Reference Architectures: Fundamentals of Industrial Ethernet Network Design

Workshop #07

Paul Didier - Cisco Systems
Industry Solutions Architect for Manufacturing

Gregory Wilcox - Rockwell Automation
Networks Business Development Manager
Reference Architectures
W7: Reference Architectures: Fundamentals of Industrial Ethernet Network Design

- This Workshop demonstrates core principles for designing industrial Ethernet networks using the concepts delivered in the Rockwell Automation and Cisco Converged Plantwide Ethernet Architectures. It includes best practices and recommendations that are applicable to both IT and manufacturing networks as well as switch/router deployment. A prior understanding of general Ethernet concepts is recommended.
• T40: Achieving Secure Remote Access to Plant-Wide Applications
  • Time: 1:00 PM
  • Room: Room 211B
  • Gregory Wilcox and Paul Didier

• T42: Applying Plant-Wide Industrial Wireless Communications
  • Time: 3:00 PM
  • Room: Room 211B
  • Paul Brooks and Dan Knight

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
Agenda

- Industrial Network Convergence
- Network Design Methodology and Fundamentals Utilizing Standards, Reference Models and Reference Architectures
- Networking Best Practices – Design & Implementation Considerations
  - Multicast Management
  - Segmentation
  - Prioritization
  - Resiliency Protocols and Multi-path Topologies
  - Switch Features and IP Addressing
  - Security
- Additional Resources
- Questions and Answers
Industrial Network Convergence

Convergence of Control and Information
Integrated Architecture
Enabling Convergence

Enterprise Business Systems
SCM | ERP | CRM | PLM ...

Enterprise Infrastructure

FactoryTalk® Integrated Production & Performance Suite
Design & Configuration
Production Management
Data Management
Quality & Compliance
Asset Management
Performance & Visibility

Industrial Infrastructure

Logix Control Platform
Discrete
Motion
Process
Batch
Safety
Drives

Critical Plant Assets

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
Industrial and Enterprise (IT) Network Convergence

- **Enterprise (IT) Network Requirements**
  - Internet Protocols
  - Enterprise class gear
  - High availability – redundant star topologies
  - Determinism, latency, jitter, etc.
  - Voice, video, data applications
  - IP Addressing - dynamic
  - Security - pervasive

- **Industrial Network Requirements**
  - Industrial and internet protocols
  - Industrial gear
  - Resiliency – ring topologies are prominent, redundant star topologies are emerging
  - Determinism, latency, jitter, etc.
  - Motion, control and safety
  - IP Addressing – static
  - Security - emerging

So, what are the similarities and differences?
Common LINGO

- Ethernet and IP
- Ethernet-n-IP
- EtherNet/IP
- EtherNet/IP = Ethernet + IP + CIP
How IT Ready is Your Industrial Solution?

• Align your industrial Ethernet configurations with your, or if partner, your end customers IT policies
  – Use standard Ethernet and TCP/IP protocol suite
  – Use managed switches for network and security services
  – Follow IP addressing, subnetting and default gateway settings conventions
  – Consistently use Network Services
    • Virtual LANs (VLANs), Multicast Management, Quality of Service (QoS), Resiliency, Protocols, Layer 2 and Layer 3
  – Security stance - port security, access control lists, network access control

• Are you aligned with emerging Industrial Control System security standards:
  – DHS External Report # INL/EXT-06-11478
  – NIST 800-82
  – ISA-99
Industrial Network Design Methodology

- Understand application and functional requirements
  - Devices to be connected – industrial, commercial
  - Data availability, integrity & confidentiality
  - Communication patterns, topology & resiliency requirements
  - Types of traffic – information, control, safety, time synchronization, motion control, voice, video

- Develop a logical framework (roadmap)
  - Define zones
  - Define segmentation
  - Place applications and devices in the framework based on requirements

- Determine security requirements, take into consideration IT requirements

- Use standards, reference models and reference architectures
Industry Standards

• Technology
  – IEEE 802.3 - standard Ethernet, Precision Time Protocol (PTP - 1588)
  – IETF - standard Internet Protocol (IP)
  – ODVA - Common Industrial Protocol (CIP)
  – IEC – International Electrotechnical Commission

• Manufacturing
  – Purdue Reference Model for Control Hierarchy
  – ISA-95 - Enterprise-Control System Integration
  – ISA-99 - Manufacturing and Control Systems Security
  – NIST 800-82 – Industrial Control System Security
Logical Framework

Level 5
- Router
- Enterprise Network

Level 4
- E-Mail, Intranet, etc.
- Site Business Planning and Logistics Network

DMZ
- Terminal Services
- Patch Management
- AV Server
- Application Mirror
- Web Services Operations
- Application Server

Enterprise Zone
- Firewall
- Web E-Mail CIP

Manufacturing Zone
- Site Manufacturing Operations and Control

Cell/Area Zone
- Area Supervisory Control

Level 3
- FactoryTalk Application Server
- FactoryTalk Directory
- Engineering Workstation
- Domain Controller

Level 2
- FactoryTalk Client
- Operator Interface
- Engineering Workstation
- Operator Interface

Level 1
- Batch Control
- Discrete Control
- Drive Control
- Continuous Process Control
- Safety Control

Level 0
- Sensors
- Drives
- Actuators
- Robots
- Process

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
The OSI Reference Model

<table>
<thead>
<tr>
<th>Layer Name</th>
<th>Layer No.</th>
<th>Function</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Layer 7</td>
<td>Network Services to User App</td>
<td>CIP</td>
</tr>
<tr>
<td>Presentation</td>
<td>Layer 6</td>
<td>Encryption/Other processing</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>Layer 5</td>
<td>Manage Multiple Applications</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>Layer 4</td>
<td>Reliable delivery/Error correction</td>
<td>TCP - UDP</td>
</tr>
<tr>
<td>Network</td>
<td>Layer 3</td>
<td>Logical addressing - Routers</td>
<td>IP</td>
</tr>
<tr>
<td>Data Link</td>
<td>Layer 2</td>
<td>Access Endpoints MAC address</td>
<td>802.3 MAC</td>
</tr>
<tr>
<td>Physical</td>
<td>Layer 1</td>
<td>Specifies voltage, pin-outs, cable</td>
<td>TIA -568-B</td>
</tr>
</tbody>
</table>

Similar sounding network services exist at Layer 2 (L2) and Layer 3 (L3) – e.g. QoS, Resiliency, Security
Layer 1 - Physical

- Design and implement a robust physical layer
- Environment Classification - MICE
- More than cable
  - Patch panels
  - Cable management
  - Grounding & Bonding (noise mitigation)
- Physical Media
  - Wired vs. Wireless
  - Copper vs. Fiber
  - UTP vs. STP
  - Singlemode vs. Multimode
Layer 2 – Data Link Switching

- Uses the Data Link layer to determine where the frame goes
- Looks at the **MAC** address (**Media Access Control**)
- All ports are in the same broadcast domain
- Managed switches provide Layer 2 features, such as segmentation (VLAN tag), security, QoS, resiliency, etc.

<table>
<thead>
<tr>
<th>MAC Port Address Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXX1</td>
</tr>
<tr>
<td>XXX2</td>
</tr>
<tr>
<td>XXX3</td>
</tr>
</tbody>
</table>
Layer 3 – Network Routing

- Connect different LANs
- Extend network distance
  - LAN, MAN, WAN
- Switch/route packets by IP Address
- Broadcast control
- Multicast control, EtherNet/IP multicast not routable - TTL=1
- Layer 3 features such as security, QoS, resiliency, etc
- Make sure IT understands required protocols
  - Is there a need to route to other subnets?
  - Multicast traffic?
  - Security or segmentation?
Layer 4 – Transport
UDP / TCP over IP

• User Datagram Protocol
  – Connectionless/best effort
  – Does not use acknowledgements
  – Unicast and Multicast IP
  – CIP – used for Class 1 (implicit) I/O and P/C connections

• Transmission Control Protocol
  – Connection-oriented, end-to-end reliable transmission
  – Utilizes acknowledgements (ACK) to ensure reliable delivery
  – Unicast IP
  – CIP – used for Class 3 (explicit) messaging such as Operator Interface

<table>
<thead>
<tr>
<th>Source Port Number</th>
<th>Destination Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length</td>
<td>Checksum</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

**UDP Header**

<table>
<thead>
<tr>
<th>Source Port Number</th>
<th>Destination Port Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sequence number</td>
<td></td>
</tr>
<tr>
<td>Acknowledgment number</td>
<td></td>
</tr>
<tr>
<td>Header Length</td>
<td>Reserved</td>
</tr>
<tr>
<td>Reserved</td>
<td>Checksum</td>
</tr>
<tr>
<td>Data</td>
<td></td>
</tr>
</tbody>
</table>

**TCP Header**
• Offers hierarchy modular topology - building blocks
• Easy to grow, understand and troubleshoot
• Creates small fault domains - clear demarcations and isolation
• Promotes load balancing and redundancy
• Promotes deterministic traffic patterns
• Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
• Utilizes Layer 3 routing for load balancing, fast convergence, scalability and control
Converged Plantwide Ethernet Architectures (CPwE)

- Logical framework
- Industrial and IT network convergence
- Hierarchical segmentation
  - Scalability
  - Resiliency
  - Traffic management
  - Policy enforcement
- Security policies
  - Defense in depth
- Secure remote access
CPwE Design Guide 2.0 vs. 1.2

- Application Centric vs. Network Centric
- Stratix 8000 vs. 2955
- Resiliency
  - MSTP/rPVST+: Ring & Redundant Star
  - Flex Links: Redundant Star
  - EtherChannel: Redundant Star
- Screw-to-screw Application Performance
- Multicast Management
- Quality of Service
- Secure Remote Access
Examples of Customer Extremes

Innovation & Agility Challenges
- Duplication of efforts, prone to errors
- No remote access
- False sense of security

Convergence & Agility Challenges
- Traffic management
- Security

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
Networking Best Practices

Best practices for reducing Latency and Jitter, and to increase data Availability, Integrity and Confidentiality

• IP Multicast Control
  – IGMP Management

• Segmentation
  – Multi-tier Network Model
  – Topology
  – Virtual LANs (VLANs)

• Prioritization
  – Quality of Service (QoS)

• Resiliency Protocols and multi-path topologies

• Defense-in-Depth Security

W1: Build a Solid Plant-floor Infrastructure through Network and Security Design and Implementation

Time: 8:30 AM
Room: 213A
Unicast vs. Broadcast

One-to-one, individual transactions

One-to-all, single transaction
Multicast

One-to-many, single transaction
Multicast Protocols

- **IGMP** – Internet Group Management Protocol
- **IGMP snooping** is used to prevent multicast from flooding all ports on a VLAN. It does so by monitoring the Layer 3 IGMP packets
  - IGMP snooping becomes operational as soon as a **Querier** is detected
  - A Layer 2 access switch, such as the Stratix 8000, can act as an **IGMP querier**
  - If there are multiple queriers are on the local network, the one with the lowest IP address becomes the “querier.” Recommendation to select the acting querier by giving it the lowest IP on the VLAN.
- Make sure IT is aware of multicast requirements
- Stratix 8000, enabled by default
  - **IGMP v2**, Querier, Snooping, Reports
IP Multicast Group Concept

- The device must join a group in order to receive its data
- All members of a group receive the same data
- A device can send to a group without being a member of that group
IGMP Querier Positioning

Enable querier, one per VLAN interface, set as lowest IP address to ensure as default querier

IGMP Snooping and Querier enabled by default

Levels 0–2

Cell/Area #1
Redundant Star Topology
Flex Links Resiliency

Cell/Area #2
Ring Topology
Resilient Ethernet Protocol (REP)

Cell/Area #3
Bus/Star Topology

Cell/Area Zones

Controller

Layer 2 Access Switch

Catalyst 3750 StackWise Switch Stack

Rockwell Automation Stratix 8000

HMI

Drive

Distributed I/O

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
Multicast Forwarding

• **Layer 2 - Switch focus**
  – Internet Group Management Protocol (IGMP)
    • Stratix 6000 & 8000
    • Example – Rockwell Automation EtherNet/IP Multicast, TTL=1

• **Layer 3 - Router focus**
  – Protocol Independent Multicast (PIM)
    • Dense mode – implicit, flood then prune
    • Sparse mode – explicit, join requests
      – Rendezvous points
    • Example - Precision Time Protocol (PTP) IEEE-1588, Grandmaster
IGMP Filtering Summary

• In a producer-consumer model traffic grows exponentially with the number of hosts unless multicasts are constrained
• IGMP filtering limits the amount of multicast traffic to only valid consumers
• All consumers have equal access to data
IP Multicast Review
Multicast Addresses

- IP multicast uses the Class D range of IP addresses, from 224.0.0.0 through 239.255.255.255.

- Within this range, several addresses are reserved by the Internet Assigned Numbers Authority (IANA):
  - 224.0.0.0 through 224.0.0.255 – Used by network protocols, only in a local segment
  - 239.0.0.0 through 239.255.255.255 - Used in private domains and not routed between domains

The IANA maintains a list of Multicast addresses at:
http://www.iana.org/assignments/multicast-addresses
Multicast Management
Design and Implementation Considerations

• Implement IGMP Querier and Snooping, on a per VLAN basis, to restrict forwarding of multicast traffic
• Stratix 8000 – Querier and Snooping enabled by default
• Implement IGMP default Querier higher and centrally within the network architecture such as at the Layer 3 Distribution switch
• If there are multiple queriers within a VLAN, the one with the lowest IP address becomes the “querier.”
• Make sure IT is aware of Multicast requirements
Network Segmentation
Virtual Local Area Networks (VLANs)

- Assign VLAN’s to devices when traffic patterns are known
- VLANs: Group assets by type, role, logical area, physical area or a hybrid of these
- Limit the flow of traffic to only required devices (example: one VLAN per Cell/Area Zone)
- Use Layer 3 switch to route data between VLANs
- Use Layer 3 ACLs to restrict traffic between VLANs
- Consider Trunking, Routing, Asset placement in the context of degraded operations
Example of Using VLANs
Industrial Ethernet System

Production - VLANs
IP Security Camera - VLAN
Spanned VLAN (Application Specific)
VLAN Trunking

- **Trunking Methods**
  - IEEE 802.1Q, generally referred to as “dot1q” - Stratix 8000
  - Cisco Inter-Switch Link Protocol (ISL), no longer used
  - Dynamic Trunking Protocol (DTP), negotiate trunking method, no longer used

- **VLAN Trunking Protocol (VTP)**
  - Provides centralized VLAN management, runs only on trunks
  - Three modes:
    - Server: updates clients and servers
    - Client: receive updates—cannot make changes
    - Transparent: allow updates to pass through – Stratix 8000 default
  - Use VTP transparent mode to decrease potential for operational error. Define VLANs at each switch
Stratix VLAN capability

- **Stratix 6000**
  - Supports VLANs within a switch (local)

- **Stratix 8000**
  - Supports VLANs with trunking
    - Trunking – allows communications of like VLANs across multiple switches
  - Layer 3 switching (future)
    - Allows routing across VLANs and Subnets

Switch without Trunking Configured
VLAN 102 SW1 cannot talk to VLAN 102 SW2

Switch with Trunking Configured
VLAN 102 SW1 can talk to VLAN 102 SW2
VLAN Design and Implementation Considerations

- Design small Cell/Area zones, segment traffic types into VLANs and IP Subnets to better manage the traffic
- Segment traffic types via VLANs to manage network traffic and establish domains of trust
- Within Cell/Area Zone - Layer 2 VLAN trunking between switches for similar traffic types
- Within Cell/Area Zone – Layer 3 InterVLAN routing between different traffic types
- Between Zones - Layer 3 InterVLAN routing, minimize Layer 2 VLAN trunking
- When trunking, use 802.1Q, VTP in transparent mode
- Do not use VLAN 1 for EtherNet/IP Control & Information Traffic
- Create a Network Management VLAN, don’t use VLAN 1
## Not All Traffic is Created Equal
Prioritization is Required

<table>
<thead>
<tr>
<th></th>
<th>Control (e.g., CIP)</th>
<th>Video</th>
<th>Data (Best Effort)</th>
<th>Voice</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bandwidth</strong></td>
<td>Low to Moderate</td>
<td>Moderate to High</td>
<td>Moderate to High</td>
<td>Low to Moderate</td>
</tr>
<tr>
<td><strong>Random Drop Sensitivity</strong></td>
<td>High</td>
<td>Low</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td><strong>Latency Sensitivity</strong></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td><strong>Jitter Sensitivity</strong></td>
<td>High</td>
<td>High</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>

Control Networks **Must** Prioritize Control Traffic over Other Traffic Types to Ensure Deterministic Data Flows with Low Latency and Low Jitter
Quality of Service (QoS)
Reduce Latency and Jitter

- QoS prioritizes traffic into different service levels
- Provides preferential forwarding treatment to some data traffic, at the expense of others
- Allows for predictable service for different applications and traffic types
Quality of Service
Ethernet Switch

- Layer 2 … Class of Service (CoS) … 802.1Q/p
- Layer 3 … type of service (ToS) … DiffServ Code Point (DSCP)
- ODVA EtherNet/IP QoS Specification
## Quality of Service Operations

<table>
<thead>
<tr>
<th>Classification and Marking</th>
<th>Queuing and (Selective) Dropping</th>
<th>Post-Queuing Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Classification Tools
Ethernet 802.1Q Class of Service

- 802.1p user priority field also called Class of Service (CoS)
- Different types of traffic are assigned different CoS values
- CoS 6 and 7 are reserved for network use

CoS | Application
---|---
7 | Reserved
6 | Routing
5 | Voice
4 | Video
3 | Call Signaling
2 | Critical Data
1 | Bulk Data
0 | Best Effort Data
Classification Tools
IP Precedence and DiffServ Code Points

IPv4: three most significant bits of Type of Service (ToS) byte are called IP Precedence (IPP)—other bits unused

DiffServ: six most significant bits of ToS byte are called DiffServ Code Point (DSCP)—remaining two bits used for flow control

DSCP is backward-compatible with IP precedence
Cell/Area Zone QoS

Typical Enterprise QoS

- Output Queue 1: Voice
- Output Queue 2: Call Signaling
- Output Queue 3: Network Control
- Output Queue 4: Video
- Bulk Data
- Best Effort
- Scavenger

Cell/Area Zone QoS

- Output Queue 1: PTP-Event (59)
- Output Queue 2: CIP Motion
- Output Queue 3: PTP Management, Safety I/O & I/O
- Output Queue 4: CIP Explicit Messaging
- Call Signaling
- Video
- Critical Data
- Bulk Data
- Best Effort
- Scavenger

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
QoS Design Considerations

- **Goals**
  - Highest traffic priority for latency and jitter sensitive CIP I/O traffic
  - Guaranteed delivery for CIP sync, CIP motion
  - Minimize impacts by DDoS attacks

- **QoS throughout industrial network**

- **With ODVA update, QoS trust boundary moves from switch access ports to QoS-capable CIP device**

- **For existing CIP devices, marking at the access port is based on port number**
  - CIP I/O UDP 2222
  - CIP Explicit TCP 44818

- **Egress scheduling with four queues**
  - First priority: CIP sync, CIP motion
  - Second priority: CIP I/O
  - Third priority: CIP explicit
  - Default: others
ODVA has specified QoS markings for CIP and PTP traffic

- Smartport Macros in switch applies markings for legacy devices
- Switch initial configuration sets up the policing, queuing and scheduling

<table>
<thead>
<tr>
<th>Traffic Type</th>
<th>CIP Priority</th>
<th>DSCP</th>
<th>CoS Priority*</th>
<th>CIP Traffic Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>PTP event (IEEE 1588)</td>
<td>n/a</td>
<td>59</td>
<td>7</td>
<td>PTP event messages, used by CIP Sync</td>
</tr>
<tr>
<td>PTP management (IEEE 1588)</td>
<td>n/a</td>
<td>47</td>
<td>5</td>
<td>PTP management messages, used by CIP Sync</td>
</tr>
<tr>
<td>CIP class 0 / 1</td>
<td>Urgent (3)</td>
<td>55</td>
<td>6</td>
<td>CIP Motion</td>
</tr>
<tr>
<td></td>
<td>Scheduled (2)</td>
<td>47</td>
<td>5</td>
<td>Safety I/O</td>
</tr>
<tr>
<td></td>
<td>High (1)</td>
<td>43</td>
<td>4</td>
<td>I/O</td>
</tr>
<tr>
<td></td>
<td>Low (0)</td>
<td>39</td>
<td>0</td>
<td>Open</td>
</tr>
<tr>
<td>CIP UCMM CIP class 3</td>
<td>All</td>
<td>35</td>
<td>n/a</td>
<td>CIP messaging</td>
</tr>
</tbody>
</table>

- disabled by default
• Express Setup creates the QoS service policy within the Stratix 8000, but does not apply QoS to the switch interfaces. The “Automation Device with QoS” Smartport enables QoS on that port.

• The Stratix 8000 recognizes or ‘trusts’ QoS capable devices and prioritizes CIP traffic as it exits from the switch.

• Quality of Service does not increase bandwidth. QoS gives preferential treatment to some network traffic at the expense of others.

• Deploy QoS consistently throughout industrial network.
Redundant Paths and Loop Avoidance

Why is this important?

- Ring and Redundant Star topologies require a resiliency protocol to provide redundant network paths while preventing loops.
### Reliability, Availability & Network Segmentation

#### Cell/Area Zone Topology Options

<table>
<thead>
<tr>
<th></th>
<th>Redundant Star</th>
<th>Ring</th>
<th>Linear</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cabling Requirements</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>East of Configuration</strong></td>
<td>Redundant Star</td>
<td>Ring</td>
<td>Linear</td>
</tr>
<tr>
<td><strong>Implementation Costs</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Bandwidth</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Redundancy and Convergence</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Disruption During Network Upgrade</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Readiness for Network Convergence</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Overall in Network TCO and Performance</strong></td>
<td></td>
<td>Best</td>
<td>Worst</td>
</tr>
</tbody>
</table>

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
## Reliability, Availability & Network Segmentation

### Cell/Area Zone Topology Options

<table>
<thead>
<tr>
<th>Topology/Resiliency</th>
<th>Stratix 8000</th>
<th>Stratix 6000</th>
<th>Embedded 2-Port</th>
<th>Stratix 2000</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Redundant Star</strong></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(STP, EtherChannel, Flex Links)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ring</strong></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(STP, REP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Ring</strong></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(Device Level Ring - DLR)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Star</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>(None)</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td><strong>Linear</strong></td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>
Loop Avoidance

- A resiliency protocol is required to maintain parallel links for redundancy while avoiding loops.
- A redundant connection (loop) stifles a Layer 2 bridged network.
  - Layer 2 packets do not have a time-to-live (TTL).
  - A single packet can consume all the bandwidth in a broadcast storm.
Network Resiliency Protocols

- **Layer 2**
  - Automation Devices
    - Device Level Ring (DLR) – IEC & ODVA
  - Switches
    - Spanning Tree Protocol (STP), Rapid STP (RSTP), Multiple instance STP (MSTP) – IEEE
      - Stratix 8000 – MSTP - default
      - Rapid Per VLAN Spanning Tree Plus (RPVST+) – Cisco Technology
    - Resilient Ethernet Protocol (REP) – Cisco Technology
    - EtherChannel - 802.3ad LACP (port aggregation) – IEEE
    - Flex Links – Cisco Technology

- **Layer 3**
  - StackWise (3750), stack management – Cisco Technology
  - Hot Standby Router Protocol (HSRP) – Cisco Technology
  - Virtual Router Redundancy Protocol (VRRP) – IETF RFC 3768
  - Gateway Load Balancing Protocol (GLBP) – Cisco Technology

- **Layer 2 vs. Layer 3 Resiliency**
  - Layer 3 has maintainability advantages
  - Layer 2 has performance advantages
Spanning Tree Protocol

- Only standard protocol for network resiliency - IEEE 802.1D
- Redundant Star and Ring Topology
- Provides alternate path in case of failures, avoiding loops
- Unmanaged switches don’t support STP
- STP, RSTP, MSTP & RPVST+
- Differences
- Coordinate with IT before implementing

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
EtherChannel

- Link Aggregation Control Protocol (LACP) port aggregation – IEEE 802.3ad
- Redundant Star Topology
- A way of combining several physical links between switches into one logical connection to aggregate bandwidth (2 to 8 ports)
- Provides resiliency between connected switches if a connection is broken
Flex Links

- Cisco Technology
- Redundant Star Topology
- Active/Standby Port Scheme
- Provides alternate path in case of failures, avoiding loops
- Unmanaged switches don’t support this concept
- Coordinate with IT before implementing
Resilient Ethernet Protocol
Segment Protocol

• REP operates on chain of bridges called segments
• A port is assigned to a unique segment
• A segment can have up to two ports on a given bridge
Resilient Ethernet Protocol

Blocked Port

- When all links are operational, a unique port blocks the traffic on the segment
- If any failure occurs within the segment, the blocked port goes forwarding
Resilient Ethernet Protocol
Redundant Link

- Segments can be wrapped into a ring
- Can be seen as a redundant link in that case
- Note: Identification of edge ports requires additional configuration in that case
Resilient Ethernet Protocol

Summary

• REP is a segment concept
  – A segment is a chain of bridges
  – If all the links are available, REP blocks
  – If there is a failure, REP unblocks

• Redundant networks can be built with REP segments

• Support for flexible topologies - supports both closed and open rings in various topologies, but requires manual configuration

• Ring recovery time is less than 70 ms for fiber implementations

• Cisco innovation, included with Stratix 8000
Device Level Ring
Normal Operation

• Supervisor blocks traffic on one port
• Sends Beacon frames on both ports to detect break in the ring
• Sends Announce frames on unblocked port
Device Level Ring
Physical Layer Failure

- All faults that are detectable at physical layer
- Physical layer failure detected by protocol-aware node
- Status message sent by ring node and received by ring supervisor
Device Level Ring Convergence

- After failure detection, ring supervisor unblocks blocked port
- Network configuration is now a linear topology
- Fault location is readily available via diagnostics
- Once ring is restored, supervisor hears beacon on both ports, and transitions to normal ring mode, blocking one port
Device Level Ring
Summary

• Open standard (ODVA) allows 3rd party suppliers to develop compatible products
• Network traffic is managed to ensure timely delivery of critical data (Quality of Service, IEEE-1588 Precision Time Protocol, Multicast Management)
• Designed for 1 ms convergence for simple automation device networks
• Support for ring and linear topologies, fiber and copper implementations
First Hop (Layer 3) 
Resiliency Protocols

- Distribution switches typically provide first hop (default gateway) redundancy
  - StackWise (3750), stack management
  - Hot Standby Router Protocol (HSRP)
  - Virtual Router Redundancy Protocol (VRRP)
  - Gateway Load Balancing Protocol (GLBP)
• Fiber vs. Copper
• MSTP/rPVST+ - CIP Explicit Messaging such as HMI, or 100 ms CIP Implicit I/O RPI applications
• Flex Links or EtherChannel for Redundant Star - CIP Implicit I/O
• REP or DLR for Ring CIP Implicit I/O
Representative Configurations

Enterprise Zone

DMZ
- Patch Management
- Terminal Services
- Application Mirror
- AV Server

Manufacturing Zone
- FactoryTalk
- Applications
- and Services

Cell/Area Zone #1
- Embedded Layer 2 Switch
- Ring Topology

Cell/Area Zone #2
- Embedded Layer 2 Switch
- Linear Topology

Cell/Area Zone #3
- Ring Topology

Cell/Area Zone #4
- Linear Topology

ERP, Email, Wide Area Network (WAN)

Network Enterprise

Cisco 2960
Layer 2 Access Switch

Cisco 3750G
Stackwise Layer 3 Distribution Switch

Cisco Adaptive Security Appliance (ASA) 5520 Firewall

Cisco 4402
Wireless LAN Controller (WLC)

Cisco 1252G
802.11n – Dual Band Access point

Cisco 4402
Wireless LAN Controller (WLC)

Stratix 8000
Rockwell Automation
IE Managed
Layer 2 Switch

Lightweight AP
(LWAP)

Mobile User

AP as Workgroup Bridge (WGB)
Topology and Resiliency
Design and Implementation Considerations

• Balance of path redundancy with loop avoidance
• Ring and Redundant Star topology requires a resiliency protocol
• Topology and Resiliency Protocol choice is application dependant
  – Mixed switch vendor environment
    • Legacy Migration
  – Switch vs. Device
  – Geographic dispersion
  – Location within the hierarchal architecture - Layer 2 vs. Layer 3
  – Performance
    • Convergence time
    • Packet loss
    • Latency & Jitter Tolerance
Understanding Your Switch Options

- Industrial versus commercial
- Managed versus unmanaged

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Managed Switches</th>
<th>Disadvantage</th>
<th>Managed Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to manage multicast traffic</td>
<td>• Provide diagnostics data</td>
<td>• More expensive</td>
<td>• Requires some level of support and configuration to start up</td>
</tr>
<tr>
<td>Provide security options</td>
<td>• Provide QoS &amp; VLAN services</td>
<td>• No management capabilities</td>
<td>• No security</td>
</tr>
<tr>
<td>Network resiliency support</td>
<td></td>
<td>• No diagnostic information provided</td>
<td>• Difficult to troubleshoot</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Unmanaged Switches</th>
<th>Disadvantage</th>
<th>Unmanaged Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inexpensive</td>
<td>• Simple to set up</td>
<td>• No resiliency support</td>
<td></td>
</tr>
</tbody>
</table>
Rockwell Automation Stratix 8000/8300

Best of Cisco
• Secure integration with enterprise network
  Cisco internetworking operating system (IOS™)
  Cisco Catalyst™ switch architecture and feature set
  Familiar tools for IT professionals: command line interface (CLI), Cisco Network Assistant (CNA) and Device Manager

Best of Rockwell Automation
• Premier (CIP) interface to Integrated Architecture
  Integrated Architecture premier integration
  RSLogix 5000 for configuration … Add-on Profile (AOP)
  Predefined Logix tags for diagnostics
  FactoryTalk View Faceplates

Best for the Plant Floor Environment
• Easy to Integrate and Maintain
  Default configurations for Industrial Automation market (Global macros and Smartports)
  Removable Compact Flash for one step device replacement
Cultural Convergence
Common Tools

- Device Manager
- Command Line Interface
- Cisco Network Assistant
- FactoryTalk View, Faceplates
- RSLogix 5000, Add-on Profile
## IP Addressing Management

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static</td>
<td>All devices hard coded with an IP Address</td>
<td>Simple to commission and replace</td>
<td>In large environments, can be burdensome to maintain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Limited ranged of IP addresses and subnet</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Not all devices support</td>
</tr>
<tr>
<td>Static via BOOTP Configuration</td>
<td>Server assigns devices IP addresses</td>
<td>Supported by every device</td>
<td>Requires technician to configure IP address/Mac address when a device is replaced</td>
</tr>
<tr>
<td></td>
<td>Precursor to DHCP</td>
<td></td>
<td>Adds complexity and point of failure</td>
</tr>
<tr>
<td>DHCP</td>
<td>Server assigns IP addresses from a pool (NOT RECOMMENDED for Cell/Area devices)</td>
<td>Efficient use of IP address range</td>
<td>More complex to implement and adds a point of failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can reduce administration work load</td>
<td>Devices get different IP addresses when they reboot</td>
</tr>
<tr>
<td>DHCP Option 82</td>
<td>Server assigns consistent IP addresses from a pool (NOT RECOMMENDED)</td>
<td>Efficient use of IP Address range</td>
<td>More complex to implement and adds a point of failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can reduce administration work load</td>
<td>Mixed environments may not work</td>
</tr>
<tr>
<td>DHCP port-based allocation</td>
<td>Automatically assign IP address per physical switch port</td>
<td>Efficient use of IP Address range</td>
<td>Cisco/Rockwell Automation only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Eases commissioning and maintenance in large environments</td>
<td>Requires some maintenance and upkeep, on a per switch basis</td>
</tr>
</tbody>
</table>
Maximize Plant Floor Uptime
Device Replacement

- EtherNet/IP device requests IP address upon power up
- DHCP per port - Assigns the consistent IP address to EtherNet/IP devices on a per port basis
- Network recovers from EtherNet/IP device replacement automatically

Reduces MTTR and Increases Machine OEE
EtherNet/IP Network Infrastructure
Design and Implementation Considerations

• Use managed switches
  – Consistent network service implementation
• Use the right tools for your function
  – Industrial vs. IT
• Use static or per port IP address assignments
• Use Fiber (SFP) Gigabit Ethernet ports for trunks/uplinks
Manufacturing Zone
Level 3

FactoryTalk Application Servers
- View
- Historian
- AssetCentre
- Transaction Manager

FactoryTalk Services
Platform
- Directory
- Security/Audit

Data Servers

Network Services
DNS, DHCP, syslog server
Network and security management

Cisco Catalyst 6500/4500
Layer 3 Router
Cisco Catalyst 3750 StackWise

Layer 3 Switch Stack

Manufacturing Zone - Core
Manufacturing Zone - Distribution
Site Manufacturing Operations and Control
RSLinx & Layer 3 Devices

- **RSLinx Classic and Enterprise**
  - Local subnet
  - Autobrowse (broadcast)
  - AB-ETHIP Driver
  - Manual Configuration AB_ETH Driver

- **RSLinx Classic Autobrowse through a Layer 3 Device**
  - Enable IP Directed Broadcast on Cisco Layer 3 Device (disabled by default)
  - `ip directed-broadcast [access-list-number]` … CLI command

- **RSLinx Enterprise**
  - No support for IP Directed Broadcast, must manually configure
Manufacturing Zone
Medium

ERP, Email, Wide Area Network (WAN)

Patch Management
Terminal Services
Application Mirror
AV Server

Enterprise Zone
Levels 4 and 5
Demilitarized Zone (DMZ)

Demilitarized Zone (DMZ)
Manufacturing Zone
Site Manufacturing Operations and Control Level 3

Network Services
- DNS, DHCP, syslog server
- Network and security mgmt

Controller
Drive
HMI
DIO

Cell/Area #1
Redundant Star Topology
Flex Links Resiliency

Cell/Area #2
Ring Topology
Resilient Ethernet Protocol (REP)

Cell/Area #3
Bus/Star Topology

Rockwell Automation
Stratix 8000
Layer 2 Access Switch

Remote Access Server

Cisco ASA 5500

Firewall (Active)
Cisco ASA 5500

Firewall (Standby)

Firewall (Active)

Demilitarized Zone (DMZ)

Levels 0–2

Cell/Area Zones

Controller

Drive
HMI
DIO

Controller

Drive
HMI
DIO

Controller

Drive
HMI
DIO

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
Manufacturing Zone
Design and Implementation Considerations

• Replicate critical services in the Manufacturing Zone
  – Production software such as FactoryTalk
  – Network services such as Active Directory

• Availability: apply redundant network routers/switches and links to maintain overall network availability

• Scalability: small sites use combined core and distribution switches, larger or growing sites should separate to avoid oversubscription on uplinks
Network Convergence
Security – A Concern Everyone Must Address

- Downtime – production control systems
- Lost data – manufacturing, scheduling, tracking and quality
- Theft of intellectual property
- Physical incident
  - Minor personal injury to loss of life
  - Loss of physical assets
- Loss time to market or the loss of public confidence

The potential of risks to manufacturing can be devastating
## Cultural and Organizational Convergence

### Security Policies

<table>
<thead>
<tr>
<th></th>
<th>IT Network</th>
<th>Industrial Network</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Focus</strong></td>
<td>Protecting Intellectual Property and Company Assets</td>
<td>24/7 Operations, High OEE</td>
</tr>
<tr>
<td><strong>Priorities</strong></td>
<td>Confidentiality</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>Integrity</td>
<td>Integrity</td>
</tr>
<tr>
<td></td>
<td>Availability</td>
<td>Confidentiality</td>
</tr>
<tr>
<td><strong>Types of Data Traffic</strong></td>
<td>Converged Network of Data, Voice and Video</td>
<td>Converged Network of Data, Control, Information, Safety and Motion</td>
</tr>
<tr>
<td><strong>Access Control</strong></td>
<td>Strict Network Authentication and Access Policies</td>
<td>Strict Physical Access</td>
</tr>
<tr>
<td></td>
<td>Simple Network Device Access</td>
<td>Simple Network Device Access</td>
</tr>
<tr>
<td><strong>Implications of a Device Failure</strong></td>
<td>Continues to Operate</td>
<td>Could Stop Operation</td>
</tr>
<tr>
<td><strong>Threat Protection</strong></td>
<td>Shut Down Access to Detected Threat</td>
<td>Potentially Keep Operating with a Detected Threat</td>
</tr>
<tr>
<td><strong>Upgrades</strong></td>
<td>ASAP During Uptime</td>
<td>Scheduled During Downtime</td>
</tr>
</tbody>
</table>

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.
Common Industrial Protocol (CIP)

- Open standard to integrate I/O control, device configuration and data collection
- Security stance
  - Protect the network
  - Defend the edge

ODVA [http://www.odva.org](http://www.odva.org)
Network Security Design
Protection of Assets and Intellectual Property

- Policy - plan of action with procedures to protect company assets
- Security policies are unique from company to company, although there are some common attributes and methodology to developing
- Defense in depth approach
- Procedural, physical and electronic measures
- Assessment: current risk, acceptable risk and risk mitigation techniques
- Manufacturing security policy, unique from and in addition to enterprise security policy
- Secure Remote Access requires a defense in depth approach
Industrial and IT Convergence
Network Security Design

- Comprehensive Network Security Model for Defense in Depth
- Security is **not** a bolt-on component
- Manufacturing Security Policy
- Implement DMZ
- Engage the Network & Security Services team
- Remote/Partner Access Policy, with robust & secure implementation

**Network Security Services Must Not Compromise Operations of the Cell/Area Zone**
Security
Design and Implementation Considerations

• Industrial Control System Security Standards
  – DHS External Report # INL/EXT-06-11478
  – NIST 800-82
  – ISA-99
• Establish an open dialog between Manufacturing and IT
• Defense-in Depth: no single methodology nor technology fully secures industrial networks
• Manufacturing security policy, unique from enterprise security policy
• Establish a DMZ between the Enterprise and Manufacturing Zones
• Deploy a methodology and/or procedure to buffer production data to and from the Enterprise Zone in the event DMZ connectivity is disrupted
• Work with Rockwell Automation Network and Security Services team
Where to Find More Information

• Website
  – http://www.ab.com/networks/architectures.html

• Design guides
  – Rockwell Automation and Cisco – Converged Plantwide Ethernet - DIG 2.0
  – ODVA - Network Infrastructure for EtherNet/IP: Introduction and Considerations
  – ODVA - EtherNet/IP Media Planning and Installation Manual

• Education series

• Whitepapers
  – Securing Manufacturing Computer and Controller Assets
  – Production Software within Manufacturing Reference Architectures
  – Achieving Secure Remote Access to Plant Floor Applications and Data
Education Series Webcasts

- The Trend - Network Technology and Cultural Convergence
- What every IT professional should know about Plant Floor Networking
- What every Plant Floor Controls Engineer should know about working with IT
- Industrial Ethernet: Introduction to Resiliency
- Fundamentals of Secure Remote Access for Plant Floor Applications and Data
- Securing Architectures and Applications for Network Convergence
- Available Online
  - http://www.ab.com/networks/architectures.html
Summary
Converged Plantwide Ethernet Architectures

• Establish an open dialog between Manufacturing and IT
• Understand your network protocols/devices, IP addressing, VLANs, QoS, Security
• Defense-in-Depth Security: no single methodology nor technology fully secures industrial networks
• Utilize standards, reference models and reference architectures
  – Foundation for success when deploying the latest, innovative technologies
  – Documented - less trial and error – reduced equipment costs and commissioning time – risk mitigation
  – Robust and secure network infrastructure providing low latency & jitter delivery and high availability
Thank you for participating!

Questions

Please tidy up your area before leaving.

http://www.ab.com/networks/architectures.html
Rockwell Automation and Cisco Alliance

**Common Technology View**
Support use of open, unmodified standards, with intelligent networking features in industrial networks through ODVA, ISA and others

**Collaborating on Reference Architectures**
Tested and validated design and implementation guidance and best practices for a converged Industrial/IT network architecture

**People and Process Optimization**
Develop process guidelines for help with convergence, facilitate training and dialogue with IT and Control System Engineers

**Product Collaboration**
Developed industrial Ethernet switch incorporating the best of Cisco and the best of Rockwell Automation
Converged Plantwide Ethernet Architectures (CPwE)

- Manufacturing focused Reference Architectures
- Common reference and common language for IT and manufacturing
- A set of tested and validated design and implementation best practices (Cisco Validated Design - CVD)
- Education Series

“With this implementation guide, for the first time IT and manufacturing professionals can share a common document for planning a converged IP network including the factory floor and automation equipment.”

– Harry Forbes, ARC Advisory Group
CPwE - A Set of Manufacturing Focused Reference Architectures

- These resources, 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.

- Converged Plantwide Ethernet Architectures provides education, design guidance, recommendations and best practices to help establish a robust and secure network infrastructure for manufacturing assets.
CPwE Overview

System-level validated Reference Architectures for Industrial Networks

Converged Plantwide Ethernet
- Built on standards
- Enables Secure Remote Access
- Plant specific Design & Implementation Guidance

Industrial Ethernet Switches
- CIP Integration via native EtherNet/IP support
- Enhanced Ease of Use

Ethernet-to-the-Factory
- Framework
- Network Architecture
- Security Architecture

Integrated Architecture
- FactoryTalk Platform
- Logix Control Platform
- Industrial Infrastructure

Future enabled Innovation Platform
- Extensive System-level validation testing
- United IT & Industrial expertise

© 2009 Cisco Systems, Inc. and Rockwell Automation, Inc. All rights reserved.