Address on the "Port Configuration" screen does not match the header and address you used to browse to the device. The EtherNet/IP driver will show the NAT'ed address of the device, but you will not be able to connect.

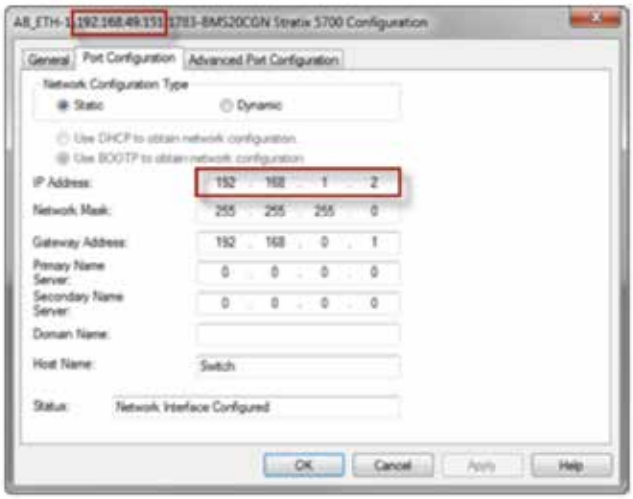

Figure 15 – RSlinx Support

Statistics

Statistics for NAT on the Stratix 5700 provide the ability to "drill down" into the configuration (Figure 16). This allows the user to see a global view for both operation and loading, then drill down into specific instances to see a detailed analysis of traffic for troubleshooting purposes (Figure 17).

Figure 16 – Overview Of NAT Statistics

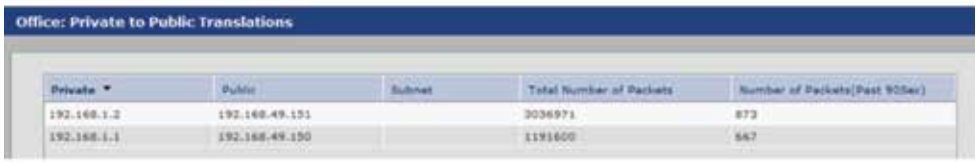

Figure 17 – Detail of NAT Statistics

Use Cases

Example 1: Using NAT With A Layer 3 Uplink

This scenario shows communications between the Line Controller (LC) and Controller 1 (C1) and the LC to Controller 2 (C2) with a Layer 3 switch, such as the Stratix 8300™, or router in between.

The LC and HMI are on the same VLAN, but a separate VLAN from Machine 1 (M1) and Machine 2 (M2). M1 and M2 are on the same VLAN and subnet. M1 is a duplicate of M2, so each share exactly the same IP Address configuration.

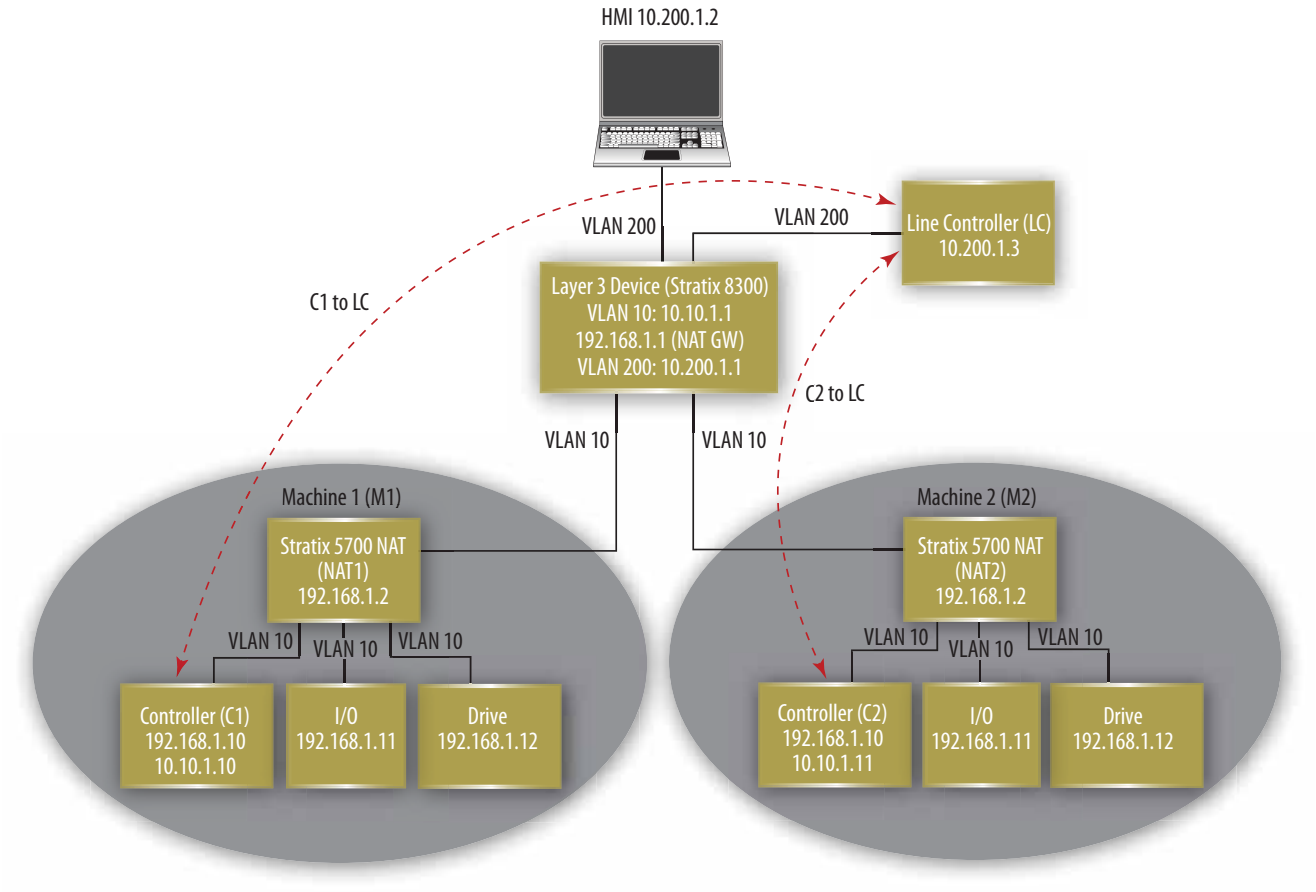

Figure 18 – Example 1

The circles show devices that fall within the private subnet of each Stratix 5700 NAT enabled switch. Communications between devices within the private subnet use private IP addressing schemes, for instance the I/O device (in M1) would not need a translation to talk to C1 and vice versa.

In this example NAT translations are done through port Gi1/1 of both switch NAT1 and switch NAT2.

C1 to LC Setup

This setup includes a translation for C1, giving it a public address of 10.10.1.10 and a translation for the default gateway. 10.10.1.10 is an address that could be any unused address on the 10.10.1.x subnet.

C1 will have a default gateway selected to be 192.168.1.1, which is an alias to 10.10.1.1. Once again, 192.168.1.1 could be any unused address in the 192.168.1.x subnet. Each device on the 192.168.1.x subnet will need to be configured to have a default gateway of 192.168.1.1. With this setup, C1 will be accessible to the LC, HMI and any other routed device on a different subnet (Figure 19).

Figure 19 – NAT1 (General Tab)

C2 to LC Setup

This setup includes a translation for C2, giving it a public address of 10.10.1.11 and a translation for the default gateway. 10.10.1.11 is an address that could be any unused address on the 10.10.1.x subnet. C2 will have a default gateway of 192.168.1.1, which is an alias to 10.10.1.1. Once again, 192.168.1.1 could be any unused address in the 192.168.1.x subnet. Each device on the 192.168.1.x subnet will need to be configured to have a default gateway of 192.168.1.1. With this setup C2 will be accessible to the LC, HMI and any other routed device on a different subnet (Figure 20).

The NAT instances on each switch will be attached to VLAN 10 of Interface Gi1/1.

Figure 20 – NAT2 (General Tab)

Example 2: NAT In A Ring Topology With Layer 3 Uplink

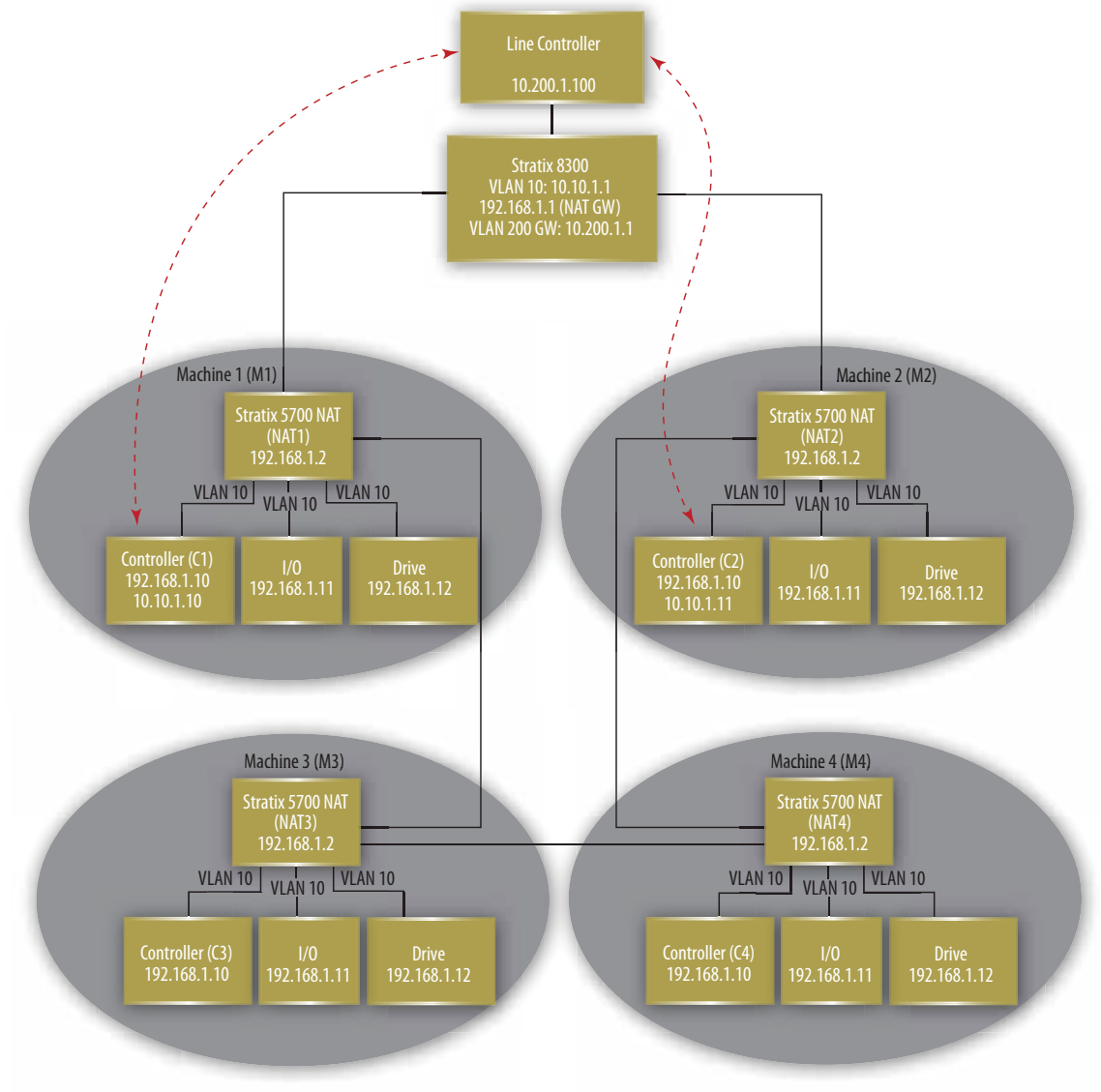

Figure 21 – Example 2

This scenario shows communications both between the Line Controller (LC) and Controller 1 (C1) and the Line Controller (LC) to Controller 2 (C2) in a ring configuration. Communications flow through a Layer 3 switch or router (such as the Stratix 8300) in between.

The LC is on a separate VLAN from Machine 1 (M1) and Machine 2 (M2). M1 and M2 are on the same VLAN and subnet. M1 is a duplicate of M2, so each share exactly the same IP address configuration.

The circles show devices that fall within the private subnet of each Stratix 5700 NAT enabled switch. Communications between devices within the private subnet use private IP addressing schemes, for instance the I/O device (in M1) would not need a translation to talk to C1 and vice versa.

In this example, NAT translations are done through both ports Gi1/1 and Gi1/2 of each of the NAT enabled switches.

C1 to LC Setup

This setup includes a translation for C1, giving it a public address of 10.10.1.10 and a translation for the default gateway. 10.10.1.10 is an address that could be any unused address on the 10.10.1.10 subnet.

C1 will have a default gateway that has been selected to be 192.168.1.1, which is an alias to 10.10.1.1. Once again, 192.168.1.1 could be any unused address in the 192.168.1.x subnet. Each device on the 192.168.1.x subnet will need to be configured to have a default gateway of 192.168.1.1. With this setup C1 will be accessible to the LC and any other routed device on a different subnet (Figure 22). In this scenario the translation will be applied to the same VLAN (10) on both ports Gi1/1 and Gi1/2. This will allow ring topologies to converge.

Figure 22 – Machine 1 NAT Switch Configuration (General Tab)

C2 to LC Setup

This setup includes a translation for C2, giving it a public address of 10.10.1.11 and a translation for the default gateway. 10.10.1.11 is an address that could be any unused address on the 10.10.1.x subnet. C2 will have a default gateway of 192.168.1.1, which is an alias to 10.10.1.1. Once again, 192.168.1.1 could be any unused address in the 192.168.1.x subnet. Each device on the 192.168.1.x subnet will need to be configured to have a default gateway of 192.168.1.1. With this setup C2 will be accessible to the LC, and any other routed device on a different subnet (Figure 23).

In this scenario the translation will be applied to the same VLAN (10) on both ports Gi1/1 and Gi1/2. This will allow ring topologies to converge.

Figure 23 – Machine 2 NAT Switch Configuration (General Tab)

Example 3: Using NAT With A Layer 2 Uplink

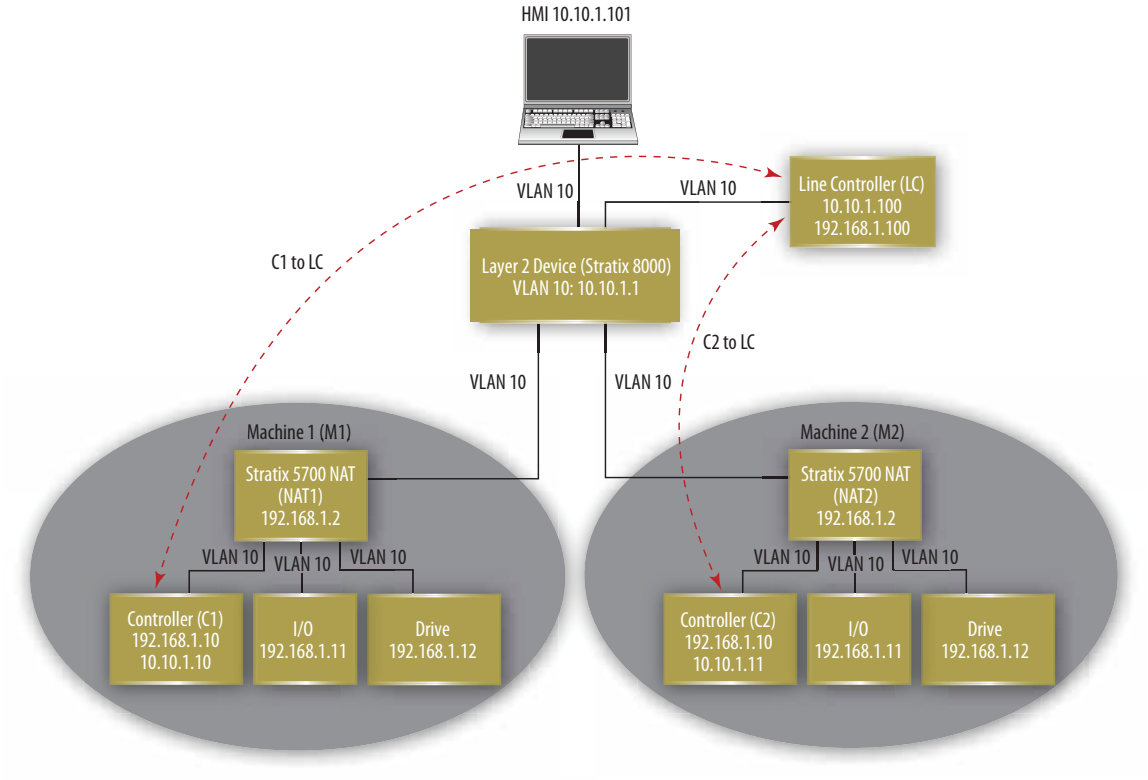

Figure 24 – Example 3

This scenario shows communications both between the Line Controller (LC) and Controller 1 (C1) and Line Controller (LC) to Controller 2 (C2) with a Layer 2 Switch such as the Stratix 8000™ in between.

In this example, everything is on the same VLAN but there are three separate subnets.

The circles show devices that fall within the private subnet of each Stratix 5700 NAT enabled switch. Communications between devices within the private subnet use private IP addressing schemes, for instance the I/O device (in M1) would not need a translation to talk to C1 and vice versa.

In this example NAT translations are done through port Gi1/1 of both switch NAT1 and switch NAT2.

C1 to LC Setup

Figure 25 – Machine 1 NAT Switch Configuration (General Tab)

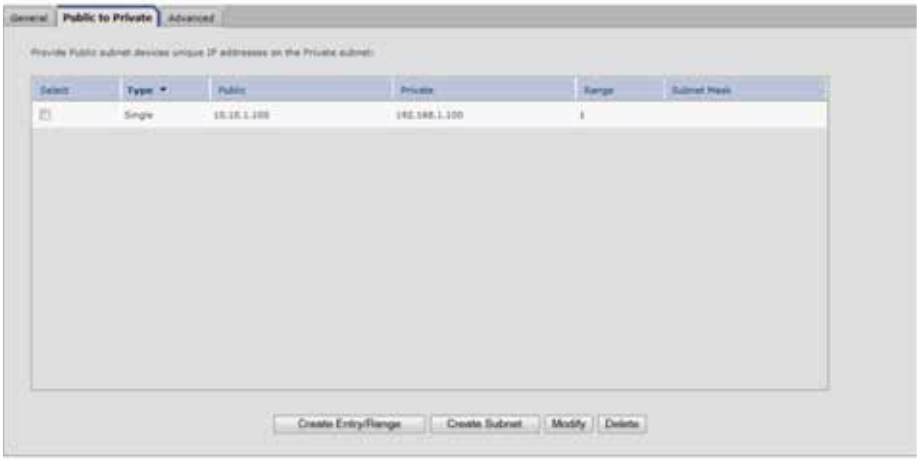

Figure 26 – Machine 1 NAT Switch Configuration (Public To Private Tab)

This setup includes a translation for C1, giving it a public address of 10.10.1.10 and a translation for the LC. 10.10.1.10 is an address that could be any unused address on the 10.10.1.x subnet (Figure 25).

The LC has an alias of 192.168.1.100, and device C1 does not need a gateway defined to talk to the LC. 192.168.1.100 is an address that could be any unused address on the 192.168.1.x subnet. With this setup, C1 will be accessible to the LC and any device on its private subnet (I/O1, Drive1) (Figure 26).

C2 to LC Setup

Figure 27 – Machine 2 NAT Switch Configuration (General Tab)

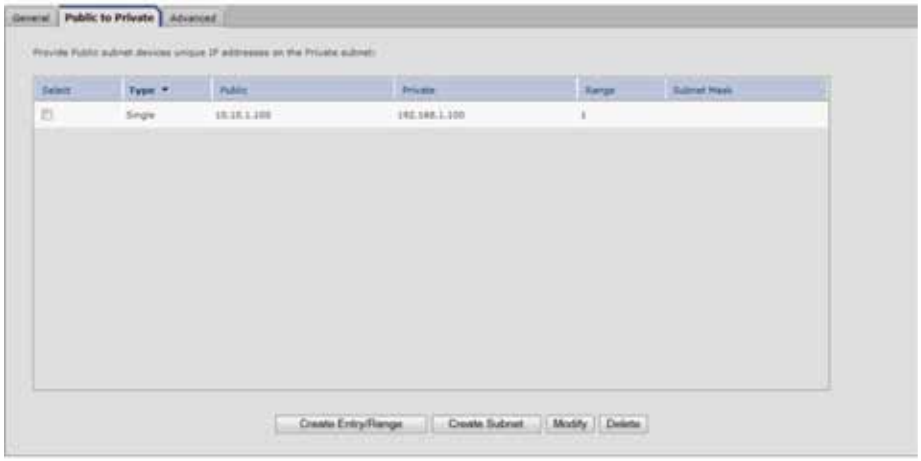

Figure 28 – Machine 2 NAT Switch Configuration (Public To Private Tab)

This setup includes a translation for C2, giving it a public address of 10.10.1.11 and a translation for the LC. 10.10.1.11 is an address that could be any unused address on the 10.10.1.x subnet (Figure 27).

The LC has an alias of 192.168.1.100, and device C2 does not need a gateway defined to talk to the LC. 192.168.1.100 is an address that could be any unused address on the 192.168.1.x subnet. With this setup, C2 will be accessible to the LC and any device on its private subnet (I/O2, Drive2) (Figure 28).

The NAT instances on each switch will be attached to VLAN 10 of Interface Gi1/1.

In this example, if C1 or C2 wants to send a message to the LC, the destination address specified in C1 or C2 would be 192.168.1.100.

Example 4: Machine To Machine Communication

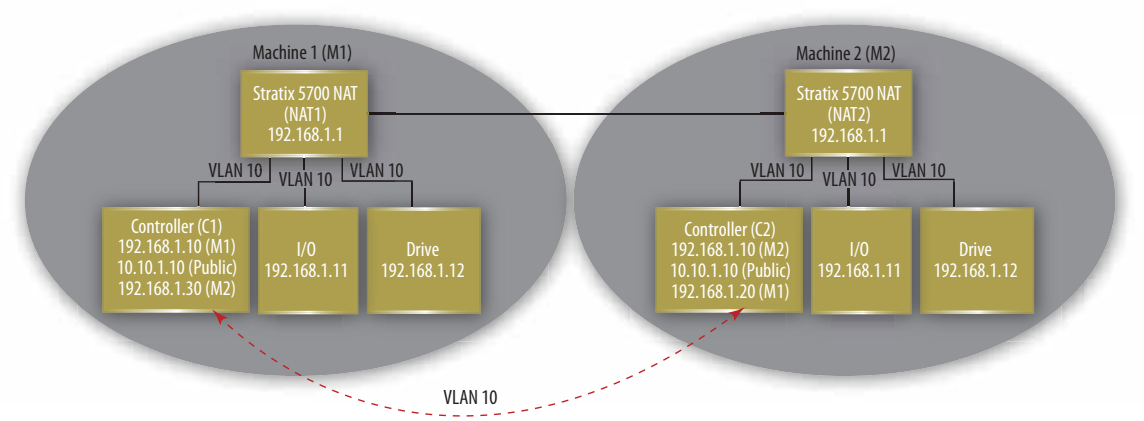

Figure 29 – Example 4

This scenario shows communications between Controller 1 (C1) and Controller 2 (C2) with two NAT enabled Stratix 5700 switches communicating directly with each other. In this example, everything is on the same VLAN but there are three separate subnets.

The circles show devices that fall within the private subnet of each Stratix 5700 NAT enabled switch. Communications between devices within the private subnet use private IP addressing schemes, for instance the I/O device (in M1) would not need a translation to talk to C1 and vice versa.

C1 to C2 Setup

Figure 30 – Machine 1 NAT Switch Configuration (General Tab)

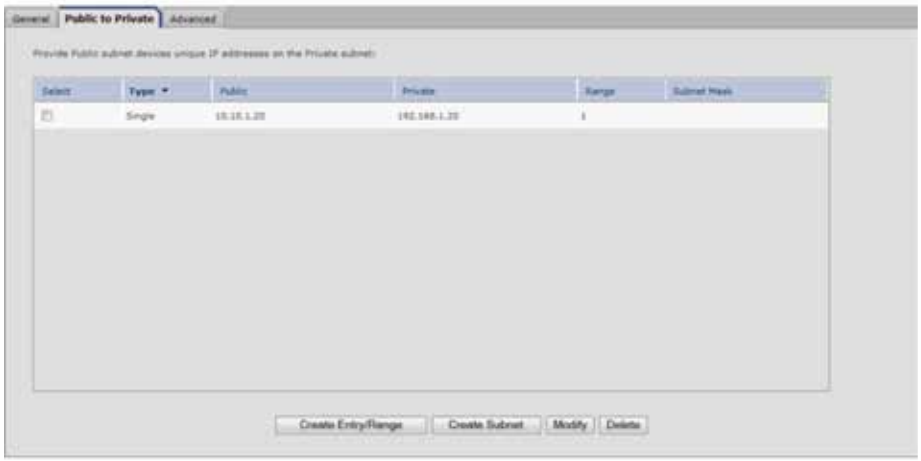

Figure 31 – Machine 1 NAT Switch Configuration (Public To Private Tab)

This setup includes a translation for C1, giving it a public address of 10.10.1.10 and a translation for C2. C2 has a public alias of 192.168.1.20, and device C1 does not need a gateway defined to talk to C2 (Figure 30, Figure 31).

Figure 32 – Machine 2 NAT Switch Configuration (General Tab)

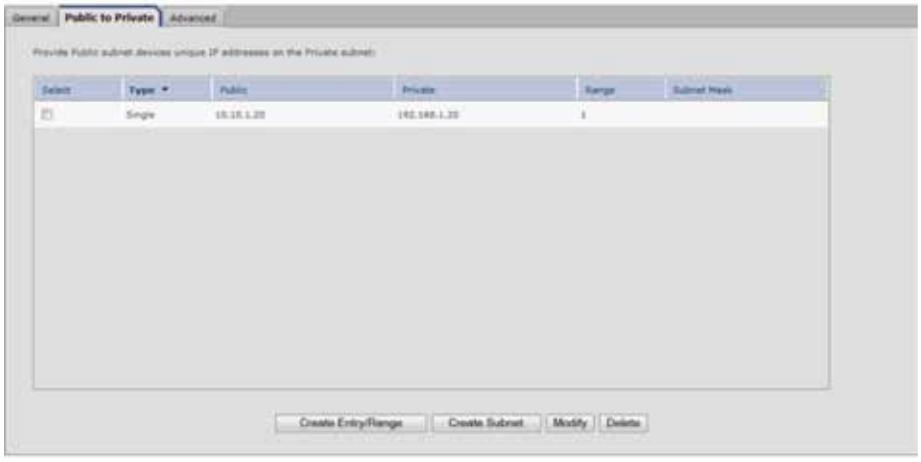

Figure 33 – Machine 2 NAT Switch Configuration (Public To Private Tab)

This setup includes a translation for C2, giving it a public address of 10.10.1.20 and a translation for the C1. The C1 has a public alias (from the perspective of M2) of 192.168.1.30. With this setup, C2 will be accessible to the C1 and vice versa (Figure 32, Figure 33).

The NAT instances on each switch will be attached to VLAN 10 of Interface Gi1/1.

Summary

Whether you're a machine and equipment builder or end user, Network Address Translation (NAT) can provide "wire speed" 1:1 IP address translations ideal for automation applications where performance is critical.

Stratix 5700 with NAT can help to:

- Easily integrate of machines into a plant network architecture
- Integrate and maintain duplicate machines without changing machine code
- Redeploy machines in new locations
- Support redundant architectures
- Differentiate OEM machine value with IT-ready solutions
- Integrate devices with single network connection
- Achieve proper segmentation for performance, reliability and security with VLANs and NAT

www.rockwellautomation.com

Power, Control and Information Solutions Headquarters

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

Publication ENET-WP032A-EN-E – August 2013