Power/mation®

Ethernet Infrastructure for The Modern Connected Plant

The Industrial Internet for Controls Engineers TRAINING 2019

COURSE LENGTH
1 Day
8:00am - 4:30pm

FEE
$250 per Person
Lunch Provided

DATE & LOCATION
January 30, 2019 St. Paul, MN

TRAINERS
Terry Busch, Business Development Manager

David Ellers, Business Development Manager

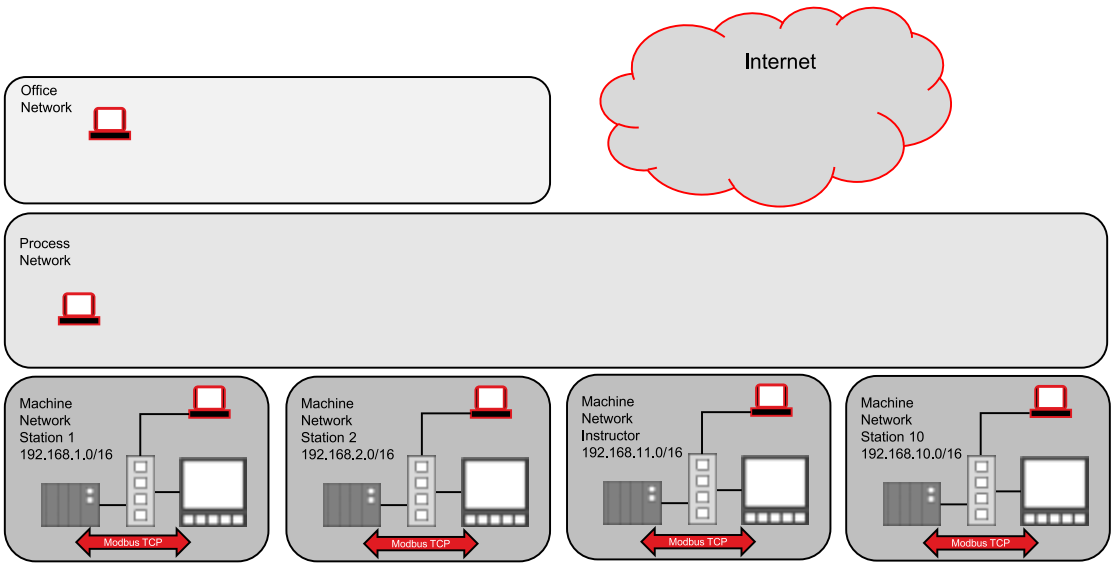
Industrial Ethernet is everywhere on the plant floor. It is the nervous system of the modern Industrial Control System (ICS). This one day class will give controls engineers an introduction to, and hands on experience with, some of the most common ethernet networking components. They can use this knowledge and experience to enhance the performance and security of their organization's ICS.

Course Agenda

LAB 1 - LANs in the Machine Network & Network Troubleshooting

Wireshark is a valuable tool for everyone working with ethernet networks. For a controls engineer, this tool allows monitoring of control data, dissecting protocol data and displaying this data in an easy to read format. You can quickly see what devices are asking for data and what devices are being sent data. In lab 1, participants will learn the following:

- ICMP Ping
- Port Mirroring
- ARP
- BootP
- Wireshark

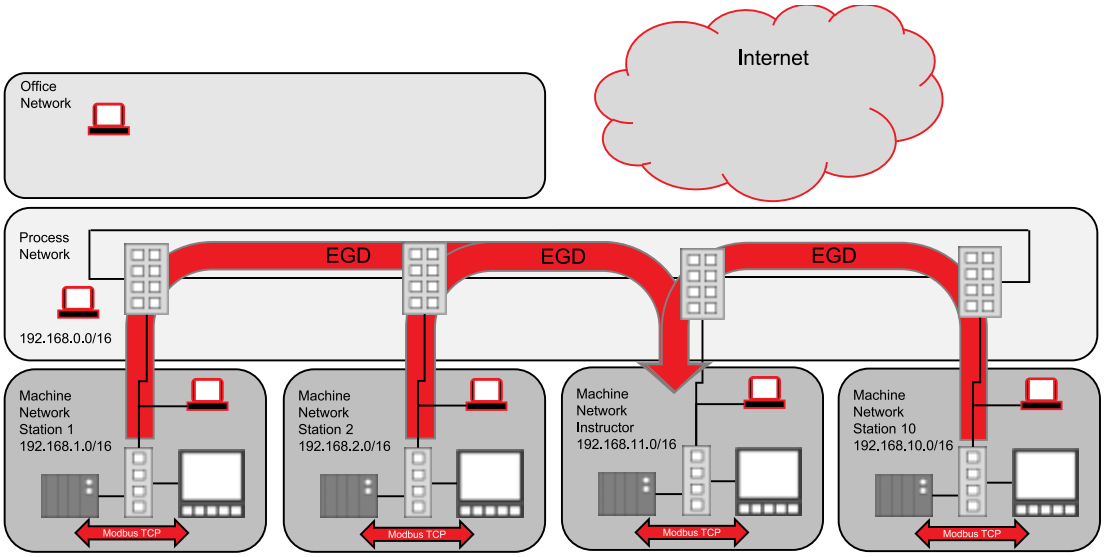


MORE INFO:
mandy.huston@powermation.com
www.powermation.com | 800.843.9859

LAB 2 – Connecting Machine Networks to the Process Network & Media Redundancy

Managed switches are the backbone to a well-designed process control network. A managed switch gives a controls engineer insight to the network connection health, as well as the ability to mirror ports and filter multicast messages. In lab 2, participants will learn the following:

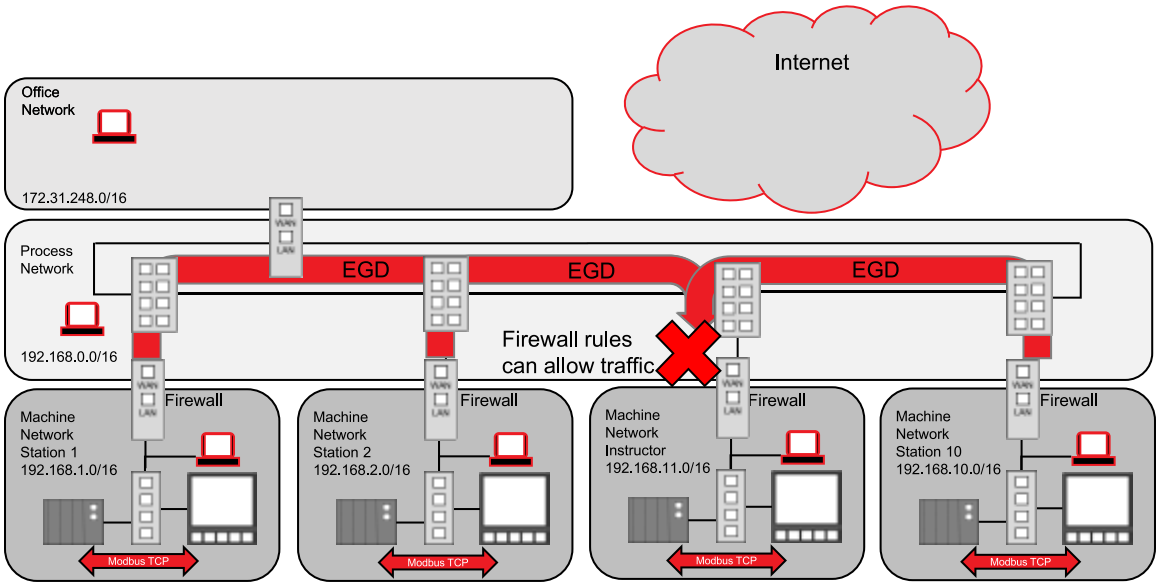
- Media Redundancy
- Port Mirroring
- Monitoring network traffic with built-in diagnostics and Wireshark



LAB 3 – Securing the Machine & Process Networks with Firewalls

Firewalls are internet security. A properly configured firewall allows traffic between devices and denies access to unwanted traffic. Industrial ethernet devices have been traditionally designed without security. If a manufacturer added security, it was typically turned off or left wide open by default. Legacy devices like these are prominent in manufacturing and infrastructure controls environments, creating potential vulnerabilities. In lab 3, participants will learn the following:

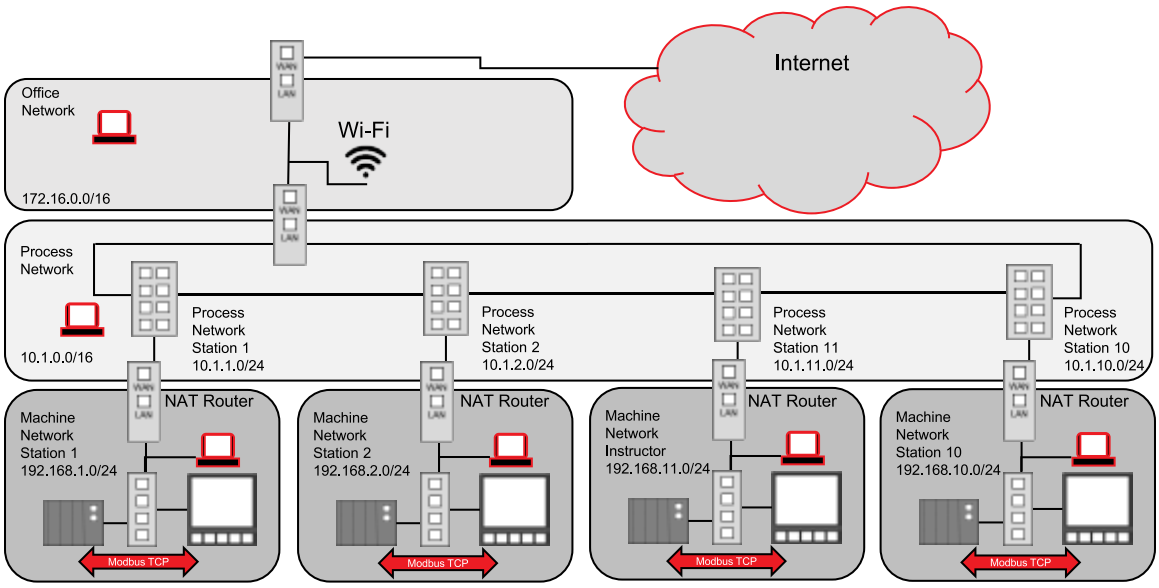
- Configuring Firewalls
- Filtering IP addresses or MAC address
- Filtering Applications or Port Numbers
- User Firewall Authentication



LAB 4 – Protecting & Segmenting the Machine & Process Networks with NAT Routers

A router is a device that forwards data packets between computer networks. Routers give controls engineers islands of automation allowing separation between control panels. Routers also give isolation between the office network and the manufacturing or process network allowing the controls engineer to use whichever IP address and whichever quantity of IP addresses they choose. Network Address Translation (NAT) allows access to a machine network from a process network. 1:1 NAT is used to allocate IP addresses in the process network to be directly translated to IP addresses in the machine network. In lab 4, participants will learn to:

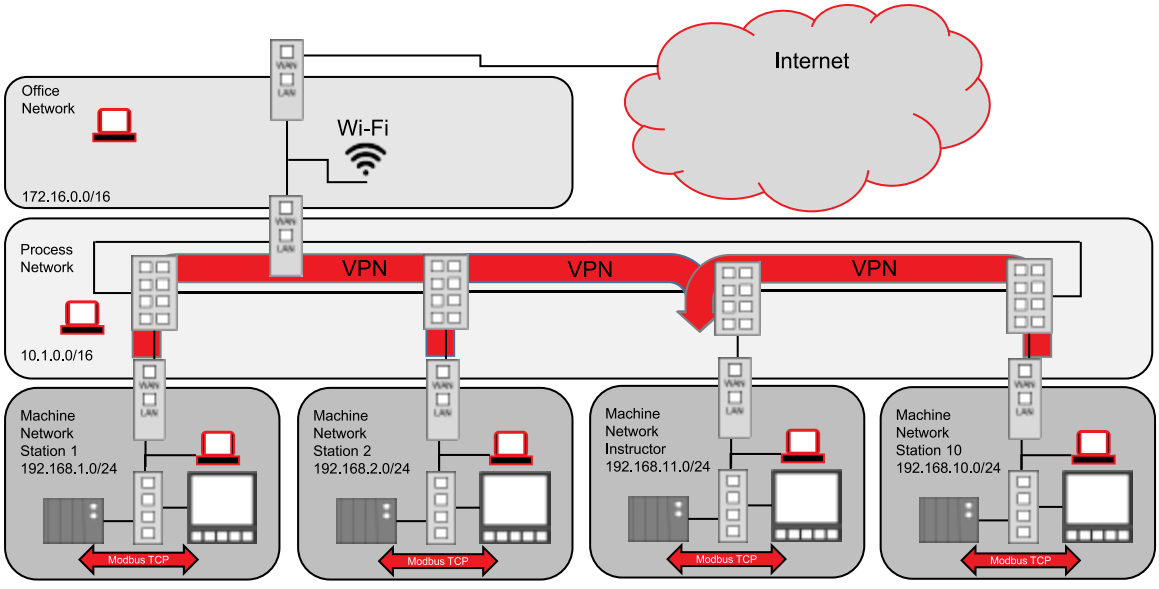
- Configure the network settings for the LAN and WAN of a router
- Demonstrate how the router acts as the default gateway of a network
- Configure 1:1 NAT
- Configure IP Masquerading



LAB 5 – Enabling Secure Machine to Machine Communications with VPN Routers

VPN is a secure method of tunneling between two networks. The tunnels can be physically in the same panel, in the same facility, in the same company, or even between an OEM and an end user. Lab 5 will introduce this method of authenticated and encrypted communications. In lab 5, participants will learn the following:

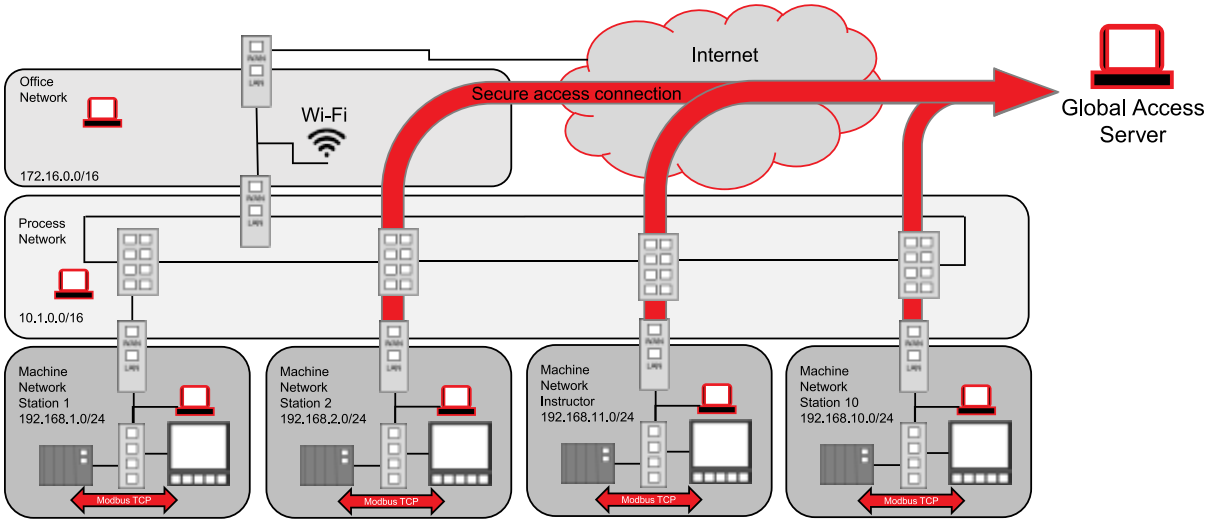
- Creating VPN tunnels between networks
- X.509 certificate based authentication
- Encryption
- VPN NAT



LAB 6 – Global Access

The tools that provide secure communication to machines or systems over a network typically beyond the control of the user. Connecting remotely enables an OEM or data services provider to deliver support, monitoring, operating, data acquisition and analytics.

- SSL Appliances
- VPN Appliances
- Multi-User Access
- Cloud-Based Access



MORE INFO:
marketing@powermation.com