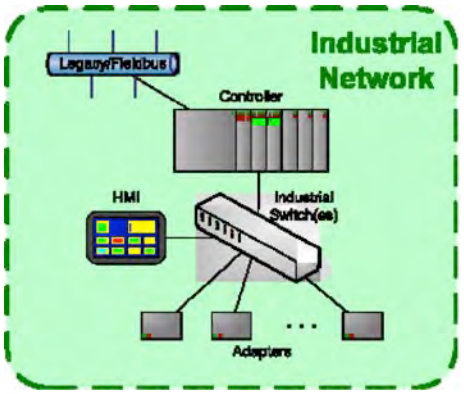
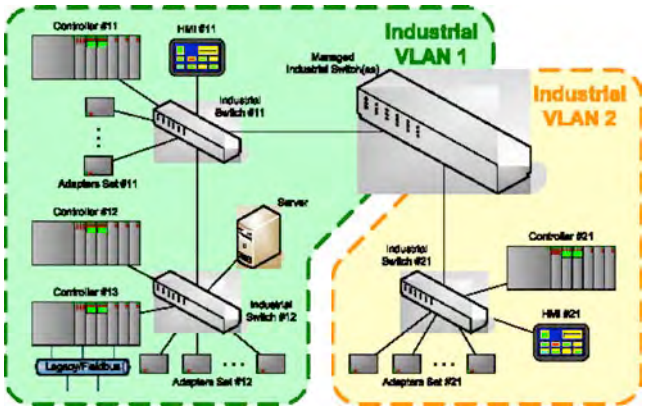
Reference Architectures for Industrial Automation and Control systems

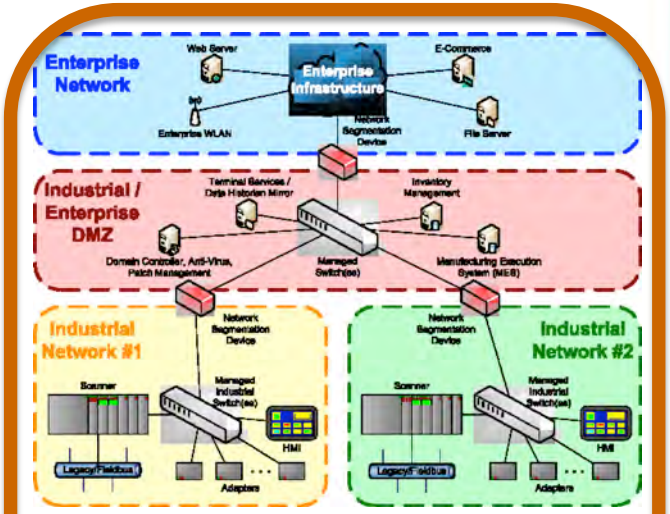
Paul Didier, Cisco Systems

Technical Track

Control Network types







Isolated Single Controller

- Single Controller
- 10s of devices
- Potentially multiple switches
- Limited non-CIP traffic
- Sharing data via sneaker net or transferable device

Isolated Multiple Controller

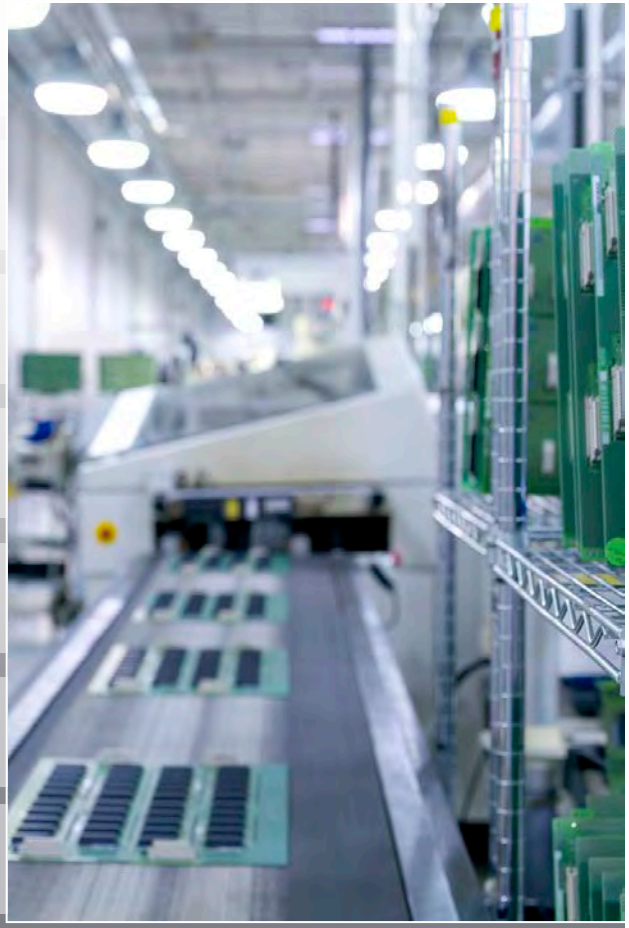
- Multiple Controllers
- Up to 100s of devices
- 10s of switches, maybe a router
- A few networks
- Potentially multiple switches
- Controllers sharing data
- Some non-CIP traffic (e.g. HTTP, file sharing, etc.)

Enterprise Connected

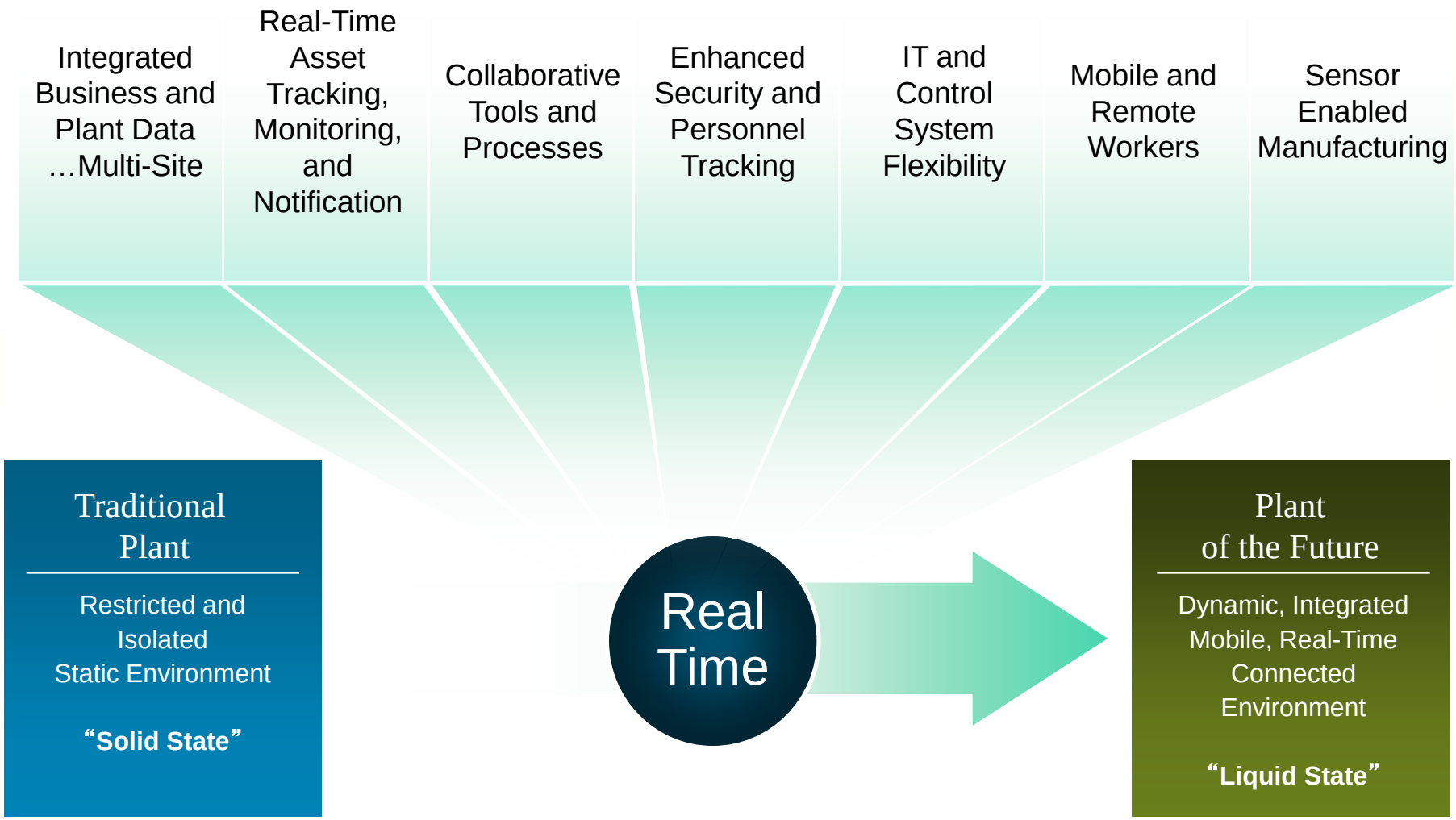
- Many Controllers
- Up to 1000s of devices
- Lots of switches and routers and other network infrastructure
- Many “networks”
- Sharing data, applications and services between Enterprise and Plant networks
- Could have lots of non-CIP traffic (e.g. Voice, Video, etc.)

Agenda

- Benefits of Reference Architecture
- Overview
- Topology and Resilience
- Multicast Management and IGMP
- Prioritization and QoS
- Routing & Layer 3
- Security



Manufacturing 2.0:
Plant Operations Transformation



Source: AMR, Industry Week, Cisco Analysis

Manufacturing and IT Convergence

Creating Challenges and Opportunities

Wide Ethernet Deployment

Increasing Business Pressures

Technology Convergence

Network Convergence

Organizational Convergence

Cultural Convergence

Business Model Innovation

- Business Agility
- Competitive Advantage

Challenges with Manufacturing Convergence

Organizational Issues

- Misaligned objectives
- Support requirements
- Different models and language

Industrial Applications

- Industrial protocols and traffic patterns
- Hardened products
- Determinism, latency, etc.
- Motion control

Security

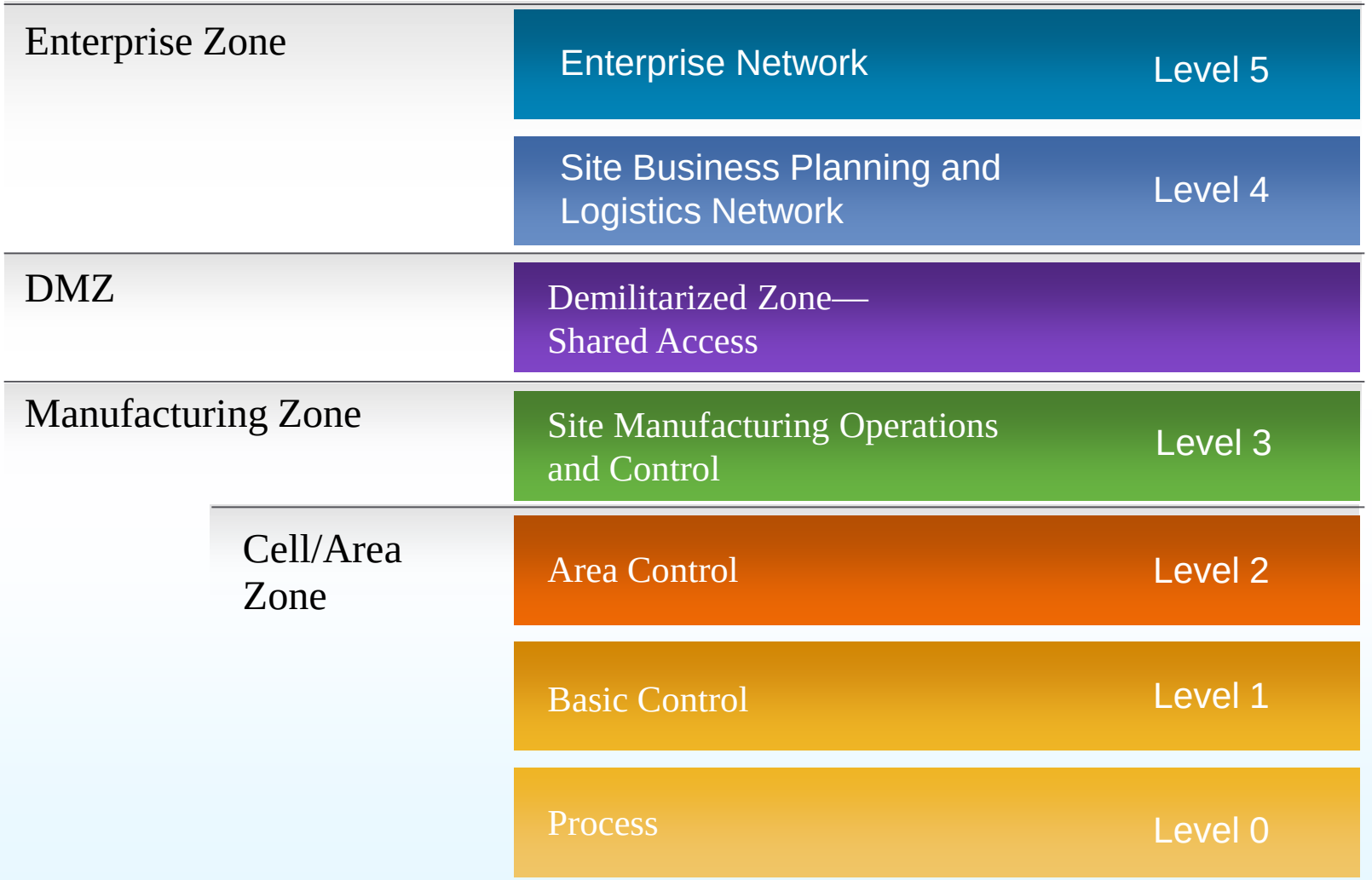
- Increased risk with COTS technology
- Patching issues
- Implications of issues
- Impact on performance & ease of use

MFG and IT Skill Alignment

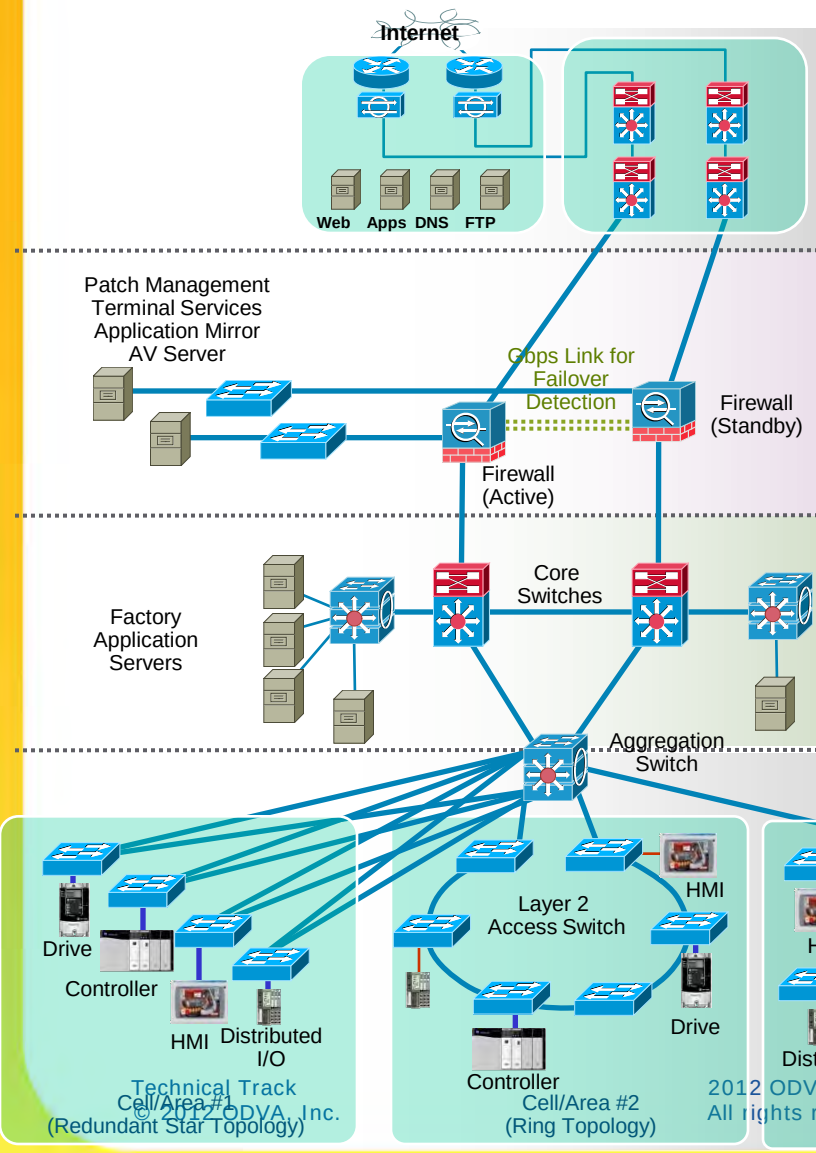
- Ease of use
- Multiple management tools
- Understanding of industrial applications

Logical Architecture

Built on Industry Standards



Converged Plantwide Ethernet Architecture



Enterprise Network
Levels 4–5

- Enterprise/IT Integration
- Collaboration
- Wireless
- Application Optimization

Demilitarized Zone
(DMZ) Firewalls

- Application and Data share
- Access Control
- Threat Protection

Manufacturing Zone
Level 3
Distribution and Core

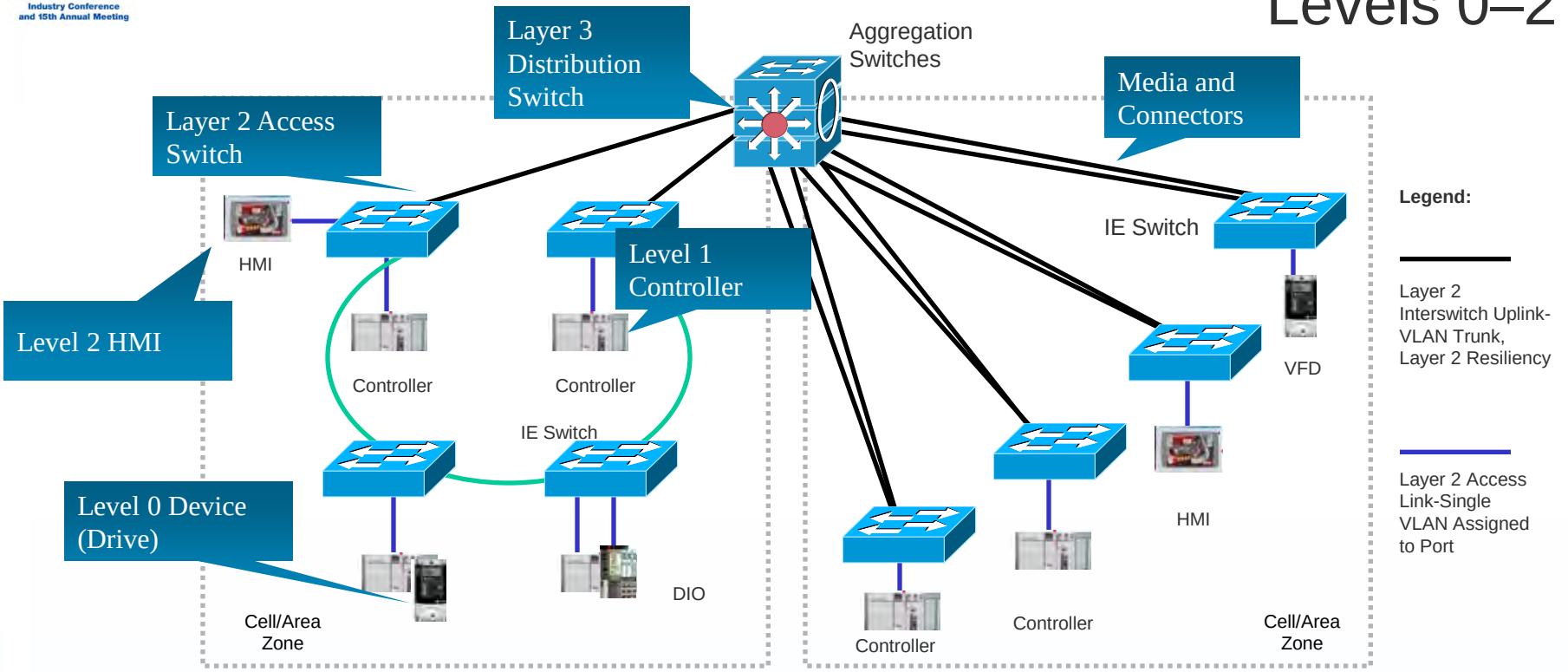
- Site Operations and Control
- Multi-Service Networks
- Network and Security Management
- Routing

Cell/Area Zone
Levels 0–2
Layer 2 Access

- EtherNet/IP (Industrial Protocols)
- Real–Time Control
- Fast Convergence
- Traffic Segmentation and Management
- Ease of Use

Cell/Area Zone Overview

Levels 0–2



The Cell/Area Zone Is a Layer 2 Network for a Functional Area of a Production Facility. Key Network Considerations Include:

- Environmental constraints
- Range of device intelligence
- Time-sensitive applications

Networking Best Practices – Cell/Area Zone

Best Practices For Reducing Latency and Jitter, and to Increase Data Availability, Integrity and Security

IP Multicast Control

- IGMP Management

Segmentation

- Virtual LANs (VLANs)

Prioritization

- Quality of Service (QoS)

Apply Resiliency Protocols and multi-path topologies

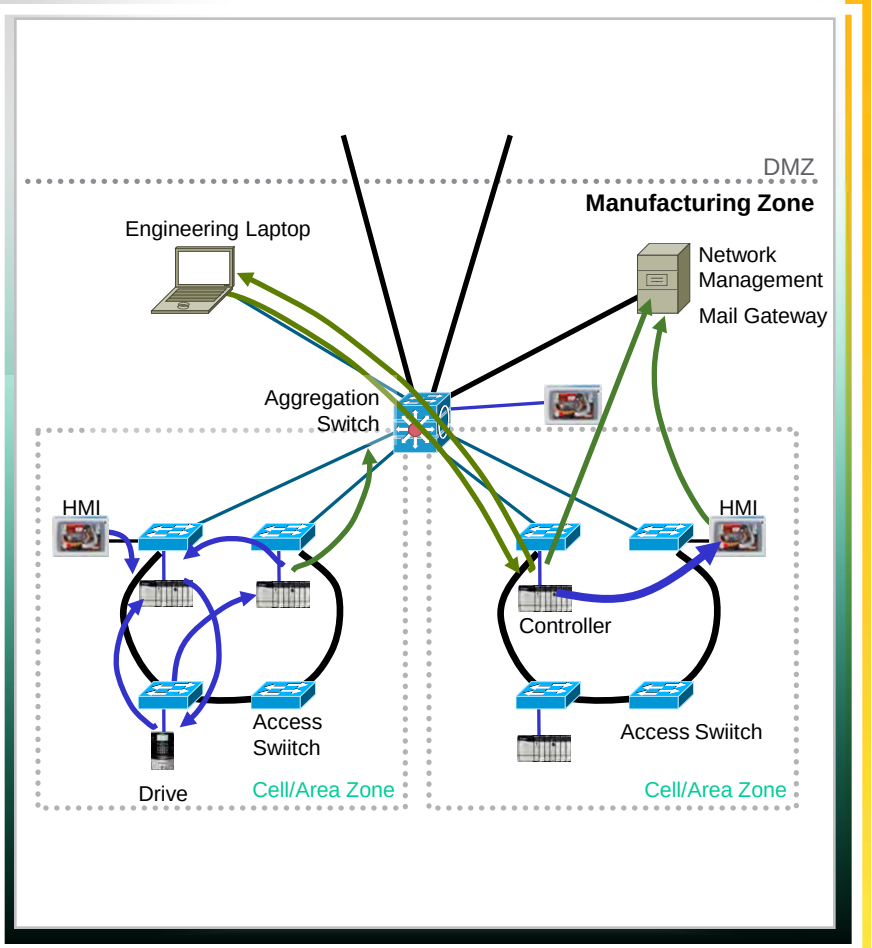
- Use Fiber-media uplinks for fast convergence

Defense-in-Depth Security

Cell/Area Traffic Flows

- Cell/area traffic is predominately (>80%) local, cyclical I/O (a.k.a. Implicit) traffic
  - Producers generated UDP multi-cast messages
  - Consumer generated UDP uni-cast messages
  - Packets are small: 100-200 Bytes, but communicated very frequently (every 0.5 to 10's of ms).
  - Typically un-routable (TTL=1 by application)

- The rest is informational control and administration (or Explicit) traffic flows intra- and inter-cell/area
  - CIP-based, non-critical administrative or data traffic
  - Diagnostic information via HTTP
  - Status and fault warnings via SNMP or SMTP
  - Packets are larger, ~500 bytes but infrequent (100s of ms)



Convergence Requirements

Requirement Class	Target Cycle Time	Target RPI	Target Network Convergence
Information/Process (e.g. HMI)	< 1 s	100 - 250 ms	< 1 sec
Time critical processes (e.g. I/O)	30 - 50 ms	20 ms	< 40 ms
Safety	10 - 30 ms	10 ms	< 15 ms
Motion	500 µs - 5ms	50 µs - 1 ms	< 1ms

Resiliency for Industrial Applications Supporting Multiple Topologies

Ring Convergence

- Resilient Ethernet Protocol (REP)
- Achieves ~50 ms convergence in large, complex networks

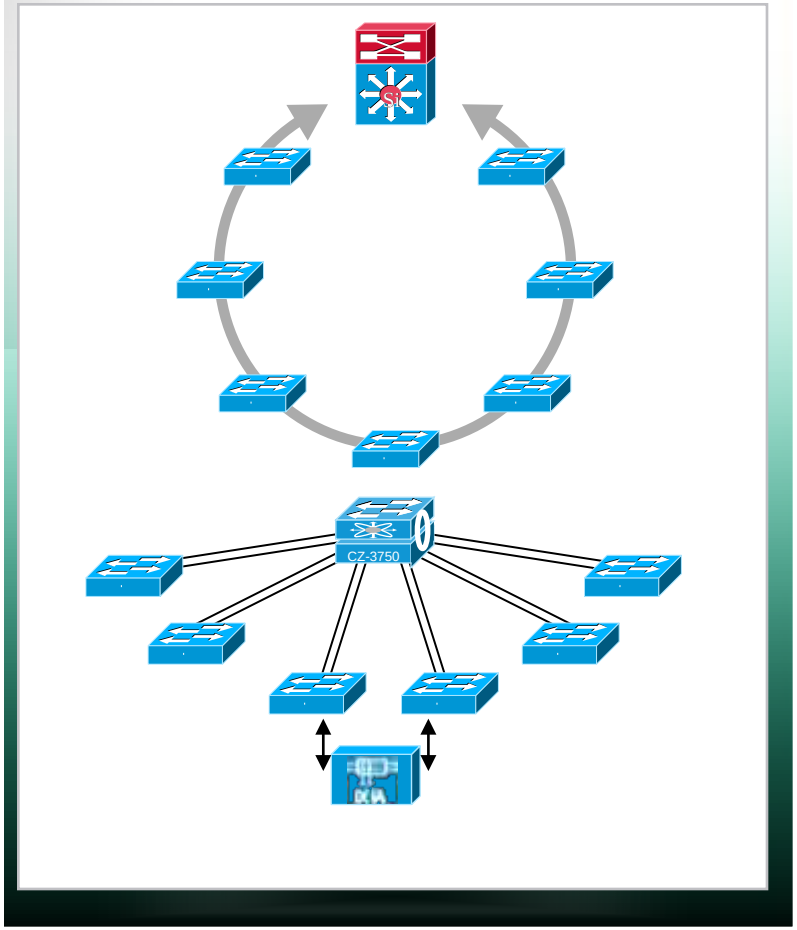
Redundant Star Convergence

- Multiple protocol options
- Convergence times of <100ms for Flexlinks and Etherchannel

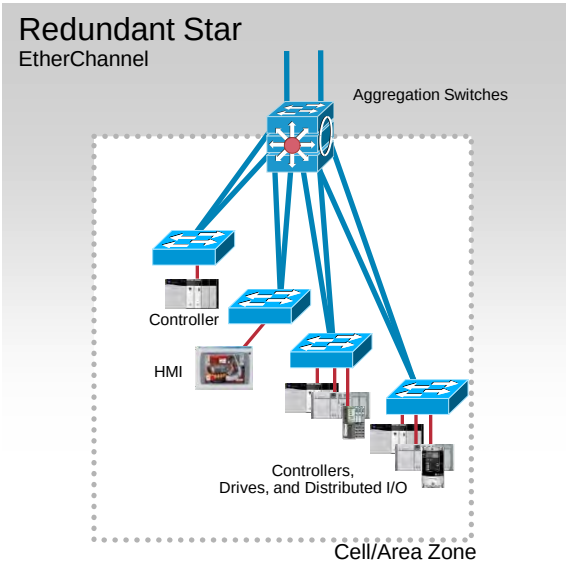
Tested with Rockwell applications and multicast traffic

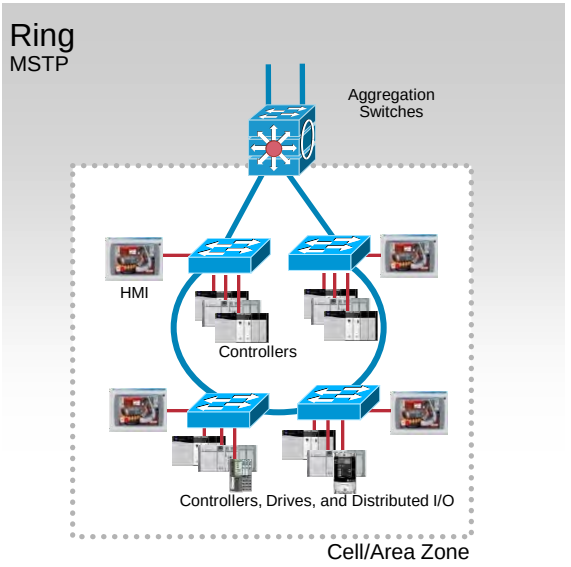
Fast convergence avoids application reset and improves uptime

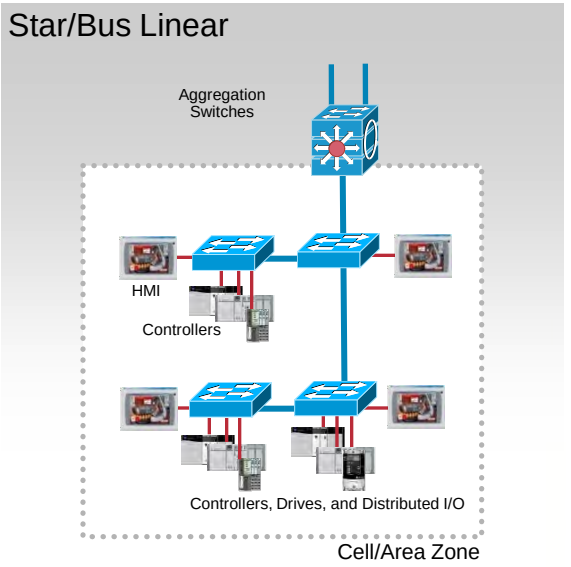
Critical for industrial applications



Reliability, Availability and Network Segmentation Cell/Area Zone Topology Options



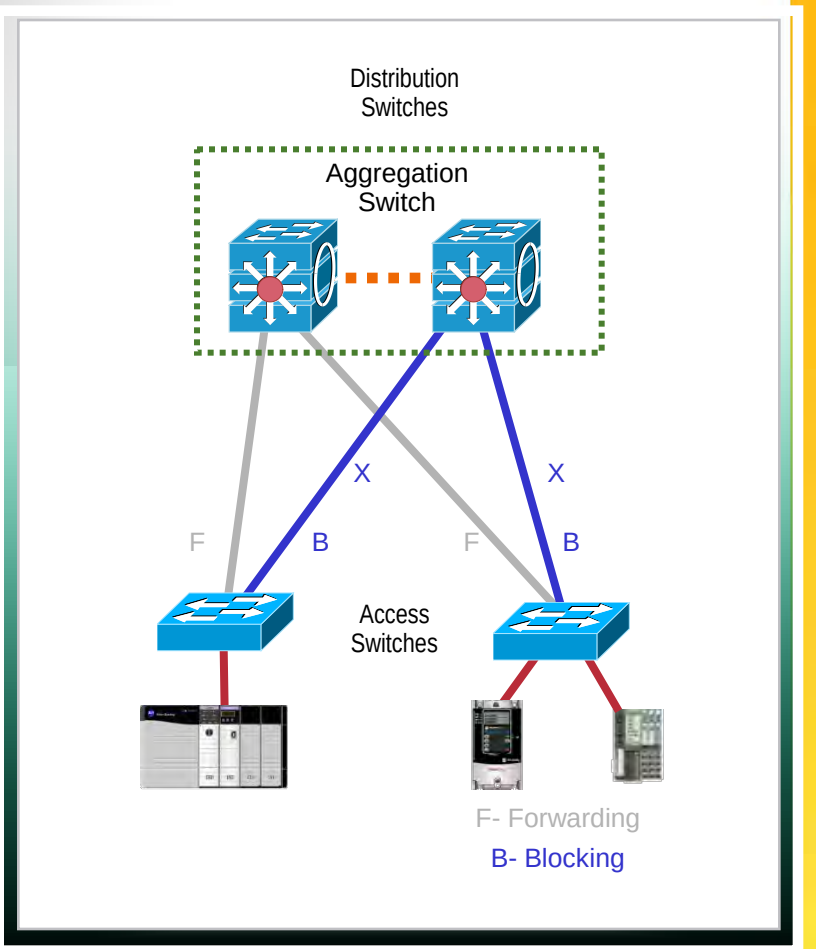




	Redundant Star	Ring	Linear
Cabling Requirements			
East of Configuration			
Implementation Costs			
Bandwidth			
Redundancy and Convergence			
Disruption During Network Upgrade			
Readiness for Network Convergence			
Overall in Network TCO and Performance	Best	OK	Worst

Spanning Tree Protocol (STP)

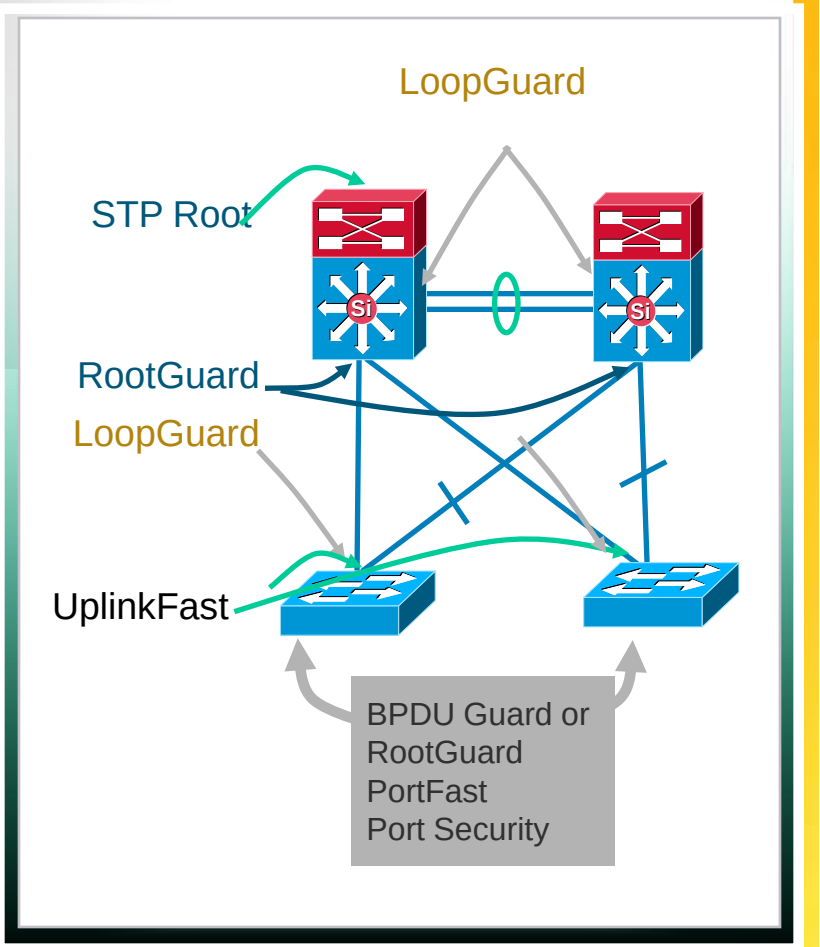
- Most common standard protocol for network resiliency—IEEE 802.1D
- Supports Redundant Star and Ring Topology
- Provides alternate path in case of failures, avoiding loops
- Unmanaged switches don't support STP
- Versions: STP, RSTP, MSTP and RPVST+ - there are differences
- Coordinate with IT before implementing



Layer 2 Hardening

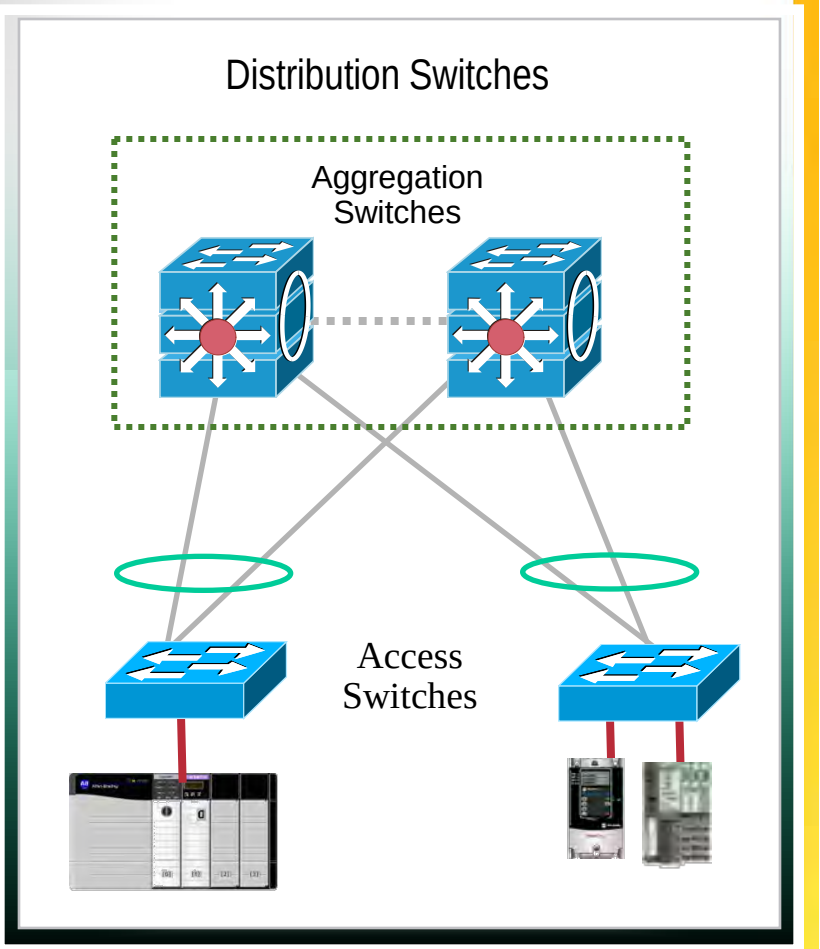
Spanning Tree Should Behave the Way You Expect

- Place the root where you want it—Distribution Switch
- Root primary/secondary macro
- The root bridge should stay where you put it
  - RootGuard
  - LoopGuard
  - UplinkFast
  - UDLD
- Only end-station traffic should be seen on an edge port
  - BPDU Guard
  - RootGuard
  - PortFast
  - Port-security
    - Standard setup applies the above



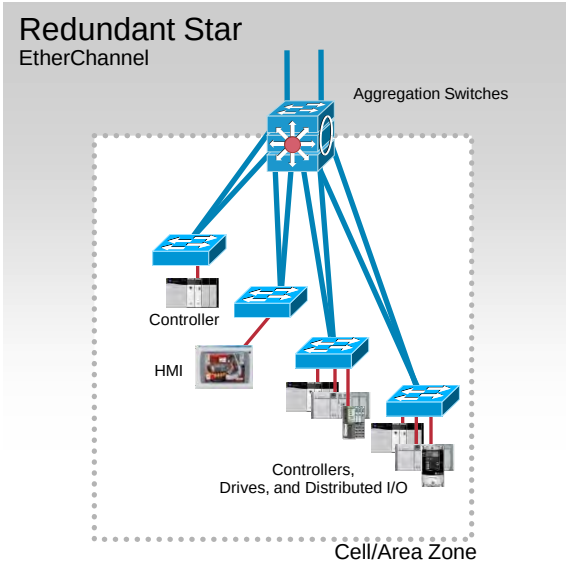
EtherChannel

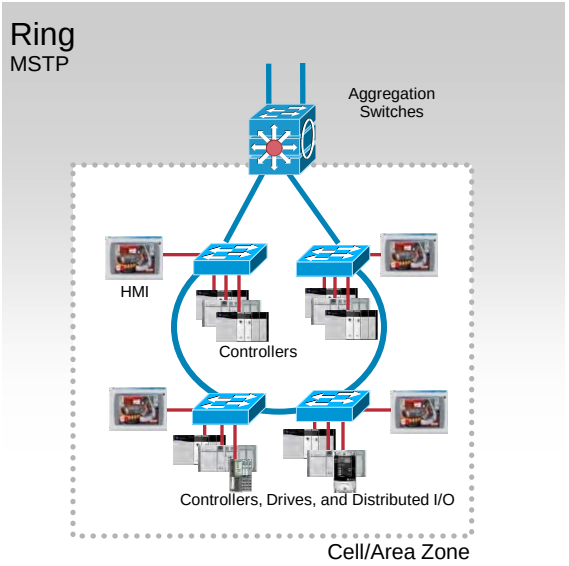
- Link Aggregation Control Protocol (LACP) port aggregation—IEEE 802.3ad
- Redundant Star Topology
- A way of combining several physical links between switches into one logical connection to aggregate bandwidth (2 to 8 ports)
- Provides resiliency between connected switches if a connection is broken

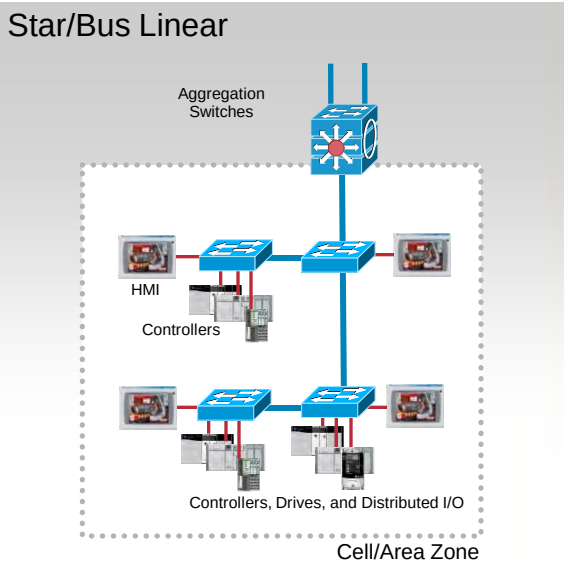


Reliability, Availability and Network Segmentation

Cell/Area Zone Topology Options



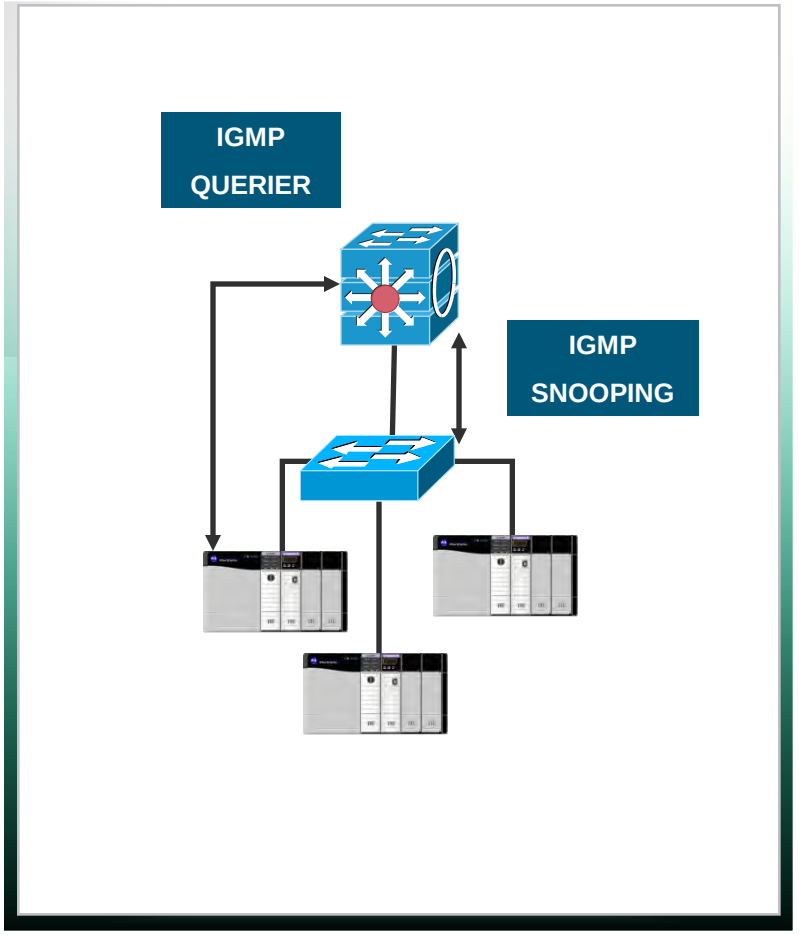




- **Use Fiber over Copper for uplinks**
- **Spanning Tree (MSTP) recovery in Ring topology for CIP Explicit Messaging such as HMI**
- **LACP in Redundant Star for CIP Implicit I/O applications**
- **Device Level Ring for device connectivity**

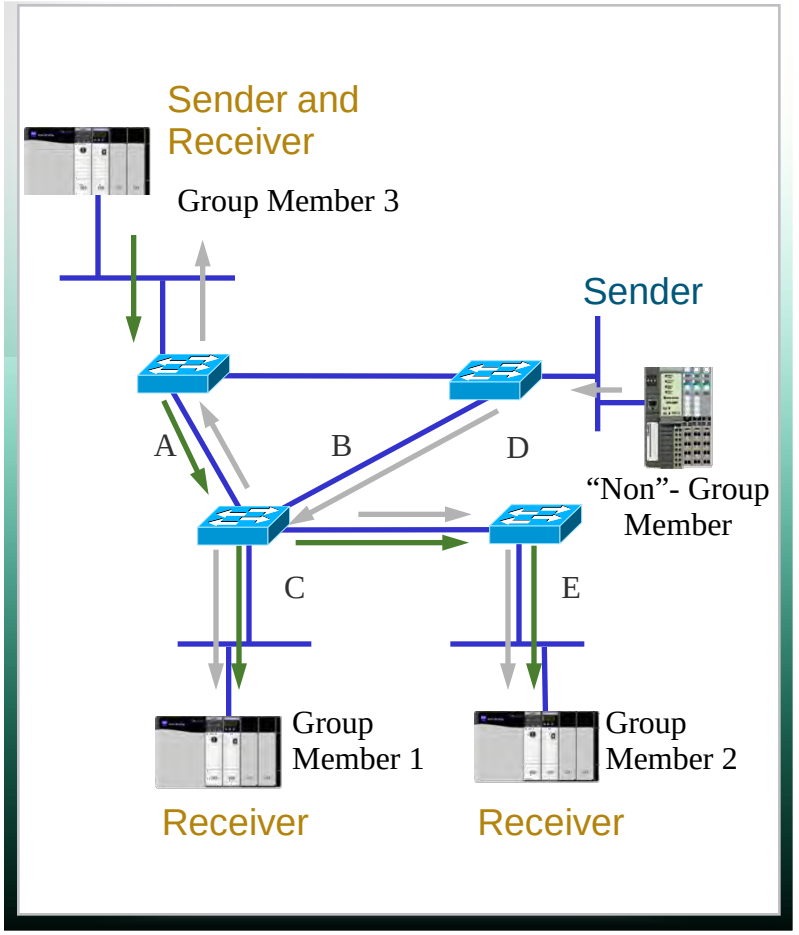
Multicast Protocols

- IGMP—Internet Group Management Protocol
- IGMP snooping is used to prevent multicast from flooding all ports on a VLAN. It monitors the IGMP packets from end devices
  - IGMP snooping becomes operational as soon as a Querier is detected
  - A Layer 2 access switch can act as an IGMP querier
  - Recommendation to select the distribution switch as acting querier by giving it the lowest IP on the VLAN
- Make sure IT is aware of multicast requirements
- IE switch enables IGMP in standard setup
  - IGMP v2, Querier and Snooping
  - Standard setup applies the above



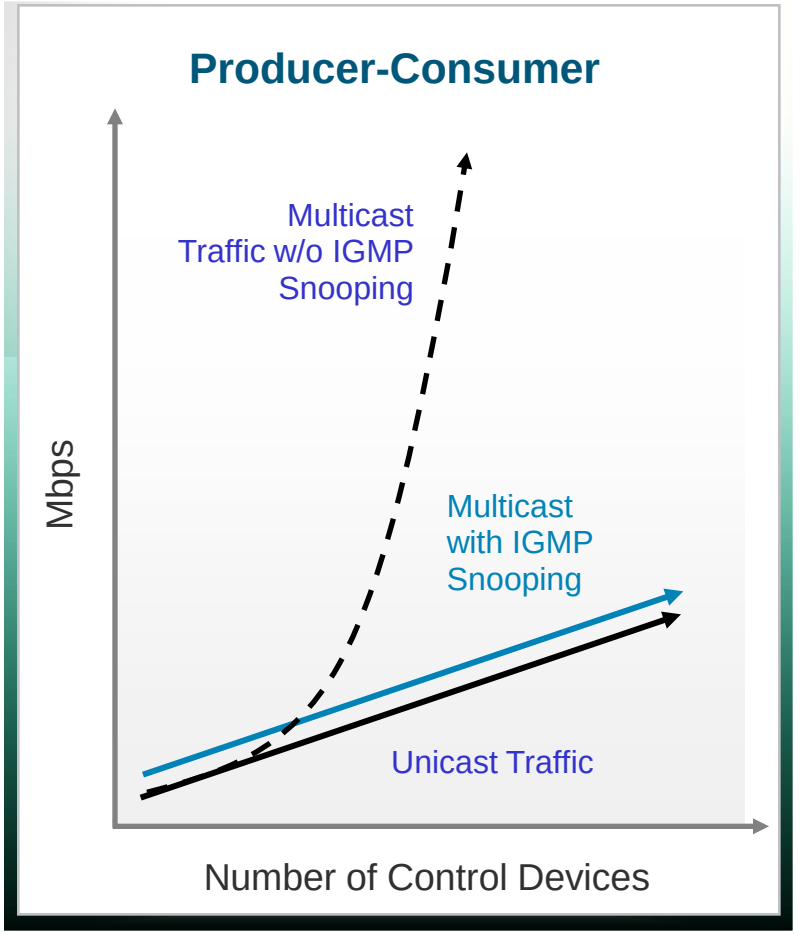
IP Multicast Group Concept

- 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



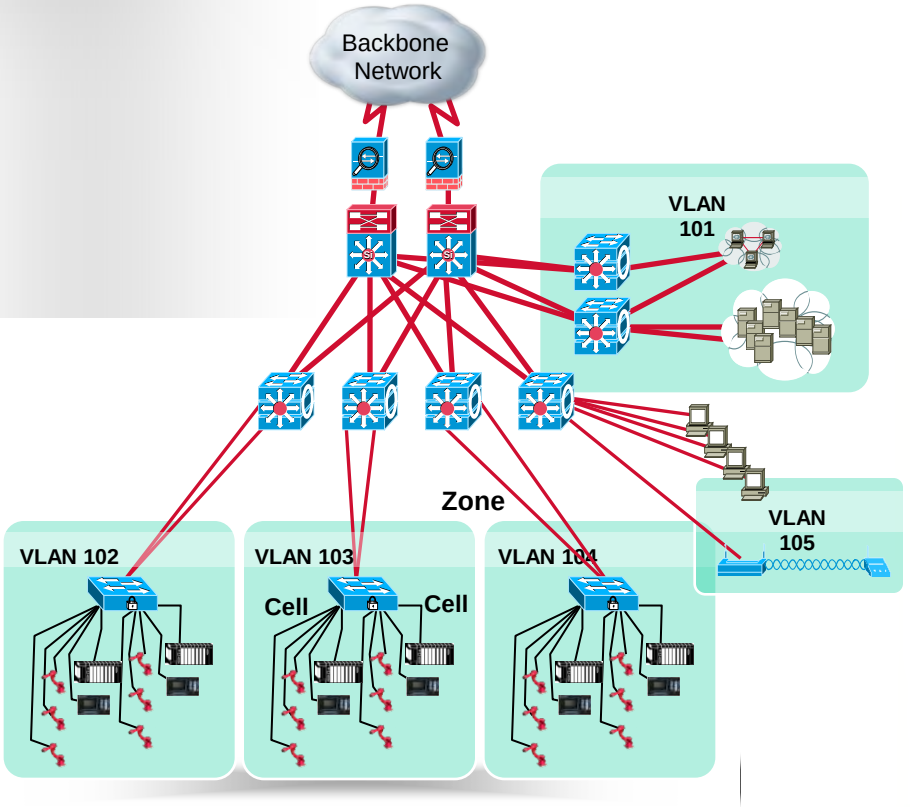
IGMP Snooping Summary

- In a Consumer-Producer Model traffic grows exponentially with the number of hosts unless multicasts are constrained
- IGMP Snooping provides scalability for Consumer-Producer Data Models by limiting the amount of multicast traffic
- Performance benefits of the Consumer-Producer model are maintained (all consumers have equal access to data)



VLANs in an Industrial Ethernet System

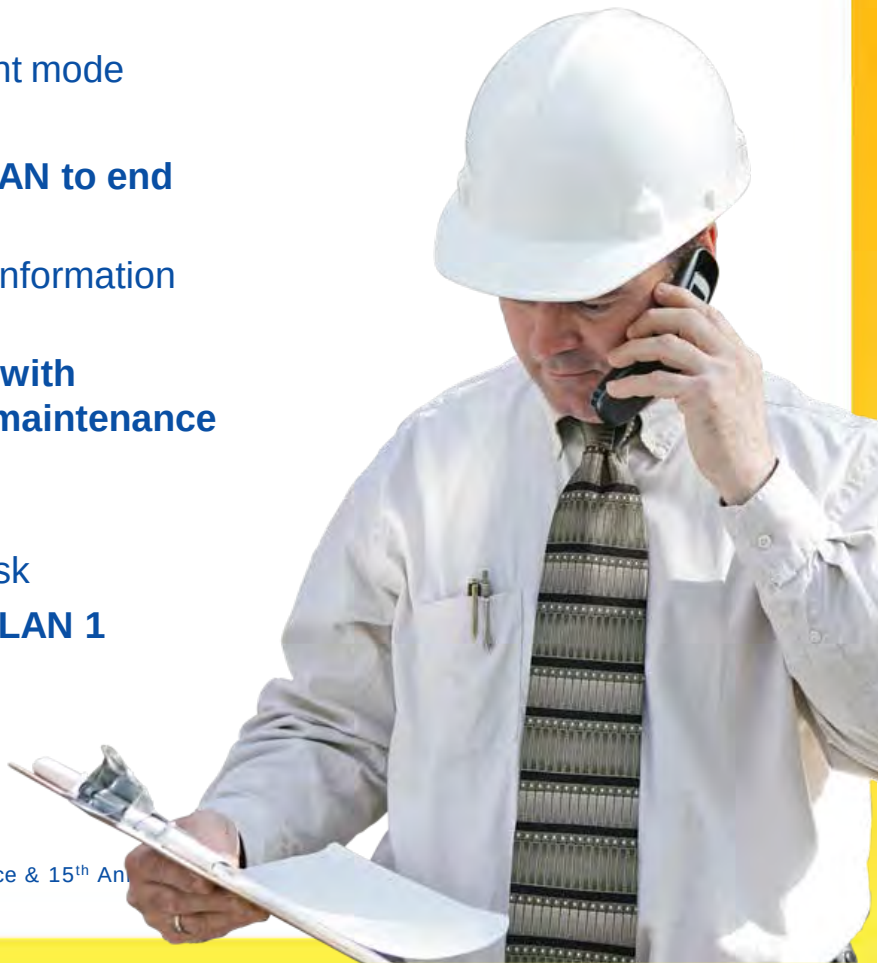
- Assign VLANs to devices when traffic patterns are known
- Limit the flow of produce of required devices **(e.g.: one VLAN per cell or zone)**
- Use L3 switch such as IE 3000 to exchange data between VLANs **(i.e. PLC interlock layer)**



Learn Your Traffic Patterns: Safemap.Sourceforge.Net

VLAN Considerations for Cell/Area zone

- **Design small Cell/Area zones, segment traffic types into VLANs and IP Subnets to better manage the traffic**
- **Requires Layer-3 switch or router to communicate between VLANs**
- **Use Layer 2 VLAN trunking between switches**
  - When trunking, use 802.1Q, VTP in transparent mode
  - Set native VLAN to something other than 1
- **Use switchport mode host command to assign VLAN to end device**
  - Do not use VLAN 1 for EtherNet/IP Control & Information Traffic
- **Enable IP directed Broadcast on Cell/Area VLANs with EtherNet/IP traffic for easy configuration and maintenance from IACS applications**
- **Prune unused VLANs for security**
  - Use VLAN 1 for data is viewed as a security risk
- **Create a Network Management VLAN, don't use VLAN 1**



Not All Traffic Is Created Equal

Prioritization Is Required

	Control (e.g., CIP)	Video	Data (Best Effort)	Voice
Bandwidth	Low to Moderate	Moderate to High	Moderate to High	Low to Moderate
Random Drop Sensitivity	High	Low	High	Low
Latency Sensitivity	High	High	Low	High
Jitter Sensitivity	High	High	Low	High

Control Networks Must Prioritize Control Traffic over Other Traffic Types to Ensure Deterministic Data Flows with Low Latency and Low Jitter

Quality of Service Operations

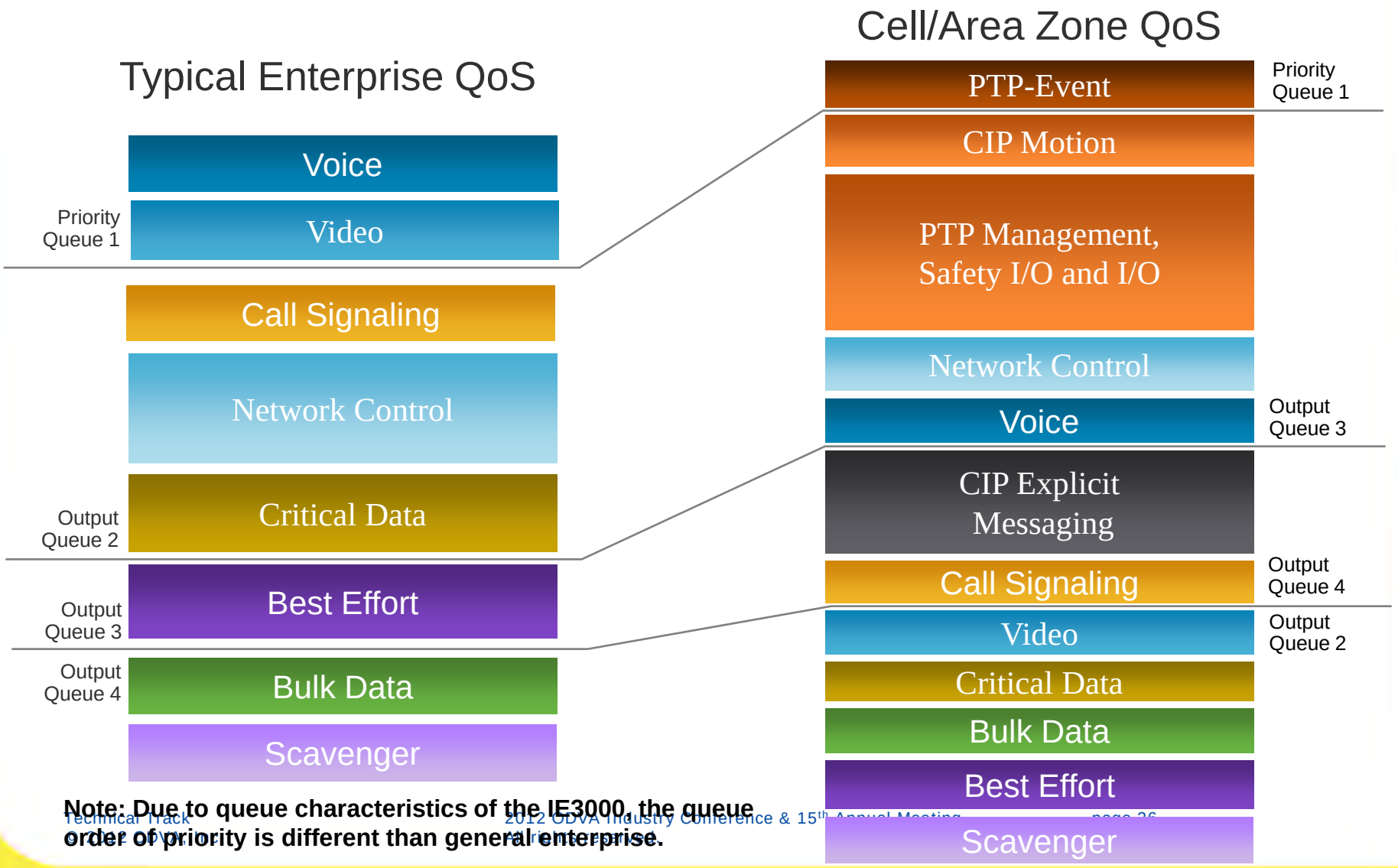
Classification and Marking

Queuing and (Selective) Dropping

Post-Queuing Operations

Cell/Area Zone QoS Priorities

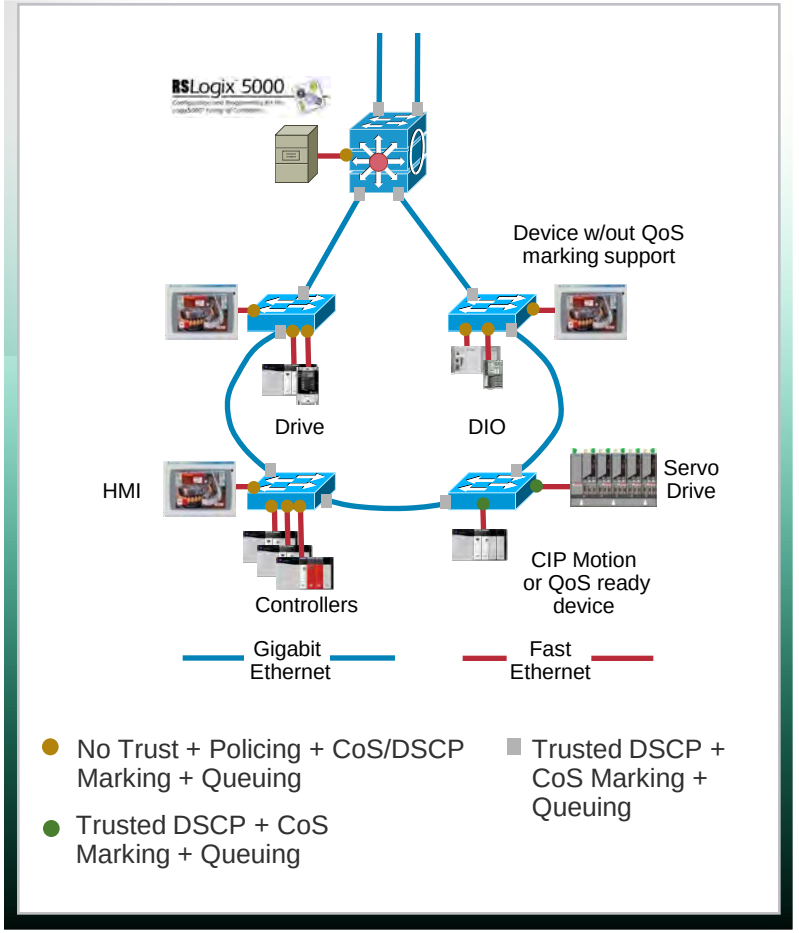
Output Queue traffic prioritization



Note: Due to queue characteristics of the IE3000, the queue order of priority is different than general enterprise.

QoS Design Considerations

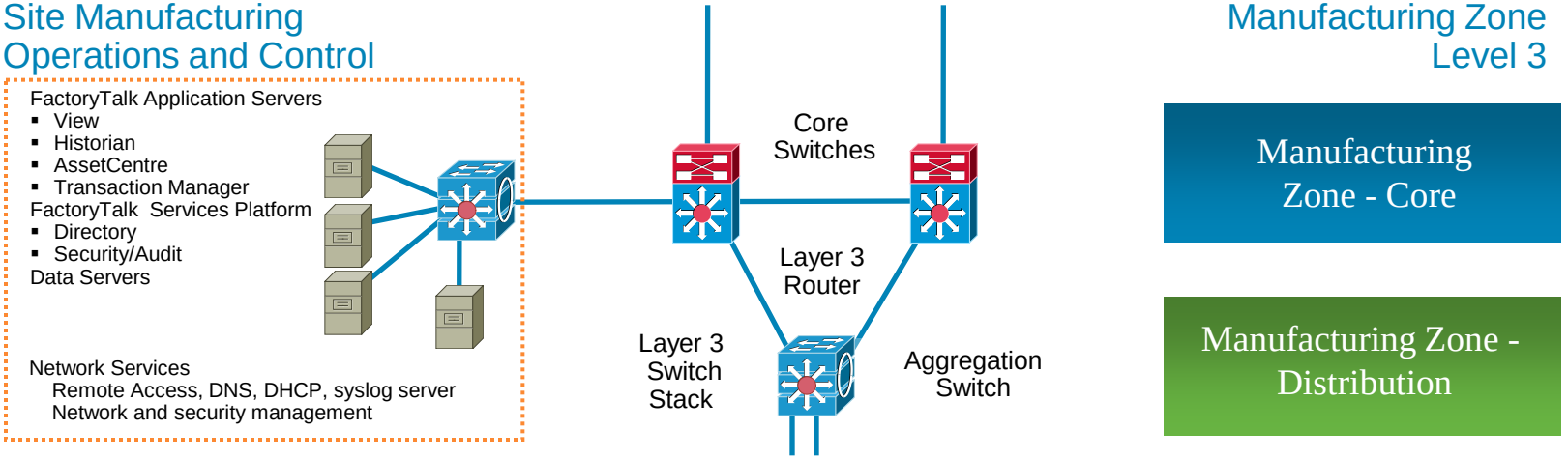
- Priority for latency and jitter sensitive CIP I/O traffic
  - Guaranteed delivery for CIP sync, CIP motion
  - Minimize impacts by DDoS attacks
- QoS deployed throughout industrial network
- QoS trust boundary moves from switch access ports to QoS-capable CIP devices
- For existing CIP devices, marking at the access port is based on port number
  - CIP I/O UDP 2222
  - CIP Explicit TCP 44818



IP Addressing
Management

Option	Description	Advantages	Disadvantages
Static	All devices hard coded with an IP Address	▪ Simple to commission and replace	▪ In large environments, can be burdensome to maintain ▪ Limited ranged of IP addresses and subnet ▪ Not all devices support
Static via BOOTP Configuration	Server assigns devices IP addresses Precursor to DHCP	▪ Supported by every device	▪ Requires technician to configure IP address/Mac address when a device is replaced ▪ Adds complexity and point of failure
DHCP	Server assigns IP addresses from a pool (NOT RECOMMENDED for Cell/Area devices)	▪ Efficient use of IP address range ▪ Can reduce administration work load	▪ More complex to implement and adds a point of failure ▪ Devices get different IP addresses when they reboot
DHCP Option 82	Server assigns consistent IP addresses from a pool (NOT RECOMMENDED)	▪ Efficient use of IP Address range ▪ Can reduce administration work load	▪ More complex to implement and adds a point of failure ▪ Mixed environments may not work

Manufacturing Zone Overview



- Highly available Layer 3, routing services for the Plant network

  Provides inter Cell/Area zone connectivity

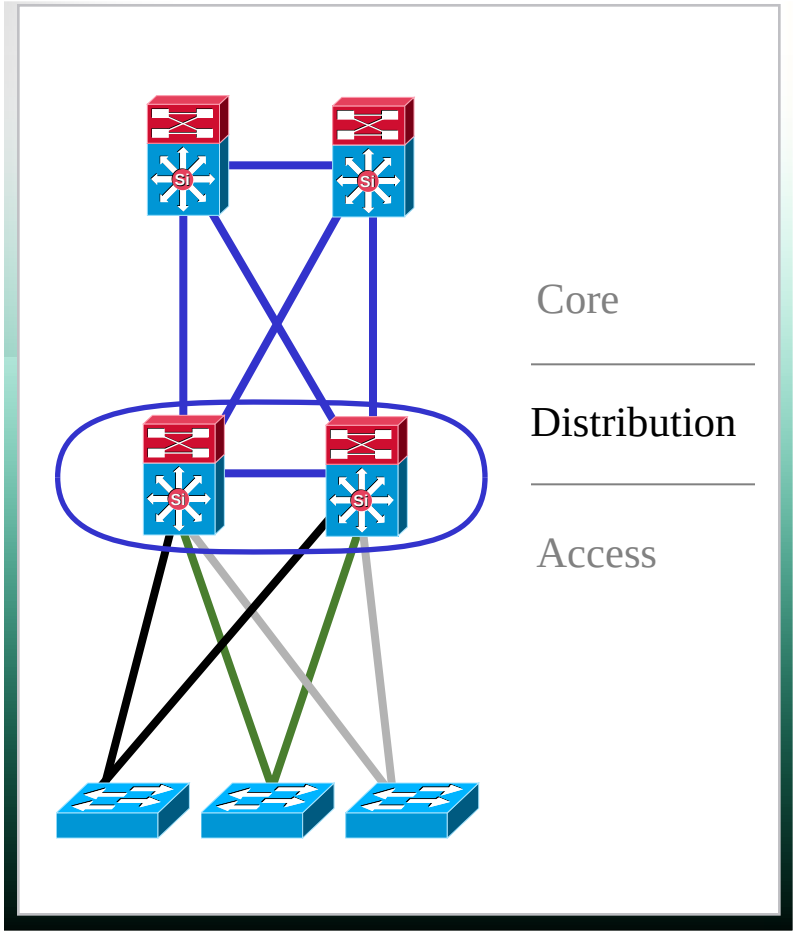
- Interconnectivity to the DMZ
- Network and Security management

- Level 3 Plantwide applications including the Factory Talk suite
- Key network-based services such as Access and Authentication (e.g. Active Directory), DHCP, DNS, etc.
- Remote Access Server

Distribution Layer

Policy, Convergence, QoS, and High Availability

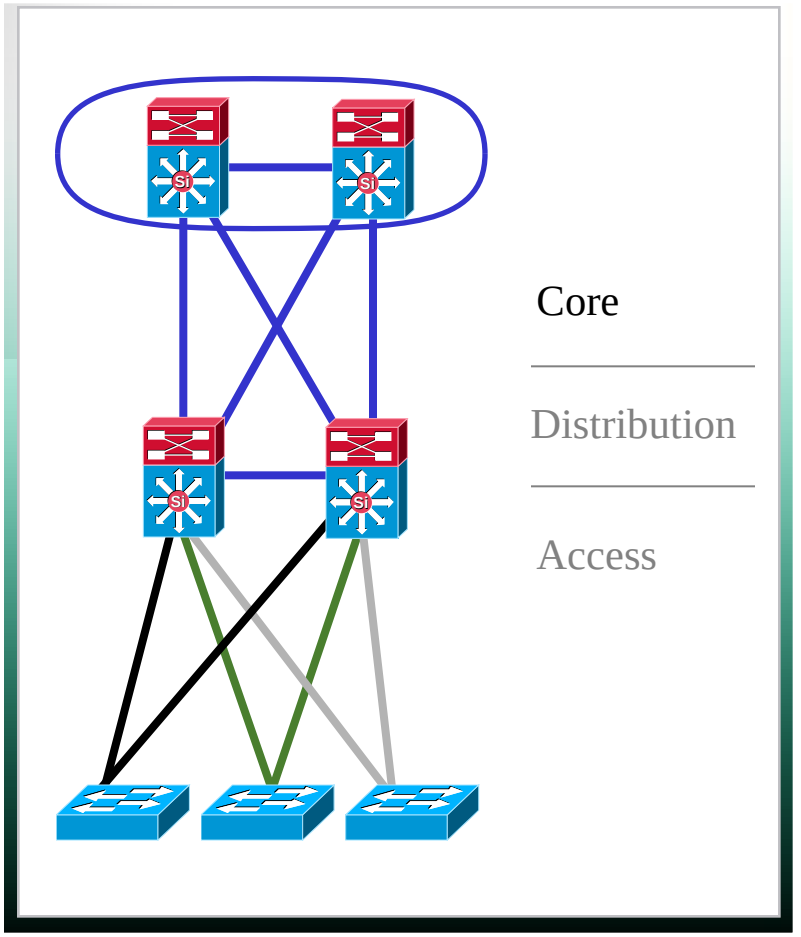
- Availability, load balancing, QoS and provisioning are the important considerations at this layer
- Aggregates Cell/Area zones (access layer) and uplinks to core
- Protects core from high density peering and problems in access layer
- Route summarization, fast convergence, redundant path load sharing
- HSRP or GLBP to provide first hop redundancy



Core Layer

Scalability, High Availability, and Fast Convergence

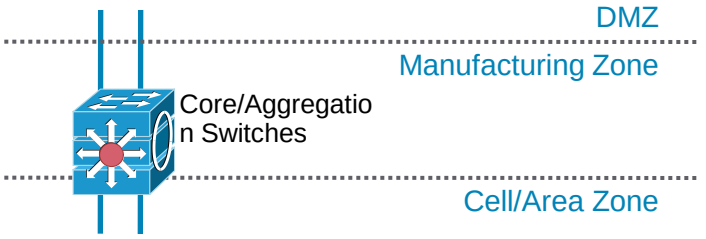
- Backbone for the network—connects network building blocks
- Performance and stability vs. complexity—less is more in the core
- Aggregation point for distribution layer
- Separate core layer helps in scalability during future growth
- Keep the design technology-independent



Manufacturing Zone Scalability

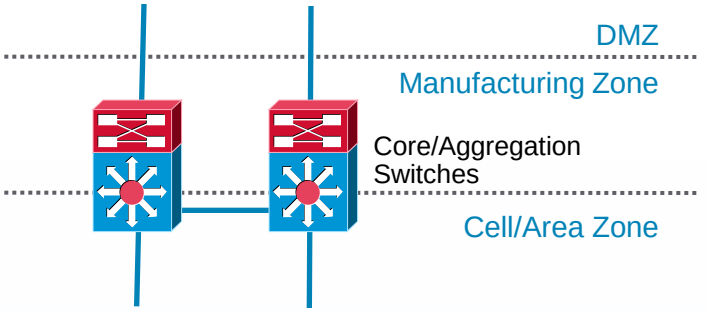
Small

- Collapsed Core/Distribution
- 30-50 Access switches



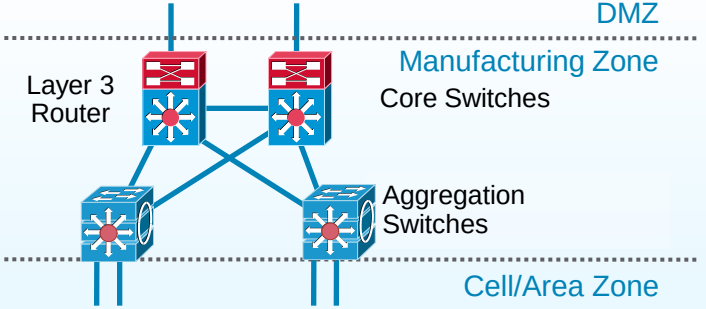
Medium

- Collapsed Core/Distribution
- <200 Access Switches



Large

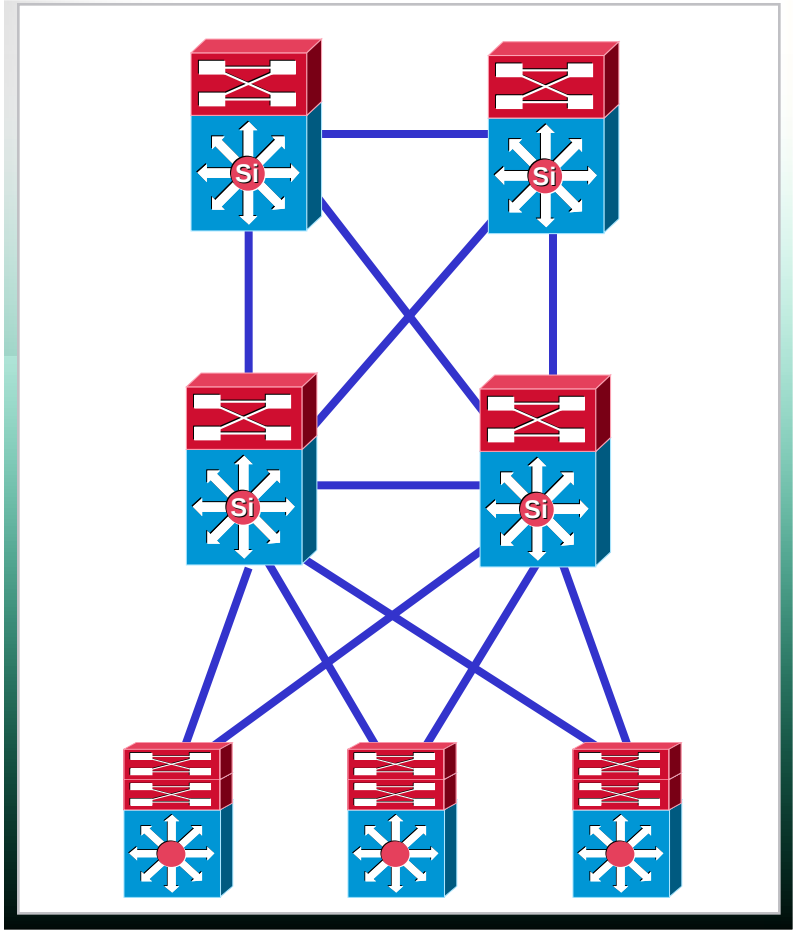
- Distinct Core/Distribution
- >200 Access Switches



Routing Design

Core and Distribution Routing Design

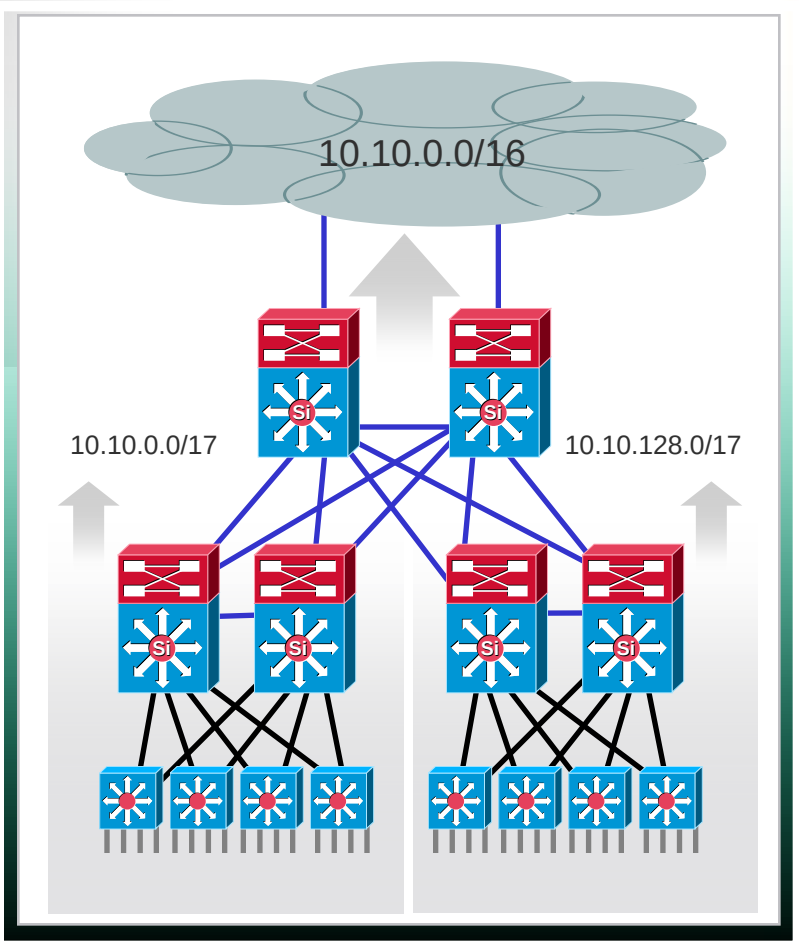
- Good routing design forms the foundation of the HA campus design
- Needed to quickly re-route around failed node/links while providing load balancing over redundant paths
- Build triangles not squares for deterministic convergence
- Only peer on links that you intend to use as transit
- Insure redundant L3 paths to avoid black holes
- Map the protocol design to the physical design



EIGRP in the Plant

Leverage the Tools Provided

- The greatest advantages of EIGRP are gained when the network has a structured addressing plan that allows for use of summarization and stub routers
- EIGRP provides the ability to implement multiple tiers of summarization and route filtering
- Relatively painless to migrate to a L3 access with EIGRP if network addressing scheme permits
- Able to maintain a deterministic convergence time in very large L3 topology

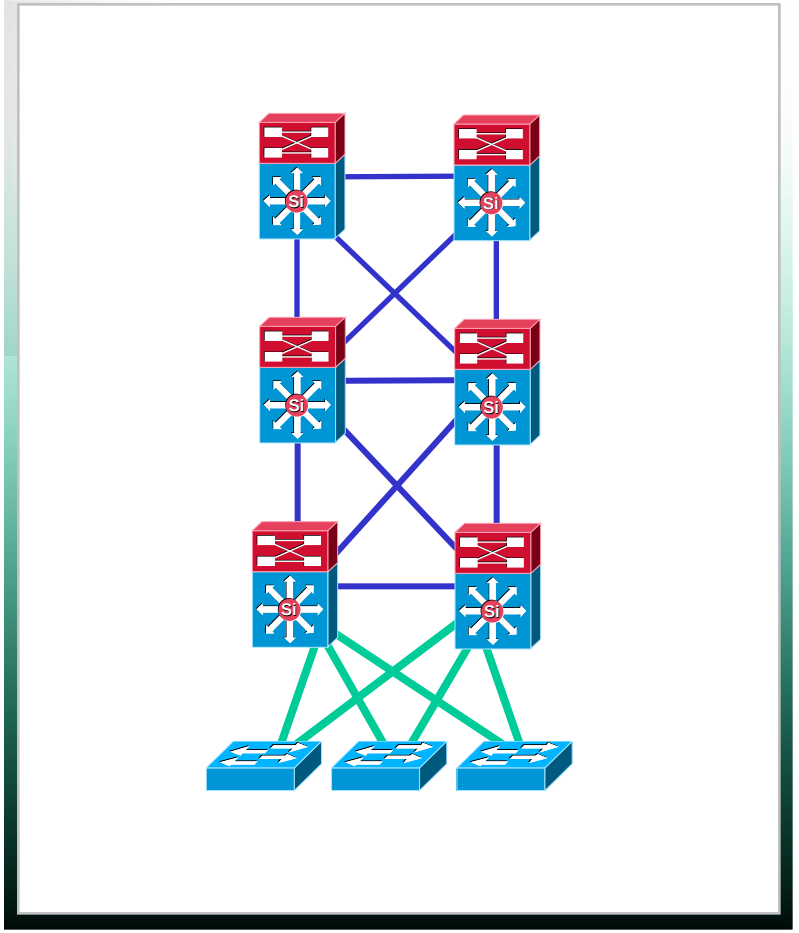


EIGRP Design Rules for HA Plant

Layer 2 Access—Same Rules Apply

- The basic EIGRP design rules apply irregardless if the access is L2 or L3
- Minimize the number and time for query response to speed up convergence
- Summarize distribution block routes upstream to the core
- Summarize at every major network tier

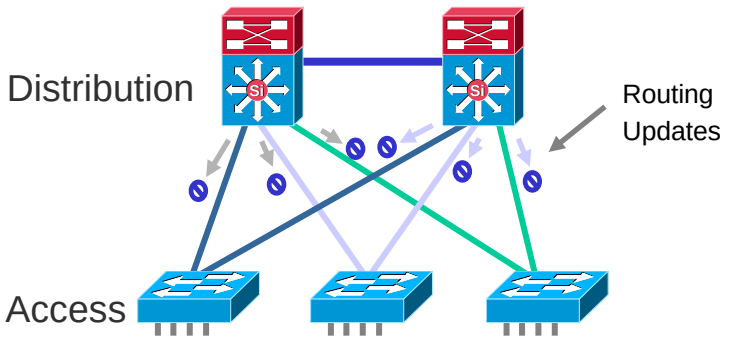
```
interface TenGigabitEthernet 4/1
 ip summary-address eigrp 100 10.120.0.0
 255.255.0.0 5

router eigrp 100
network 10.0.0.0
 passive interface <access-layer
 interface>
```



Design Principles—Plant Routing

Manage Your Routing Protocol

- Manage your routing protocol don't let it manage you
- It is easy to just turn it on and forget because it works
- Optimize your configuration to ease management and improve convergence
- Manage:
  - Router peering
  - Route summarization
  - Route propagation
  - Failure notifications (LSA and queries)
  - Protocol timers

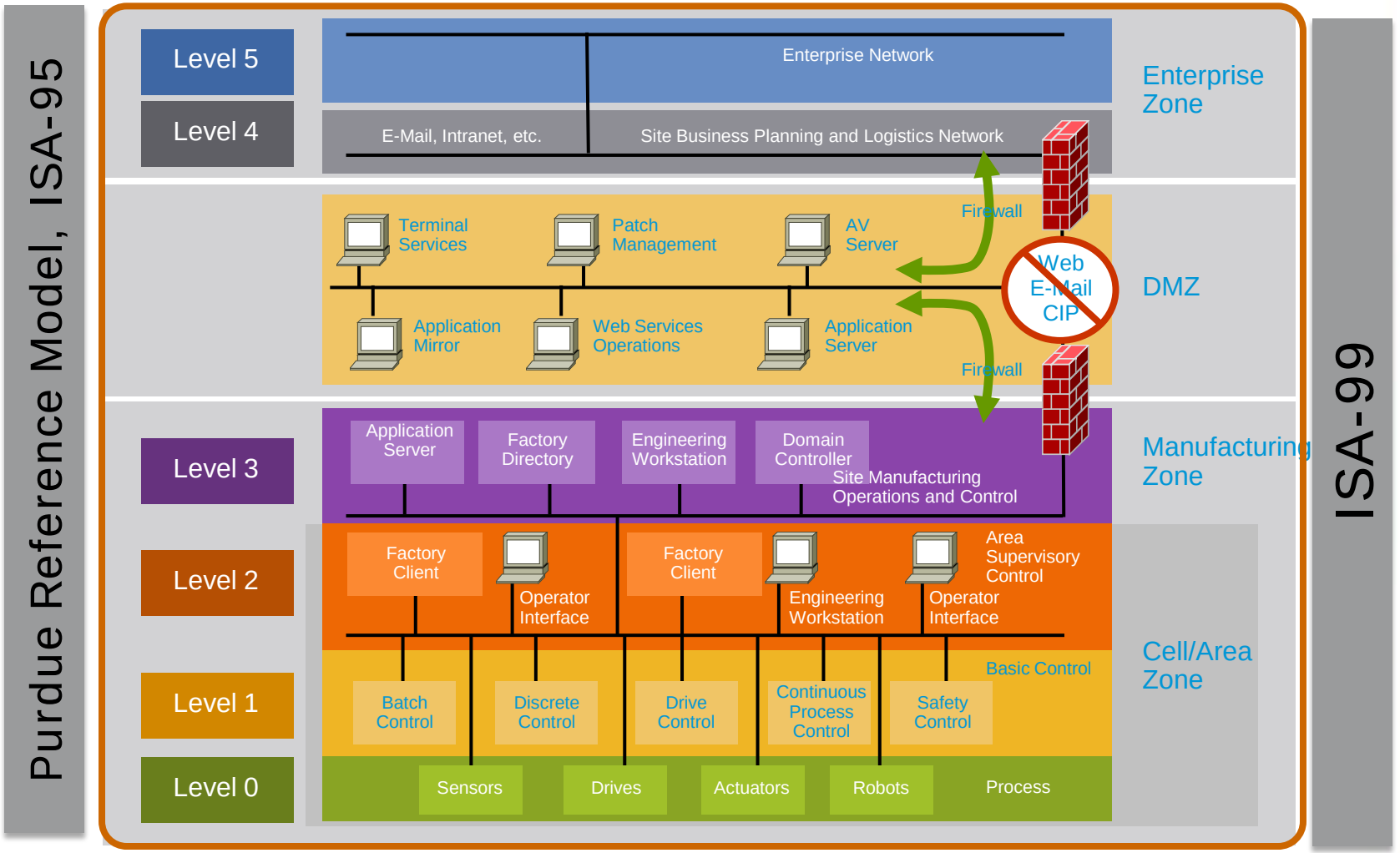


E.G. Prevent Peering Through the Access:

```
Router(config)#router eigrp 1
Router(config-router)#passive-
interface Vlan 99

Router(config)#router eigrp 1
Router(config-router)#passive-
interface default
Router(config-router)#no passive-
interface Vlan 99
```

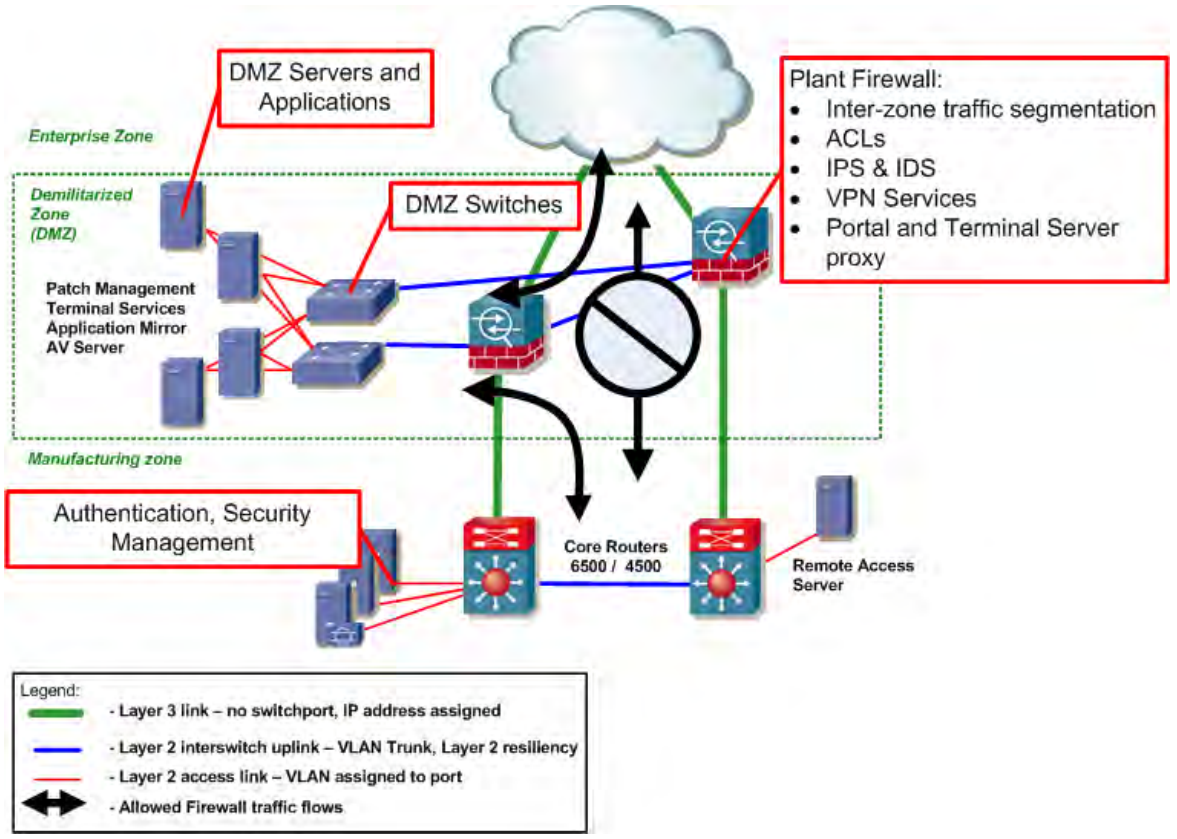
Logical Framework

Strong Segmentation



DMZ Deployment

Components and Traffic Flow



DMZ and Secure Remote Access

Guiding Principals

Use IT-Approved Access and Authentication

- VPN for secure remote access
- Enterprise Access and Authentication servers (e.g Active Directory, Radius, etc.)

IACS Protocols Stay home

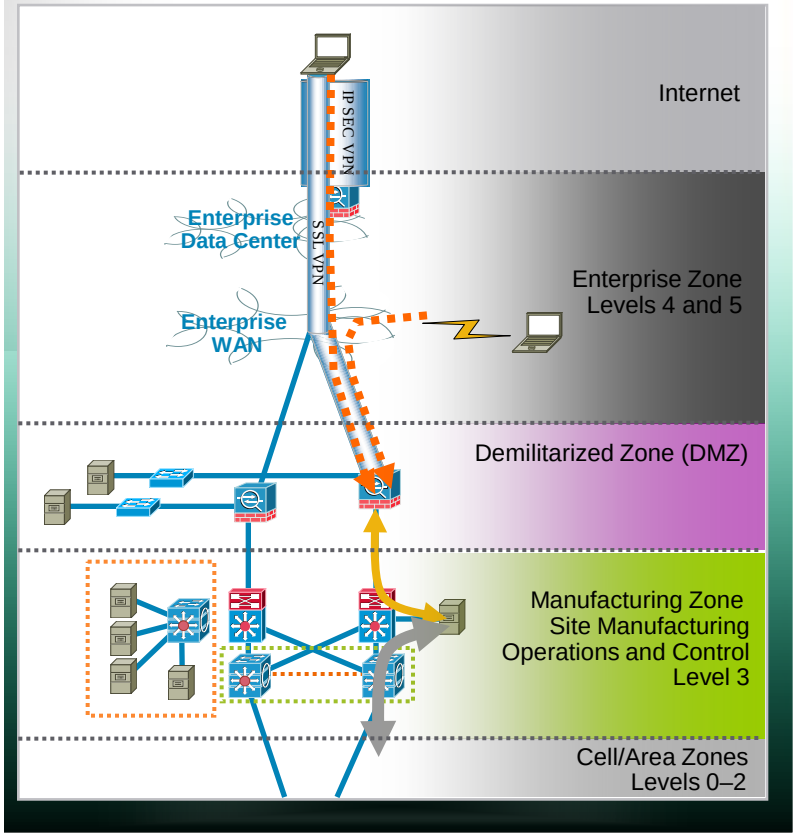
Control the Application

- Remote Access Server
- Application level security

No direct traffic

No common protocols

Only one path in and out of manufacturing zone—the firewalls



Secure Remote Access

- Remote engineer or partner establishes VPN to corporate network; access is restricted to IP address of plant DMZ firewall
- Portal on plant firewall enables access to IACS data, files and applications
  - Intrusion protection system (IPS) on plant firewall detects and protects against attacks from remote host
- Firewall proxies a client session to remote access server
- Access to applications on remote access server is restricted to specified plant floor IACS resources through IACS application security