



**Process Control Systems  
Industry Conference**

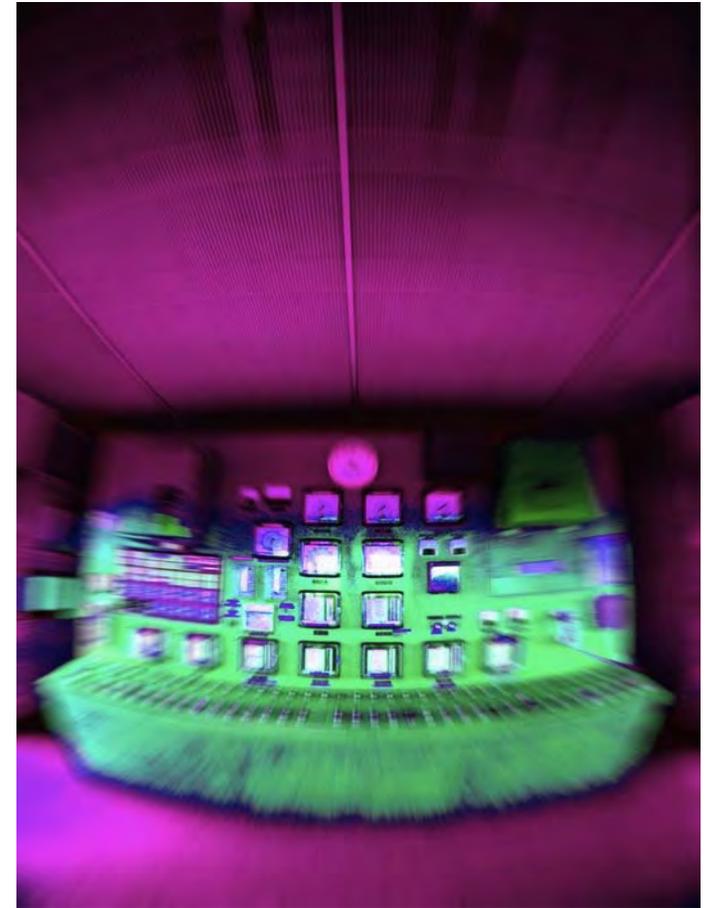
# **Policy Based Networks in Process Control**

## **Design and Deployment Techniques**

**Steve Hargis**  
**Enterasys Networks**

# The Evolving Process Control Network

- **Significant increase in use (and dependencies) on standards-based Ethernet topologies and IP communications protocol in the plant environment**
- **Modern Business/Process interfaces are driven by LAN based technologies**
- **Greatly increased security concerns (driven by the “new” process control network)**
  - Trusted Access
  - Vulnerabilities
  - Malicious Threats
  - Denial of Service
  - Theft of Information
  - Faulty Applications



# Diversity in the *Connected* Environment

## ◆ Machine-centric end systems

- PLC
- Smart Relay
- Data Historian
- IP Camera
- IP Phone
- Instrument

## ◆ Human-centric end systems

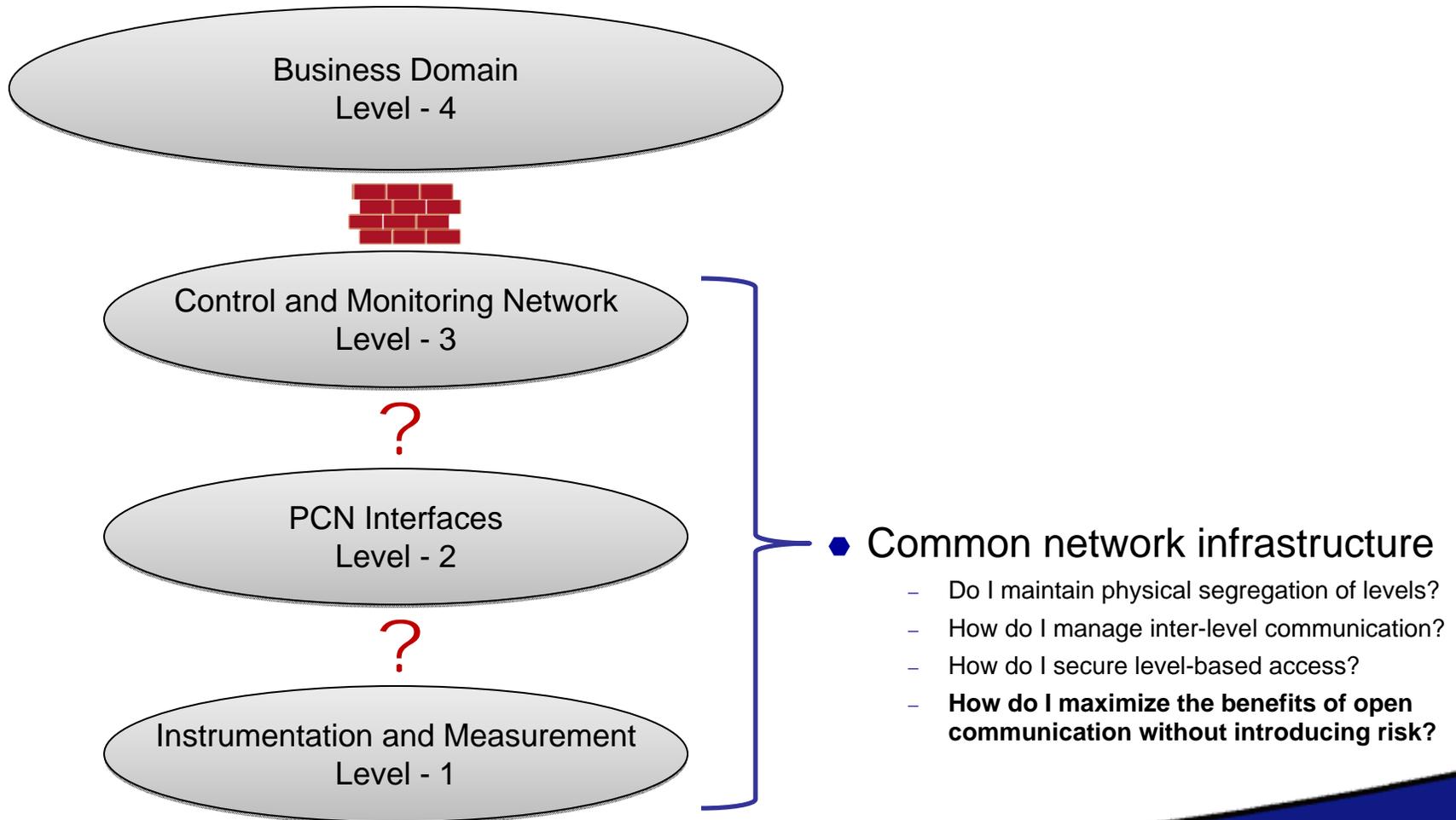
- HMI / Control Console
- Desktop
- Laptop
- Handheld

Standards-Based  
Communication



*Increased capability of communication between diverse elements offers improved process, but can introduce significant risk!*

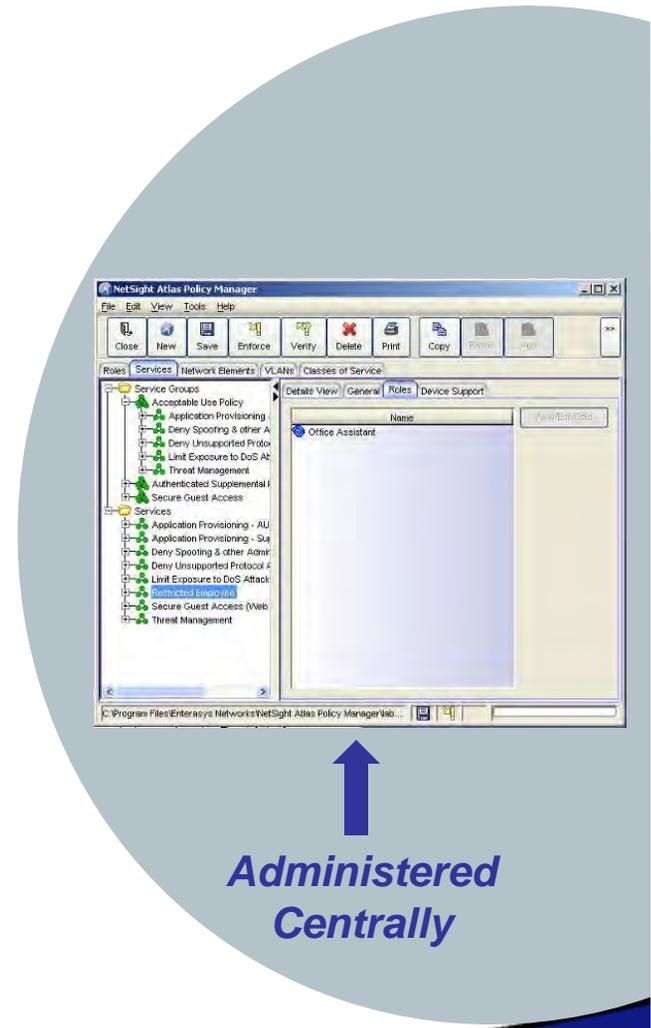
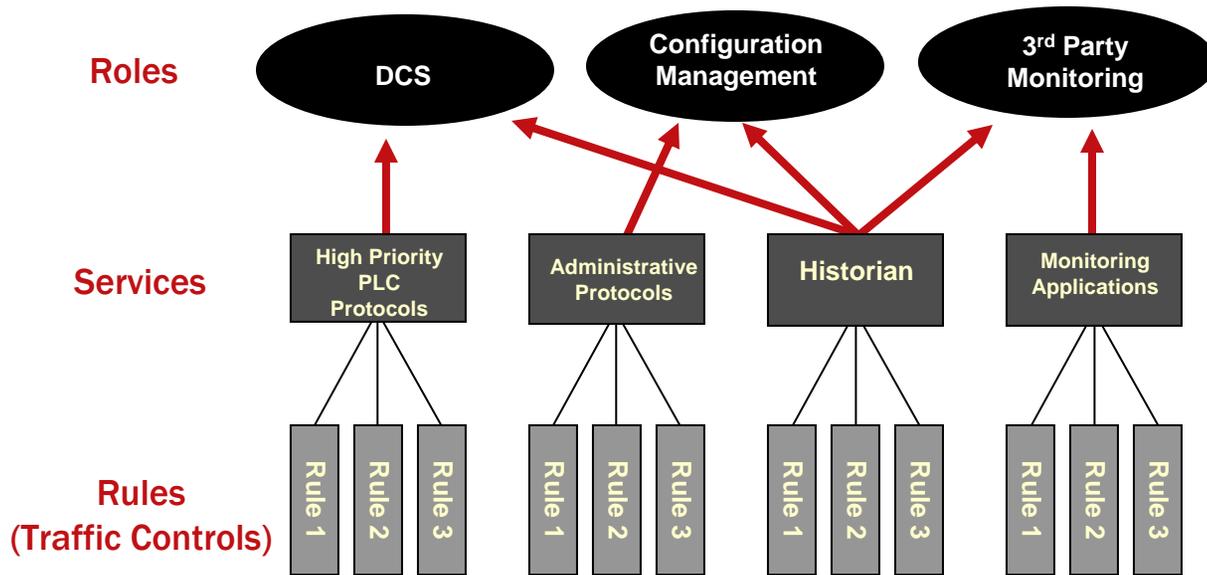
# Desegregated Communications – But How?



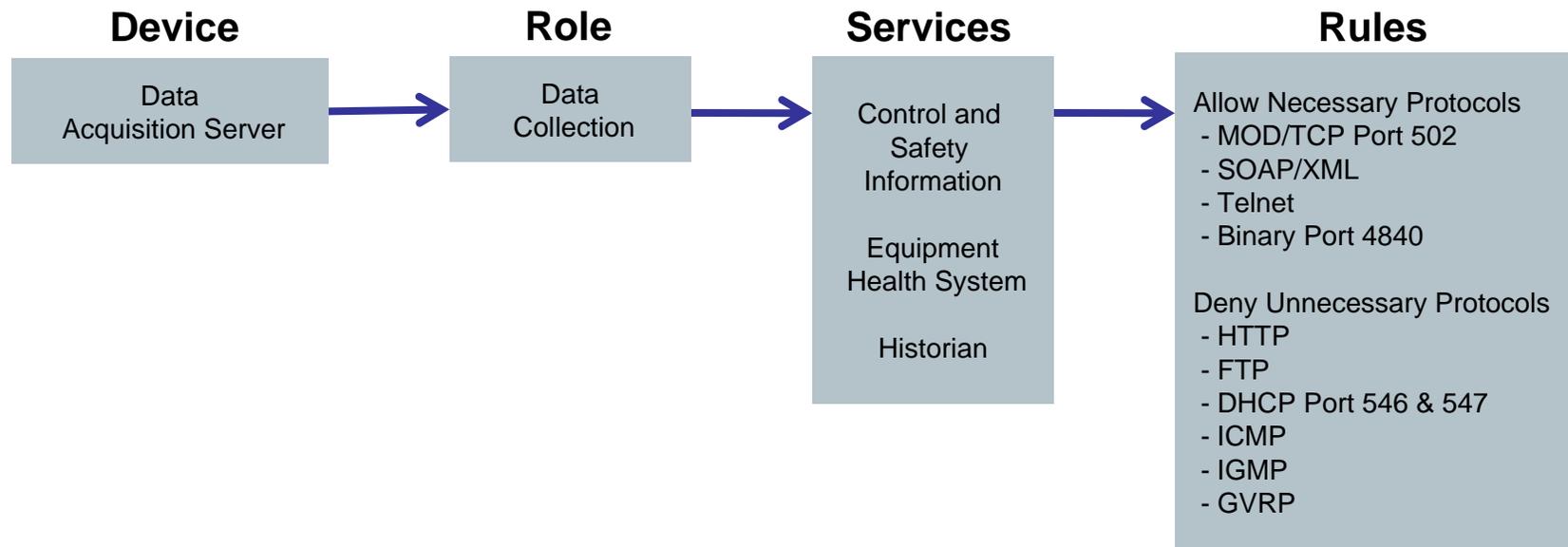
# Network Policy Maximizes Communications

- ◆ **The policy-enabled network understands context**
  - Who, want, where, when, etc.
  - This context can be used to allow or restrict communications in the network in a granular fashion
- ◆ **Segregation is now logical – and controlled from a centralized policy management console**
  - Maintains security with *boundaries* for communications – while leveraging a common physical infrastructure
- ◆ **Enables secure and deterministic communications!**
  - Business justified communications – process enablement.

# A Policy Framework



# Applying Policy Framework to Process Control



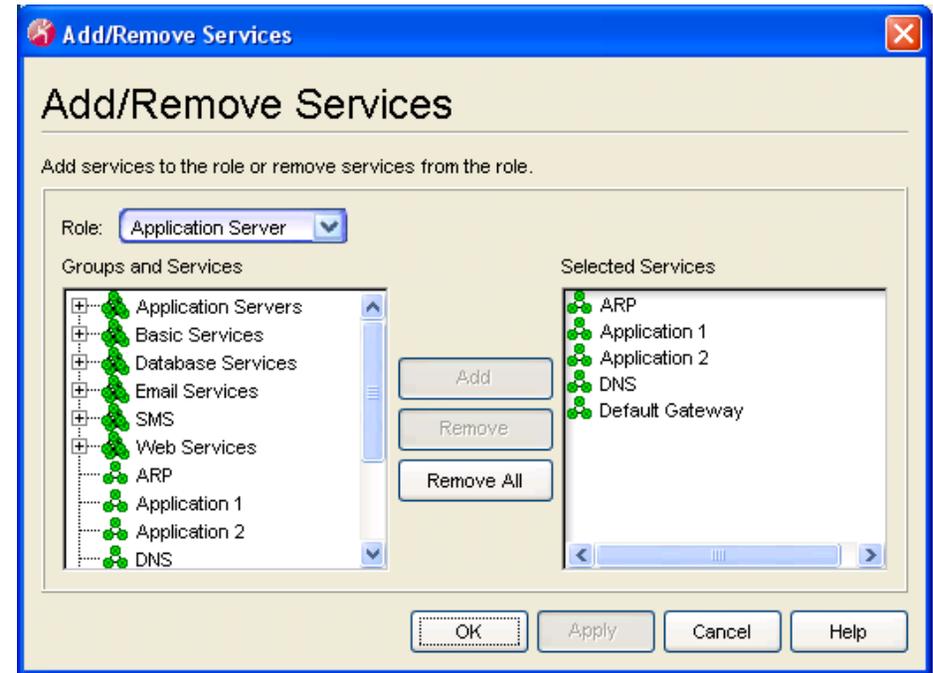
# Simple Administration is Paramount

## Non-Centralized / Complex Approach

```
31 !
32 ip nbar port-map custom-01 tcp 3389
33 ip nbar port-map dns tcp tcp 53
34 ip nbar access-list 101 permit tcp any host 192.168.1.10 eq 80
35 ip nbar access-list 101 permit tcp any host 192.168.1.10 eq 443
36 ip nbar access-list 101 permit tcp any host 192.168.1.11 eq 21
37 ip nbar access-list 101 deny ip any any
38 ip nbar access-list 102 permit tcp host 192.168.1.10 any eq 80
39 ip nbar access-list 102 permit tcp host 192.168.1.11 any eq 443
40 ! access-list 102 permit tcp host 192.168.1.10 0.0.0.255
67 !
68 class
69 match
70 access-list 101 permit tcp any host 192.168.1.2.11.10 eq 80
71 access-list 101 permit tcp any host 192.168.1.10.2.11 eq 443
72 access-list 101 permit tcp any host 192.168.1.2.13.11 eq 21
73 access-list 101 deny ip any any
74 access-list 102 permit tcp host 192.168.1.10.2.11 any eq 80
75 access-list 102 permit tcp host 192.168.1.10.1.11 any eq 443
76 access-list 102 permit tcp 192.168.1.0.10 0.0.0.255
77 _172.16.1.0.0.0.255 eq 22
78 access-list 102 deny ip any any
79 access-list 103 permit tcp host 192.168.2.13 any eq 21
80 access-list 103 permit tcp 172.16.1.0.192.168.1.12 0.0.0.1
81 172.16.1.0.0.0.255 eq 22-0.0.0.255-192.168.0.0
82 0.0.255.255 eq 22
83 access-list 103 deny ip any any
84 access-list 104 permit tcp 172.16.1.0.0.0.255
85 192.168.0.0.0.255.255 eq 22
86 access-list 104 deny ip any any
87
88 set dscp af12
89
90 priority percent 25
91 !
```

X n switches  
Hours to deploy!

## Centralized / Intelligent Management Approach



System wide  
Seconds to deploy!

# Pervasive Policy Enforcement

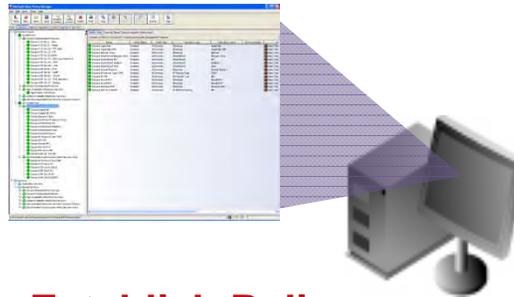
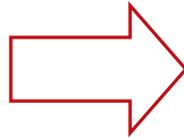
## Network Policies

“MOD/TCP and OPC Protocols are mission critical communications.”

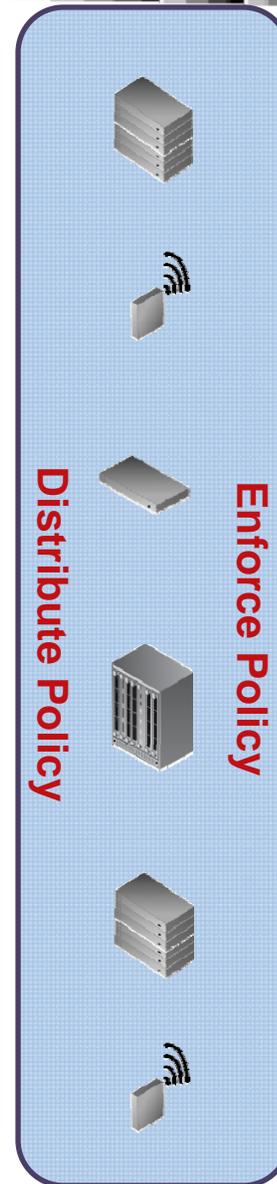
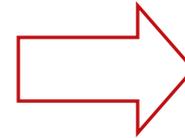
“A user or device must not use up too much bandwidth.”

“A typical end system should never be a DHCP server.”

“Only IT administrators should configure infrastructure components.”



**Establish Policy**



# Architecting a Policy Based Network

## ◆ Must be...

- simple to deploy/operate yet highly effective
- secure enough to ensure process integrity and compliance
- dynamic in controlling access
- able to accommodate all needed process communications
- intelligent to understand the context of what and who is connecting
- easily adaptable to new communication requirements
- standards based

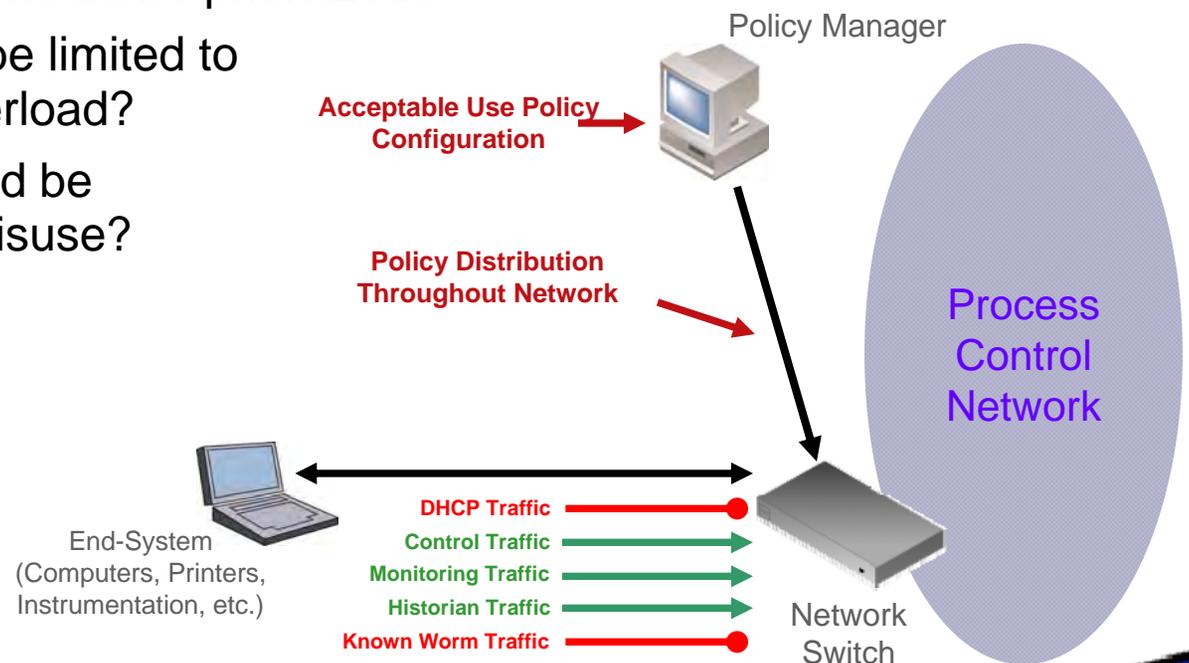
# Policy Deployment – Phased Approach

- ◆ **Phase 1 – Enforce Acceptable Use Policy to all connection points**
  - Deny any unnecessary protocols and TCP/UDP ports to minimize risk
- ◆ **Phase 2 – Enforce Deterministic Communications**
  - Use NetFlow to identify required communications between systems
  - Restrict communication between unrelated systems
  - Enforce application QoS
- ◆ **Phase 3 – Enforce Dynamic Policy Assignment**
  - Leverage endpoint assessment/identification for device-specific policy
  - Leverage device/user authentication for role-based policy

# Policy Deployment – Acceptable Use Policy

## ◆ Default Policy Rules (no end-system dependencies)

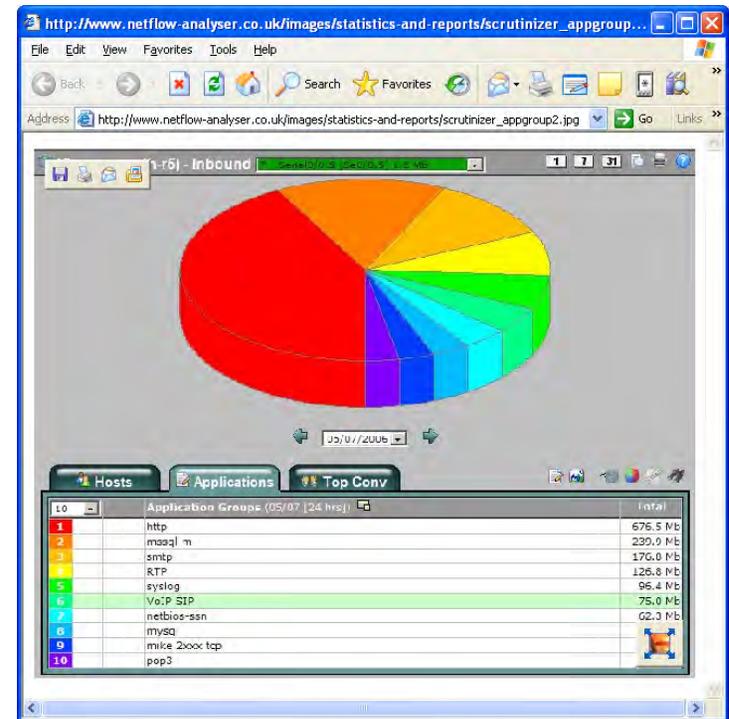
- Which protocols are allowed?
- Which applications should be prioritized?
- What traffic should be limited to prevent network overload?
- What services should be filtered to prevent misuse?



# Policy Deployment - Analysis

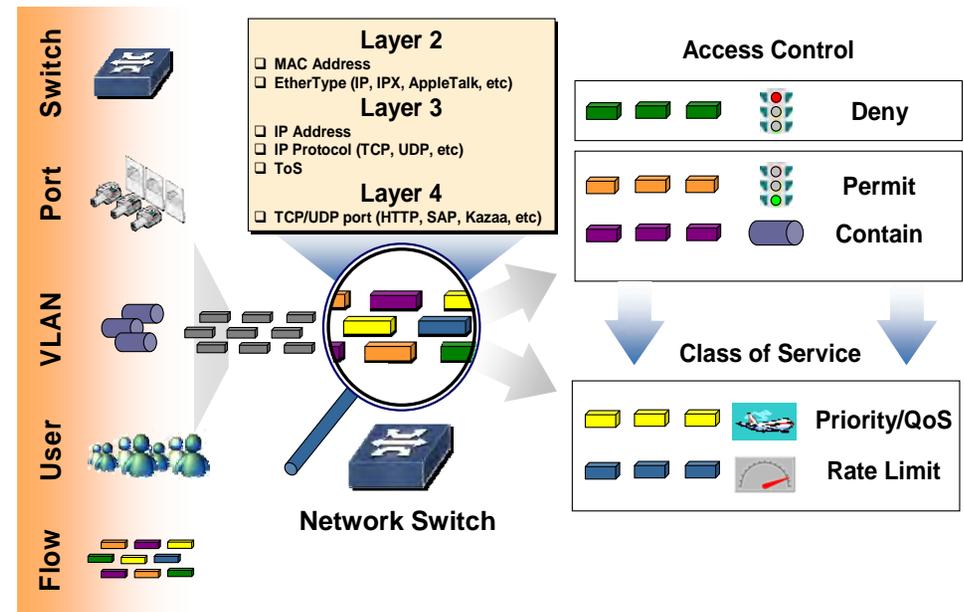
- What communication traffic is “on” the network – and is it necessary?
  - NetFlow
- To what should users and devices connect?
- How should users and devices communicate with each other?

Layers		L1	L2	L3	L4	WAN							
L1	Devices	8 (PLC)	9 (Converter)	10 (Converter)	11 (Laptop)	2a (Modbus Client)	3b (Schneider Crt)	4 (Schneider Cr)	5 (Converter)	6 (Laptop)	1 (Level 4 Client 1)	2 (Level 4 Client 2)	
L2	8 (PLC)			ModTCP (Read/Write)	ModTCP (Read/Write)	ModTCP (Read Only)							
L3	9 (Converter)			Serial over IP									
L4	10 (Converter)												
WAN	11 (Laptop)	ModTCP (Read/Write)											
	2a (Converter)	ModTCP (Read/Write)	Serial over IP										
	3b (Modbus Client)	ModTCP (Read/Write)											
	4 (Schneider Cr)	ModTCP (Read Only)											
	5 (Converter)												
	6 (Laptop)												
	1 (Level 4 Client 1)												
	2 (Level 4 Client 2)												
	User Group 2												
	User Group 3												
	Remediation Server												
	Microsoft Server												



# Policy Deployment – Deterministic Communications

- ◆ Are there applications which require low latency?
  - Instrumentation
- ◆ Are there mission critical applications?
  - MOD/TCP
- ◆ Are there remote management applications which must maintain visibility?
  - SNMP
  - TFTP



# Policy Deployment – Dynamic Enforcement

- ◆ **What is the type of device attempting to communicate on the network?**
  - MAC-Based Authentication
  - OUI Mask Association
  - Endpoint Detection (CDP, LLDP, LLDP-MED, SIP)
- ◆ **Who (if anyone) is using the device?**
  - Web-Based Authentication
  - 802.1X Authentication (Digital Certificates, Biometrics, etc.)
- ◆ **Based on the context of device type and user, what communications should be allowed?**
  - Enforced dynamically at the point and time of connection



# Summary

*A policy-based network for process control should...*

- ✓ ...control **network access** to every device, user, and application attempting to communicate on the network.
- ✓ ...completely enforce the **acceptable usage policies** of the process control network resources.
- ✓ ...**identify** each end system and user, and determine communication privileges based on their **role** in the environment.
- ✓ ...**automatically** identify any unsafe or dangerous end system **prevent** it from adversely affecting the network environment.
- ✓ ...instantly identify any **threat** on the network and then **mitigate** it at its source.
- ✓ ...**prevent** devices and users from **misusing** available bandwidth for unauthorized network communications.
- ✓ ...provide a comprehensive **audit trail** of device and user location, application communication, and security events.



***A well architected,  
policy-based network  
for process control can  
securely enable critical  
communications!***

# Thank You.

- ◆ **Secure Networks for Process Control Whitepaper**

- <http://www.enterasys.com/company/literature/sn-pc-wp.pdf>

- ◆ **See a Policy-Based Network in Action!**

- Visit the Enterasys Booth tonight at the Solution Provider evening event.