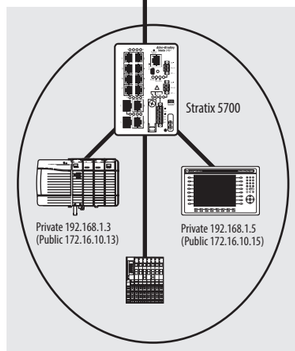
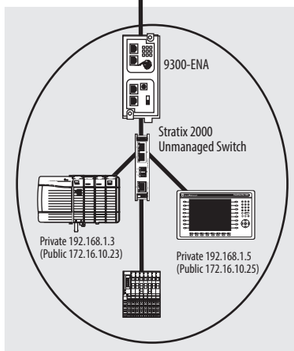
Rockwell Automation and EtherNet/IP Provide Multiple Options to Connect to Your Plant Network Using Standard Ethernet Technology



Stratix 5700 with NAT
System being designed requires NAT

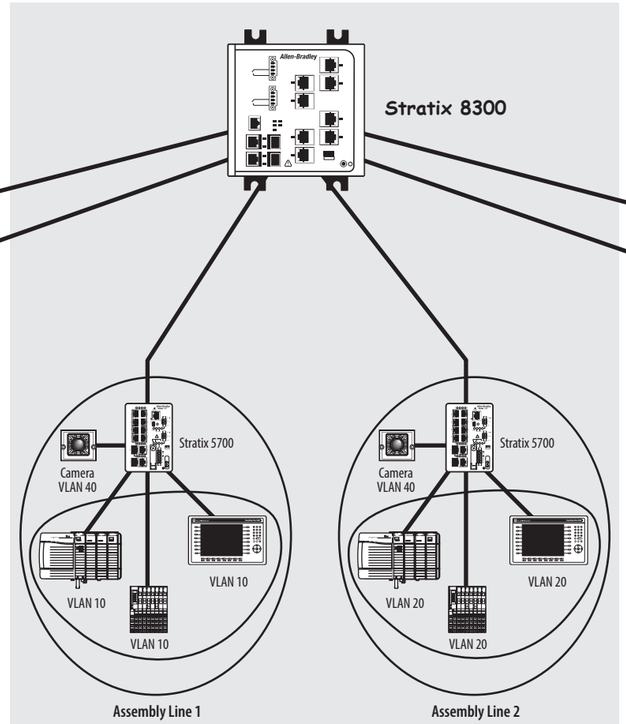


9300-ENA
NAT capability is desired to be added to an existing system

Easily Install Duplicate Machine Control Networks using NAT - Network Address Translation

"I want to install duplicate machine control networks using the same private IP addresses to reduce support issues and the need for multiple different controller program. However, I still need to access the some of the private nodes from my public plant network."

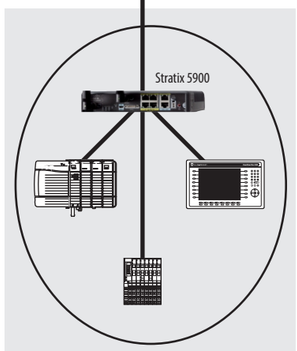
Use the Network Address Translation (NAT) capability in the Stratix 5700, Stratix 5900, or 9300-ENA to map your private nodes to addresses accessable from the public plant network. See the NAT illustration on the back for more information.



Logically Segment Networks with a Unique IP Address for Each Device using VLAN - Virtual Local Area Network

"I have VLANs on my system to logically segment nodes on the same physical network and to manage traffic levels. Typically my nodes on the same VLAN communicate together, but not outside their VLAN. However, I still need some of my nodes to communicate to multiple VLANs."

Use the Layer 3 Routing capability in the Stratix 8300 to allow some of these nodes to talk outside their VLAN. See the VLAN illustration on the back.

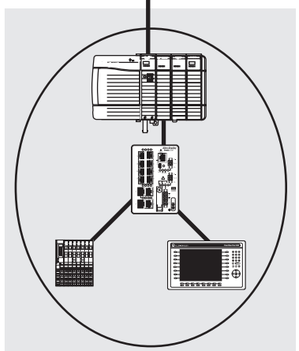


Additional Security Including a Firewall Stratix 5900

"I need to protect my network from unauthorized access or threats (i.e. viruses) from other networks from which it is connected."

Use the Stratix 5900 to control the incoming and outgoing traffic by using IP, packet, and content filtering.

The Stratix 5900 also supports NAT & VLANs for use in segmenting your networks.



Additional Security for the ControlLogix and Backplane 1756-EN2TSC

"I want additional protection for my ControlLogix (and all modules in its backplane including networks) to secure program uploads and downloads, communications between controllers, and other connections such as workstations."

Use the 1756-EN2TSC module with the IPsec protocol suite to add additional security to the EtherNet/IP network. IPsec provides authentication plus data authenticity, integrity, and confidentiality.

— Additional Security for Your Network —

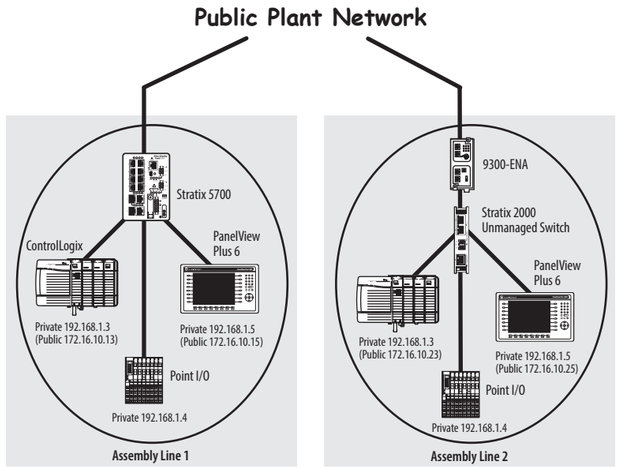
Segment Your Network

Publication IASIMP-QR029A-EN-E

Note: Information presented here is for illustrative purposes only

Rockwell Automation

Stratix/Infrastructure Product Family



Stratix 5700 with NAT
Applications requiring managed switch plus NAT capability

9300-ENA
Applications with Embedded or Unmanaged Switches

NAT Illustration

In this illustration, both lines have the same private IP addresses (ControlLogix-192.168.1.3, Point I/O-192.168.1.4, PanelView Plus 6-192.168.1.5) on their respective local control network. This allows the lines to be exact duplicates of each other, reducing development and support time. For those nodes that need to communicate to the public plant network (ControlLogix and PanelView Plus 6) the NAT mapping functionality in each of the three products shown allows these nodes to appear as a node on the plant network.

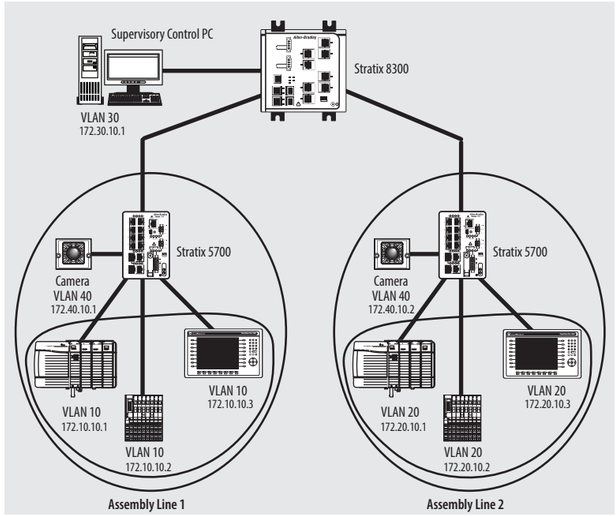
For example, if a Server PC on the public plant network (IP 172.16.10.1) needs to communicate to the ControlLogix on Line 1, it sees that ControlLogix as being on the public plant network at 172.16.10.13

Only the local control network nodes you select to map are accessable from the public plant network. The Point I/O is not accessable in this illustration.

Additional Resources

ENET-PP005B-EN-E	Stratix 5700 Industrial Ethernet Switch Product Profile
ENET-UM003A-EN-P	1756-EN2TSC EtherNet/IP Secure Communication User Manual
ENET-AT004B-EN-E	Segmentation Methods within the Cell / Area Zone
ENET-WP025-EN-E	Scalable Secure Remote Access Solutions for OEMs
ENET-WP031A-EN-E	Design Considerations for Securing Industrial Automation
ENET-TD001-EN-P	Converged Plantwide Ethernet (CPwE) Design and Implementation Guide (DIG)
ENET-QR001-EN-E	Stratix Switch Reference Chart
ENET-QR002-EN-E	Stratix 5700 Reference Chart
GMSP-PP001-EN-E	9300-ENA Network Address Translation Device Product Profile
SECUR-AT001A-EN-E	Industrial Security Best Practices

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



VLAN Illustration

In this illustration, the plant wishes to segment nodes on each of the two physical networks (Assembly Line 1 & 2) into 4 logical networks (VLANs 10, 20, 30, 40). This is to isolate devices for functional and/or traffic considerations.

The Stratix 5700 Layer 2 switch supports creating these VLANs.

VLAN 10 has a ControlLogix, it's Point I/O and a PanelView Plus 6. VLAN 20 has the same. These networks are isolated from each other.

VLAN 30 has a Supervisory Controller PC – again isolated from the others
VLAN (10 or 20 and 40) networks are on the same cable.

VLAN 40 illustrates another key advantage of VLANs. It contains streaming video cameras used for remote machine diagnostic support. These generate a lot of traffic, but since they are on a separate VLAN they have no impact on the local traffic of VLANs 10 & 20 or PC VLAN 30.

If a device on one VLAN needs to communicate to another (the Supervisory Controller PC needs to communicate to the Assembly Line 1 ControlLogix), the level 3 routing capability in the Stratix 8300 Layer 30 switch supports setting up this VLAN 30 to VLAN 10 link.

Catalog #	Description
1783-BMS10CL	Stratix 5700 Layer 2 Managed Switch, 10 Ports
1783-RMS10T	Stratix 8300 Layer 3 Managed Switch, 10 Ports
1783-MS10T	Stratix 8000 Layer 2 Managed Switch, 10 Ports
1783-SR	Stratix 5900 Security Appliance
1756-EN2TSC	ControlLogix Secure Communications Module
9300-ENA	Ethernet Network Appliance
1783-US08T	Stratix 2000 Unmanaged Switch, 8 Ports

Product Reference Table

Product	Managed Layer 2 Switch	NAT Mapping	Layer 3 Routing	Network Icon
Stratix 5700	X	X		Layer 2 Switch
Stratix 5900		X	X	Security Appliance
Stratix 8000	X			Layer 2 Switch
Stratix 8300	X		X	Layer 3 Switch (Router)
9300-ENA		X		N/A

Security Feature Table

Product	802.1x	Access Control Lists	IPSec	Firewall/ UTM	VPN
Stratix 5700	X	X			
Stratix 5900	X	X	X	X	X
Stratix 8000	X	X			
Stratix 8300	X	X			
1756-EN2TSC			X		X

802.1x Security - An IEEE standard for access control and authentication. It can be used to track access to network resources and helps secure the network infrastructure.

ACLs (Access Control Lists) - allow you to filter network traffic. This can be used to selectively block types of traffic to provide traffic flow control or provide a basic level of security for accessing your network.

IPSec (IP Security) - A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers.

Firewall - Asecurity system that controls the incoming and outgoing network traffic by analyzing the data packets and determining whether they should be allowed through or not, based on a rule set. A firewall establishes a barrier between a trusted, secure internal network and another network (e.g., the Internet) that is not assumed to be secure and trusted.

Unified Threat Management (UTM) - An evolution of the traditional firewall into an all-inclusive security product that has the ability to perform multiple security functions in one single appliance: network firewalling, network intrusion prevention and gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data leak prevention and on-appliance reporting.

VPN (Virtual Private Network) - A network that uses primarily public telecommunication infrastructure, such as the Internet, to provide remote users an access to a central organizational network. VPNs typically require remote users of the network to be authenticated, and often secure data with encryption technologies.