The Software-defined Factory Enabled by SDA

cisco Live !

Erika Franco
Solutions Architect, Cisco

BRKIOT-2299

Why Are We Here Today?

Webex App

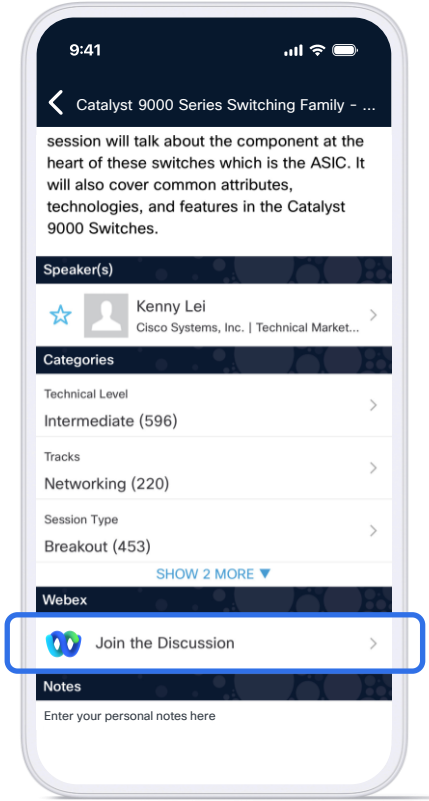
Questions?

Use Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Events App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until February 27, 2026.



Agenda

01 Why factories adopt SDA

02 Intro to SDA

03 The tale of 3 factories

04 The network as the nervous system of the factory

05 Overcoming industrial networking challenges

06 Closing remarks

Would you consider yourself...

Real-World Problems SDA Solves

Simplified Configuration

Configure networks through simple workflows instead of complex CLI commands.

AUTOMATION

AI/ML Integration

Add AI/ML applications seamlessly without redesigning the network infrastructure.

SCALABILITY

Consistent Security

Apply consistent OT/IT segmentation and security policies across the board.

COMPLIANCE

Optimized Performance

Reduce the negative effects of Spanning Tree on overall network performance.

EFFICIENCY

Location Independence

Run vPLCs and vHMIs independently of their physical hardware location.

VIRTUALIZATION

From Use Cases to Technology

We've covered the ***why*** – real OT use cases

Coming Next... the ***technology*** that makes them possible
And the practical challenges it introduces

The goal: understand SDA through an OT lens

How SDA Works

SDA is built from four planes that each solve a different problem, managing how the fabric learns, transports, secures, and manages traffic.

Control Plane

How fabric devices **learn**, register, and locate endpoints within the network.

Data Plane

How traffic is efficiently **transported** through virtual network overlays.

SDA
FABRIC

Management Plane

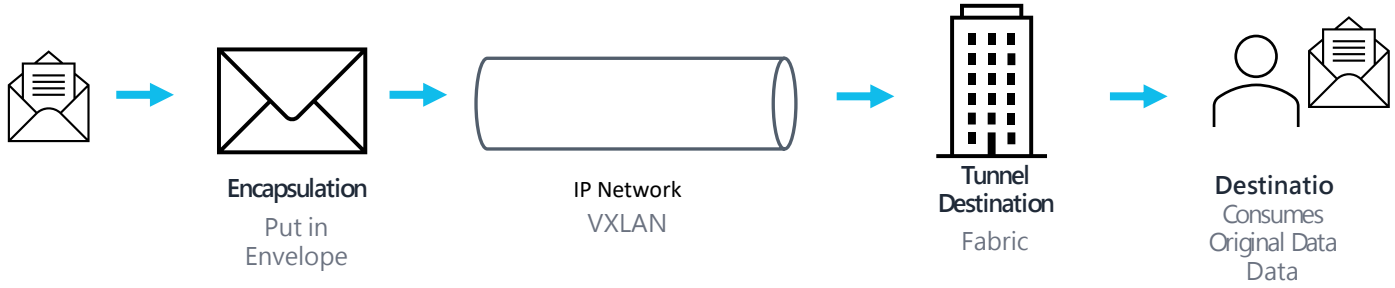
How the fabric is centralized, **orchestrated**, monitored, and **assured**.

Policy Plane

How segmentation, identity, and access rules are automatically **enforced**.

VXLAN: Virtual Networks Above the Physical Network

Data Plane



Logical Overlay

Virtual networks on physical infra

Location Agnostic

Workloads anywhere anywhere in fabric

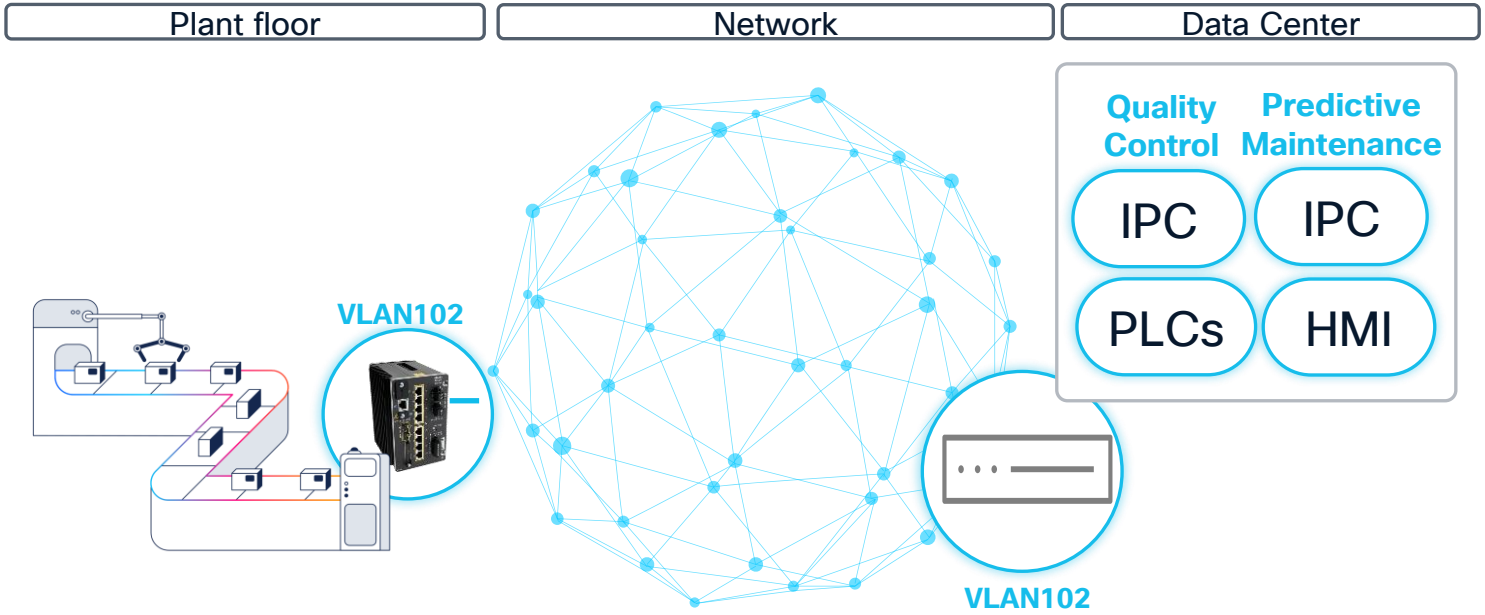
L2 over L3 Transport

Stretch L2 across L3 L3 boundaries

Massive Scalability

16 Million VNIs vs 4K VLANs

What VXLAN Means for your Factory



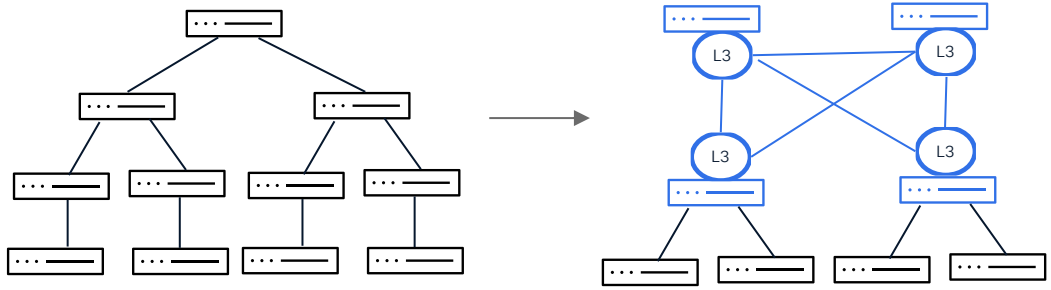
No Physical Dependency
Networks not bound to racks

Layer-2 Everywhere
Seamless subnet extension

Flexible Mobility
Move devices without re-IP

From Spanning Tree to Spanning Shrubs

- STP domains stay **small** and **local** (below the Fabric Edge)
- L2 is extended **logically**, not through physical trunks
- The fabric core is a **routed L3 network** with no blocked links
- Topology changes stay **contained** to local zones



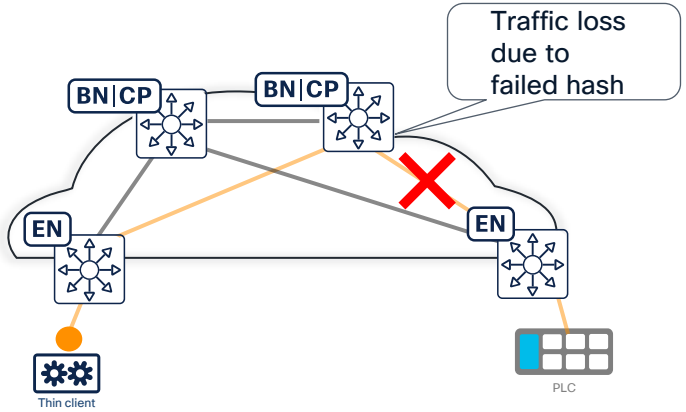
Traditional Spanning Tree

SDA Fabric

Extending L2 Over L3: The Reliability Reality

Routed Fabrics ≠ Zero-Loss

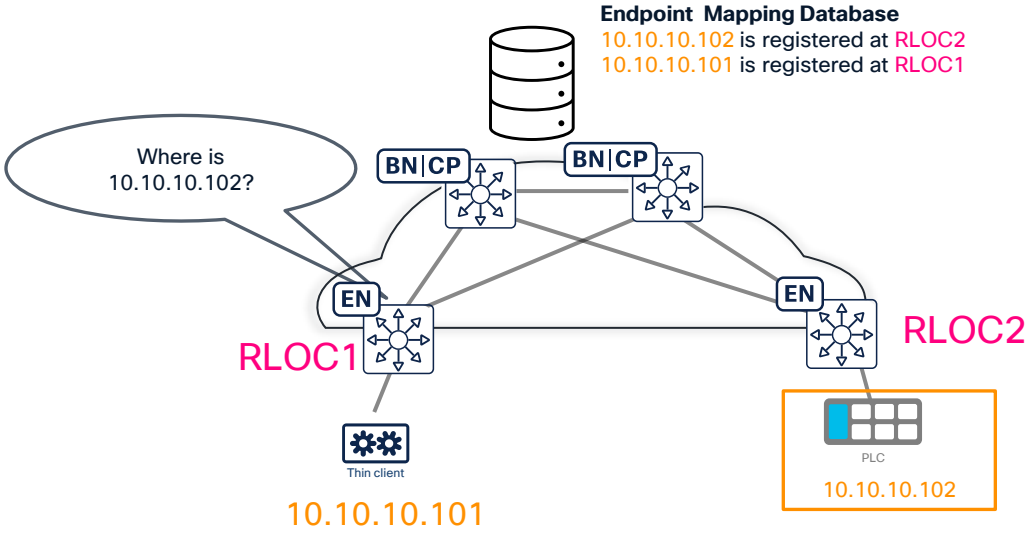
- ECMP provides redundancy, **not hitless failover**
- Traffic hashed to a failed link is dropped
- Convergence requires control-plane updates (FIB, SPF)
- Fast recovery – **not instantaneous** (even with BFD)
- OT impact: PLC communication may be **disrupted** by losses measured in **milliseconds**; **safety protocols** require even tighter tolerances.



Key Question:
Can critical control traffic rely on routed convergence alone?

LISP: The Control Plane That Decouples Identity from Location

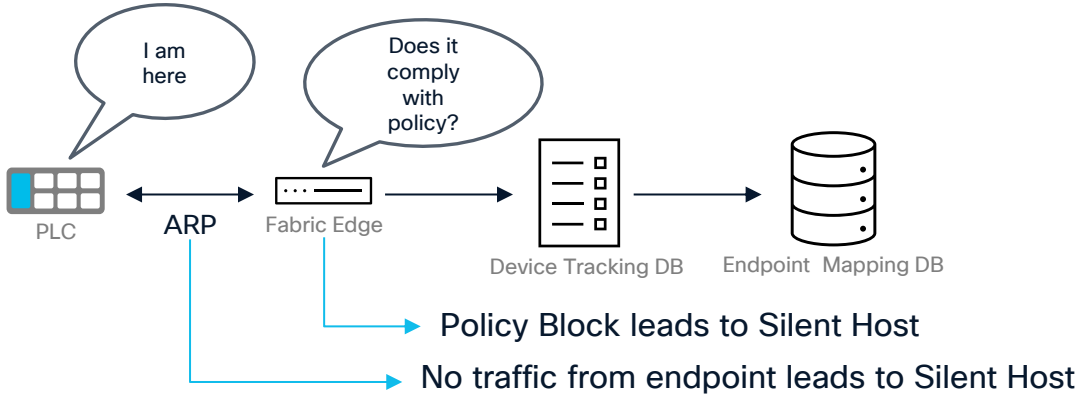
- Identity ≠ location: **an IP is no longer tied to a physical place**
- Mappings are kept in a **database**, not in every routing table
- Lookups happen on demand – **much like DNS**
- Result: Smaller tables, **lower CPU load**, faster convergence.



EID = Endpoint Identifier: (Who you are)
RLOC = Routing Locator: (Where you are)
Endpoints (EIDs) map to fabric nodes (RLOCs)

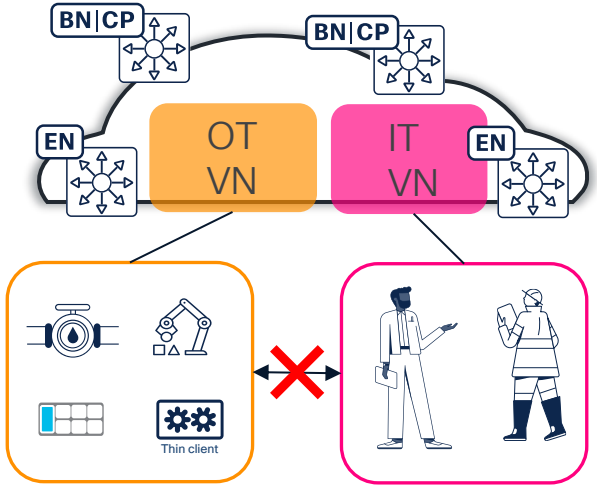
The Registration Pipeline: Why Some OT Assets Go Missing

- Devices must register so the fabric can locate them
- First ARP/DHCP traffic triggers SISF device tracking
- Policies control whether registration is allowed
- Unregistered devices become “silent hosts” and cannot be reached



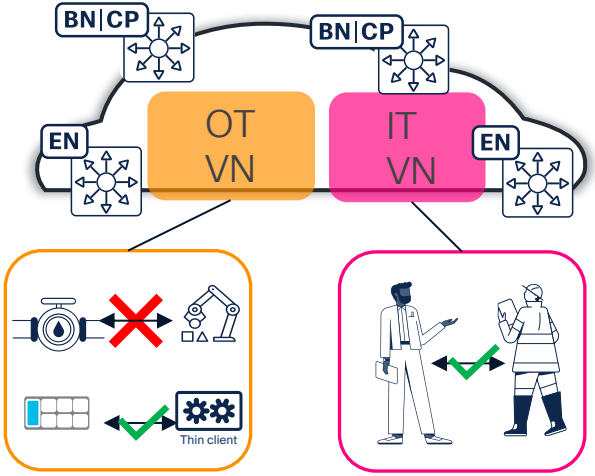
How the Policy Plane Shapes Segmentation

Policy Plane = The Rules Enforcing Movement Between and Within VNs



Macro-segmentation

Separate Wings (Virtual Networks)
OT, Management, Telemetry – isolated domains on the same fabric.



Micro-segmentation

Granular Permissions (SGTs) — Devices/users only get the permissions they need inside the VN.

What This Really Means for Manufacturing: A Decision Point

You CAN run OT & IT on the same hardware – but should you?

The answer:
It depends on **risk**, **operations**, and **lifecycle realities**.
Let's break it down.

The Case for a Dedicated OT SDA Network

Isolation from IT Changes: Prevents unintended OT disruptions. Preserves autonomy and independence of IT and OT teams. Upgrade cycles are different.

Custom Segmentation: Enables tailored OT segmentation.

Quality of Service (QoS): Simplifies prioritization of critical OT communications.

Scalability: may be an option on extensive industrial setups by enabling separate networks when the volume of OT and IT devices surpasses appliance limits

The Case for a Shared IT/OT SDA Network

Cost-Efficient Infrastructure: Optimizes resource utilization and minimizes expenses.

Simplified Administration: Streamlines network management, reducing complexity for improved efficiency.

Converged IT/OT Infrastructure: Brings IT tools to OT environments, enabling real-time telemetry and data analytics as the backbone of modern manufacturing.

slido

Please download and install the Slido app on all computers you use

Which option is best for your deployment?

ⓘ Start presenting to display the poll results on this slide.

cisco

Management Plane (SDA)

Intent In → Automated Fabric Out

KEY BENEFIT

- Deploy new networks and services from a centralized point in a fully compliant way across ALL devices.

CATALYST CENTER

1. Define Intent

Describe policies, segmentation, and onboarding requirements.

No Complex CLI

2. Centralized Orchestration

Intelligently translates high-level intent into specific device configurations.

3. Universal Compliance

Consistent provisioning of VNs, SGTs, and overlays across the entire fabric.

Why This Matters to You

Focus on the “What,” Not the “How”... at a Scale

Intent Gives You

Speed Faster deployment cycles.

Consistency Uniform policy application.

Automation Reduced manual effort.

OT Reality

Change-control discipline Strict validation required.

Limited workflow automation from Catalyst Center

Stability requirements Uptime is non-negotiable.

OUR STRATEGY

What We Recommend

Intent for core/distribution

IE switches managed differently - Tailored approach.

But this is not... "giving up automation and compliance"

The Tale of Three Factories A Journey Through Real-World Requirements

slido

Please download and install the Slido app on all computers you use

What are the most critical requirements for your factory network?

ⓘ Start presenting to display the poll results on this slide.

Three Recommended Architectures for Manufacturing

Your use cases, processes, and risk profile determine which model fits best.

① Traditional Non-Fabric Architecture

Classic and proven

Best for sites not yet ready to extend fabric across the plant.

② Fabric to the Distribution Layer

Hybrid approach

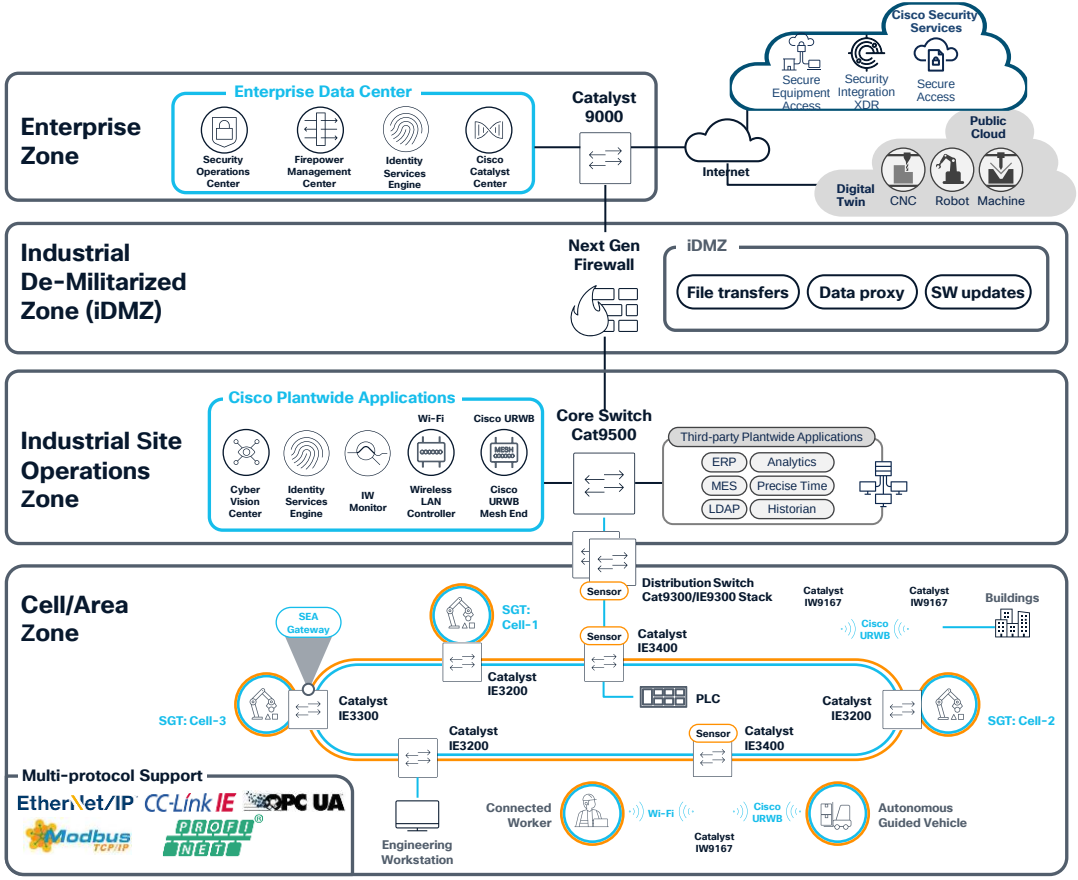
Use SDA to interconnect cell/area zones
while keeping OT cell switches non-fabric.

③ Dual SDA Fabric

End-to-end fabric

Supports control traffic traversing the fabric across the entire plant.

Non-Fabric Manufacturing Architecture

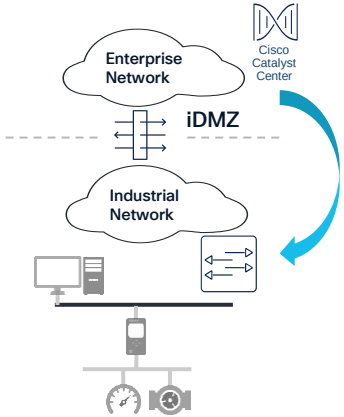


- Built on the classic Purdue Model: routed core, VLAN segmentation, and well-defined security zones.
- L2 domains stay local to cells, machines, and production lines; no fabric-wide overlays.
- The architecture is automated, monitored, and assured through **Cisco Catalyst Center**.
- The design follows **Cisco Validated Designs (CVD)** for industrial automation.

Non-Fabric OT: Catalyst Center Managed

Pros

- Faster deployment
- Reduced errors
- Streamlined management
- Preserves existing design



Cons

- Lack of SDA fabric benefits
- Limited IT/OT convergence

Best for: Dedicated industrial networks, especially brownfield environments.

Factory One – “Aligned to the Purdue Model”

SDA READINESS ASSESSMENT FORM

☐ Is IT/OT shared network infrastructure a requirement?
- ☐ Yes
- ☑ No

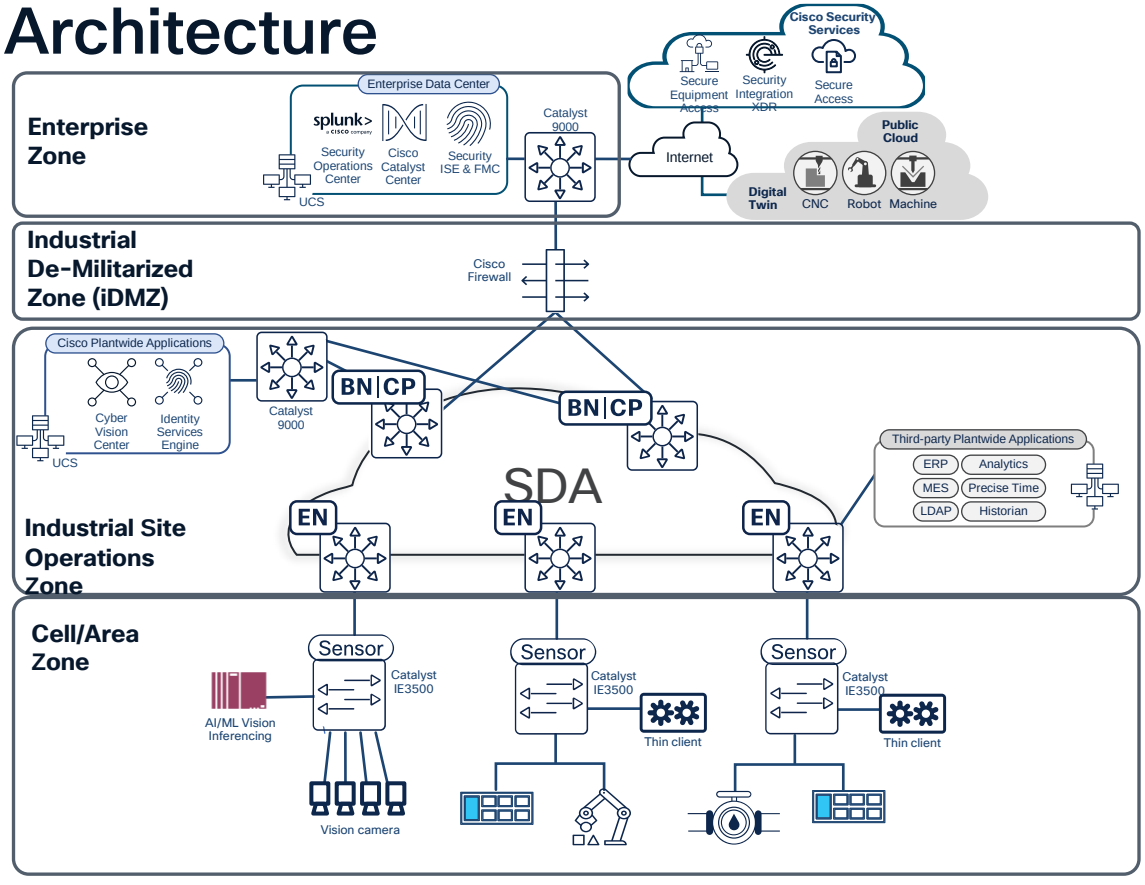
☐ Is intent-based configuration required?
- ☐ Must-have
- ☑ Nice to have

☐ Is VLAN stretching across areas a requirement?
- ☐ Yes
- ☑ No

☐ Is there strong collaboration between IT and OT?
- ☐ Yes
- ☑ No

ASSESSMENT SUMMARY
- ☑ Network follows the classic Purdue Model
- ☑ Needs: Automation and assurance

Fabric to the Distribution Layer – Manufacturing Architecture



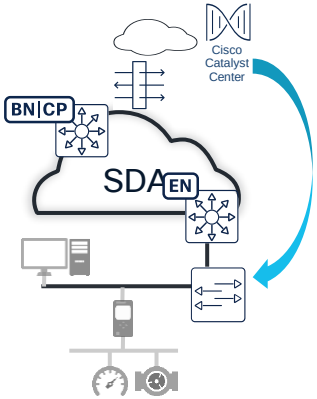
- Strict firewall control for traffic entering the OT network
- Localized services like ISE PSN and Cyber Vision to enhance network survivability
- Macro segmentation to isolate virtual networks
- Micro segmentation to enforce zones and conduits
- Intent-based configuration

SDA for OT Network Down to Distribution

OT network managed by Catalyst Center

Pros

- Automation and Assurance for IE switches
- Flexibility in administration: centralized or distributed network management
- SDA macro segmentation
- Micro segmentation
- IT manages IP pools and OT downlinks.



Cons

- Shared infrastructure requires close collaboration between OT/IT during change management

Best for: Converged IT/OT core networks

For most manufacturing use cases, IE switches are best operated as non-fabric devices

NOT RECOMMENDED
Fabric Edge (FE) or Policy-Extended Node (PEN)

- **Limited provisioning flexibility:** no SD-card or out-of-band workflows
- **Coarse, inherited permissions:** PEN shares site-level access
- **OT protocol gaps:** no Catalyst Center workflows for PROFINET, MRP, CIP, L2NAT
- **Intent conflicts:** SDA automation may override required manual configs

CRITICAL CONSIDERATION: IE3500 AS FE

Interlocks depend on routed convergence – unacceptable for time-critical OT.

RECOMMENDED
IE switches as a Non-Fabric Devices

- **Operational freedom:** SD-card and out-of-band provisioning preserved
- **Automation:** still managed by Catalyst Center
- **Advanced security:** TrustSec / SGT supported without PEN

KEY BENEFITS

Full OT Control | Automation | TrustSec

Factory Two – “SDA where it makes sense, OT where it makes sense”

SDA READINESS ASSESSMENT FORM

☐ Is IT/OT shared network infrastructure a requirement?
☑ Yes ☐ No

☐ Is intent-based configuration required?
☐ Must-have ☑ Nice to have

☐ Is VLAN stretching across areas a requirement?
☐ Yes ☑ No

☐ Is there strong collaboration between IT and OT?
☐ Yes ☑ No

ASSESSMENT SUMMARY

☑ IT has already implemented SDA at the L3 industrial boundary

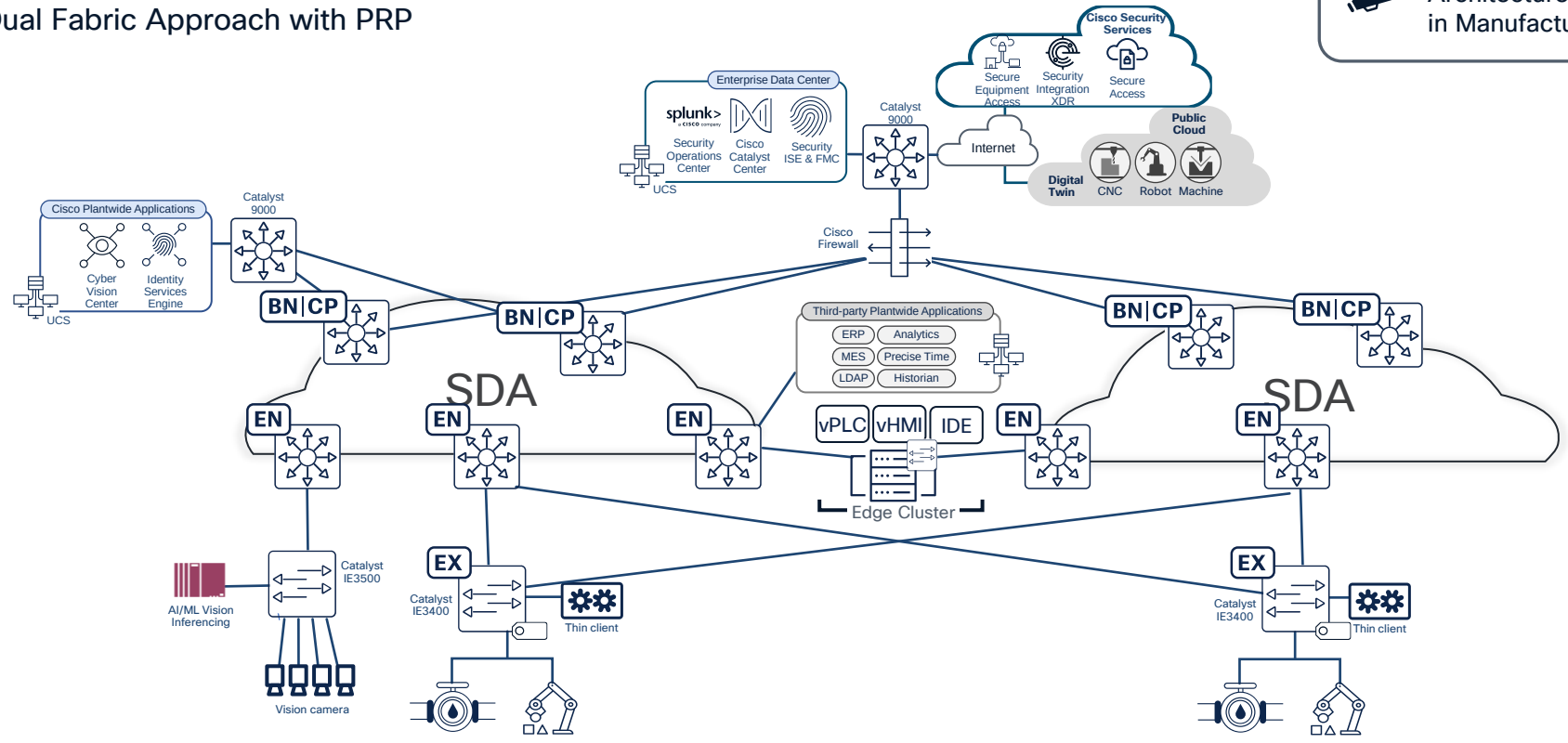
☑ OT needs automation and assurance for IE switches

☑ OT expresses interest in segmentation

Dual SDA Fabric Architecture

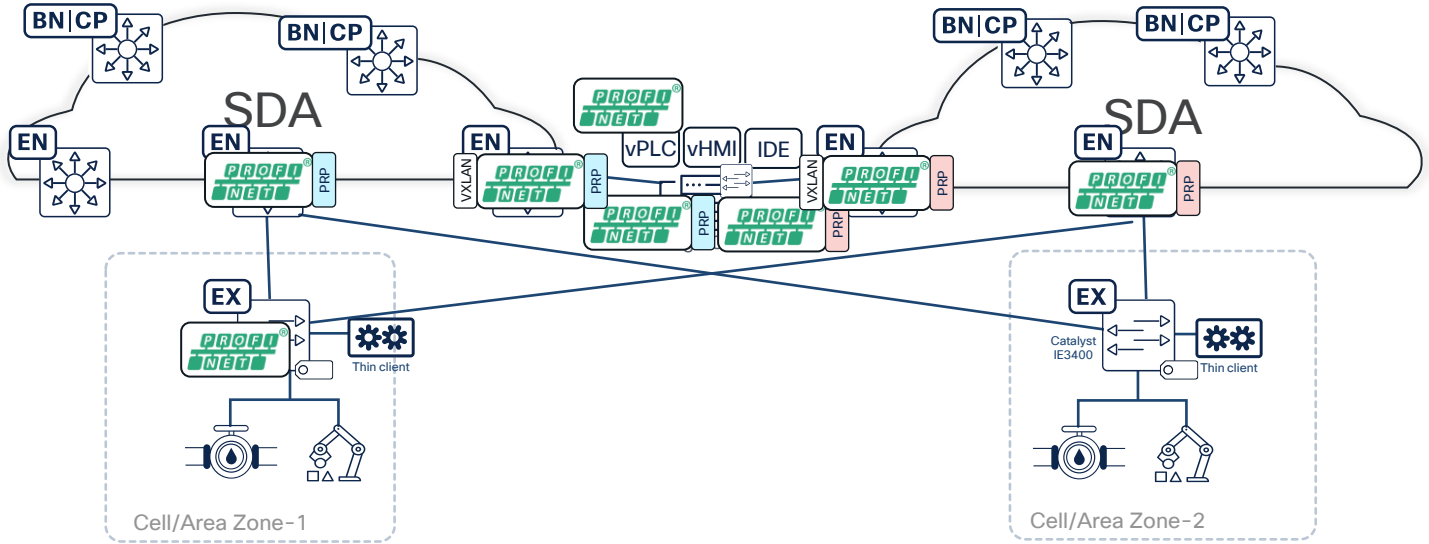
Dual Fabric Approach with PRP

New CVD: Dual Fabric Architecture for vPLC in Manufacturing



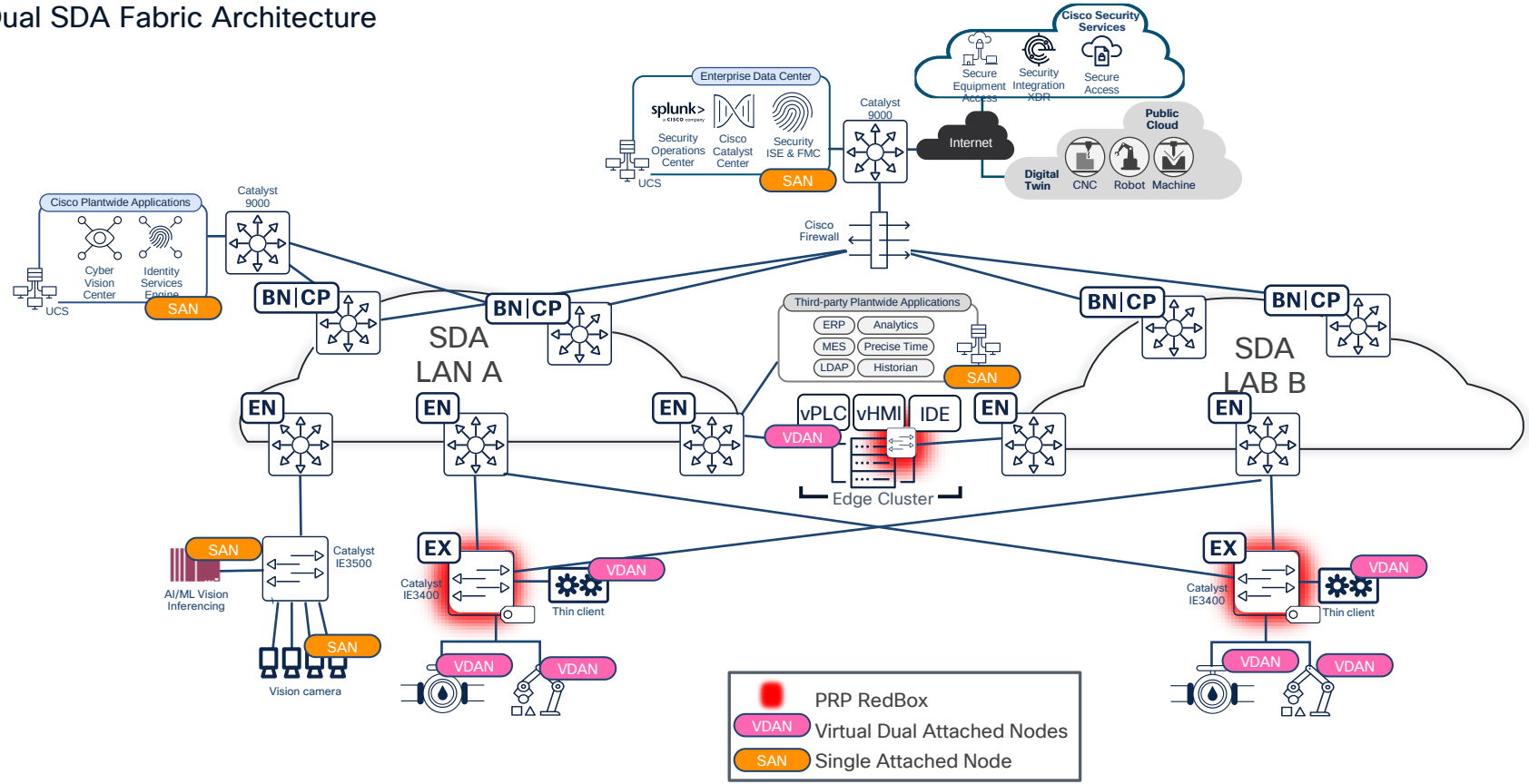
PROFINET Packet Walk

Dual Fabric Approach with PRP



PRP RedBox Placement and Endpoint Representation

Dual SDA Fabric Architecture



LAN-A and LAN-B in SDA: Practical Configuration Details

Fabric Configuration

- LAN A: L3 functionality for critical and non-critical VLANS (L3VNI)

Layer 2 Virtual Network	Associated VLAN ID	Associated Layer 3 Virtual Network	Associated Anycast Gateway
OTCell1091	1091	OT_VN1	10.130.1.1
OTCell1092	1092	OT_VN1	10.130.2.1
OTCell1093	1093	OT_VN1	10.130.3.1

Anycast gateways only in LAN-A

VLAN IDs are identical

- LAN B: L2 only for critical VLANS (L2VNI)

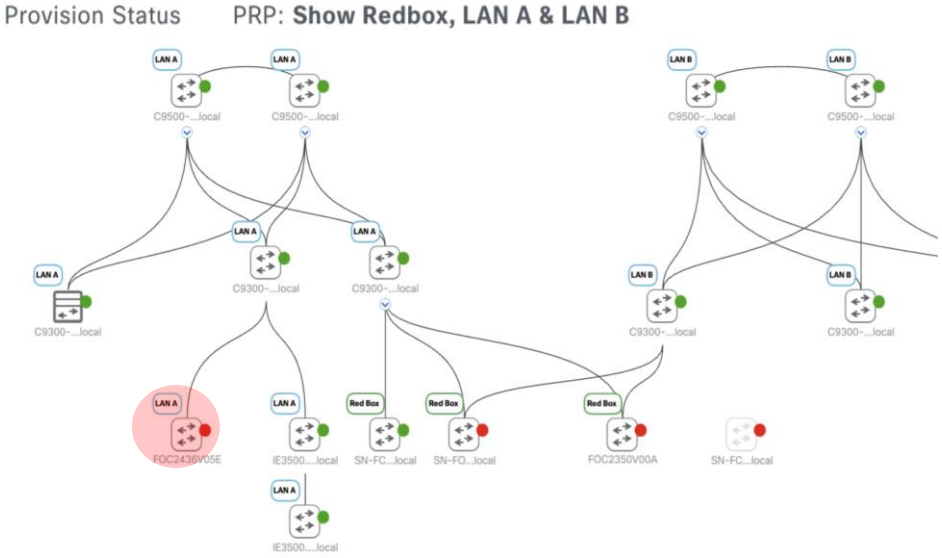
OTCell1091	1091	--	--
OTCell1092	1092	--	--
OTCell1093	1093	--	--

Aha Moment:

- Routing only on LAN A
- Gateways/outside the fabric = SANs.
- PRP protects only VDAN↔VDAN traffic

PRP RedBox Onboarding

IE Onboarding



Best Practice:

- For broadcast domain: use workflow option to prune VLANs in PRP trunk
- For scale: use PRP VLAN aware feature to limit number of nodes learned on node table

1. **Connect to Fabric A only**
   Physical connection to first fabric switch only

⚠ **WARNING: LOOP HAZARD**
Never connect both links before configuration!

2. **Complete PEN onboarding**
   Check PEN is added to LAN A

3. **Configure PRP Settings**
   Catalyst Center SDA Workflow

4. **Connect to both fabrics**
   Plug in the redundant link to Fabric B

5. **Verify Redundancy**
   Confirm seamless failover capabilities

Factory 3 – “A Factory Where Some Applications Need to Move”

SDA READINESS ASSESSMENT FORM

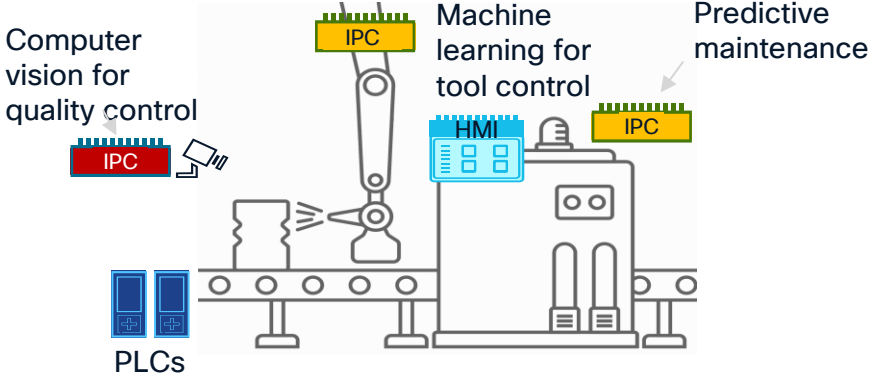
- ☐ Is IT/OT shared network infrastructure a requirement?
  - ☑ Yes ☐ No
- ☐ Is intent-based configuration required?
  - ☑ Must-have ☐ Nice to have
- ☐ Is VLAN stretching across areas a requirement?
  - ☑ Yes ☐ No
- ☐ Is there strong collaboration between IT and OT?
  - ☑ Yes ☐ No

ASSESSMENT SUMMARY

- ☑ Requires L2 overlay to support vPLC workloads
- ☑ IT for OT team created to support architecture
- ☑ Segmentation is a key requirements

Audi Use Case – The case for Virtualization

Edge Cloud 4 Production (EC4P)



> *"We will be adding more and more compute into our infrastructure and that will cause a **maintenance nightmare if we don't do something different**."*
>
> Dr. Henning Loeser, Head of Audi Production Lab, Audi AG

Complex & Costly

- Proprietary hardware
- Long lead times
- Hard to troubleshoot

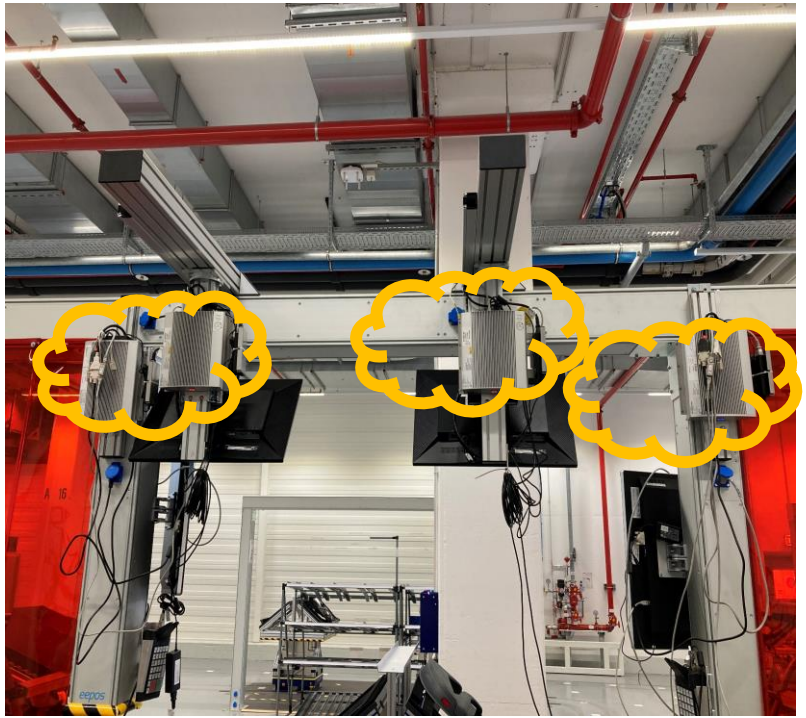
Security Risk

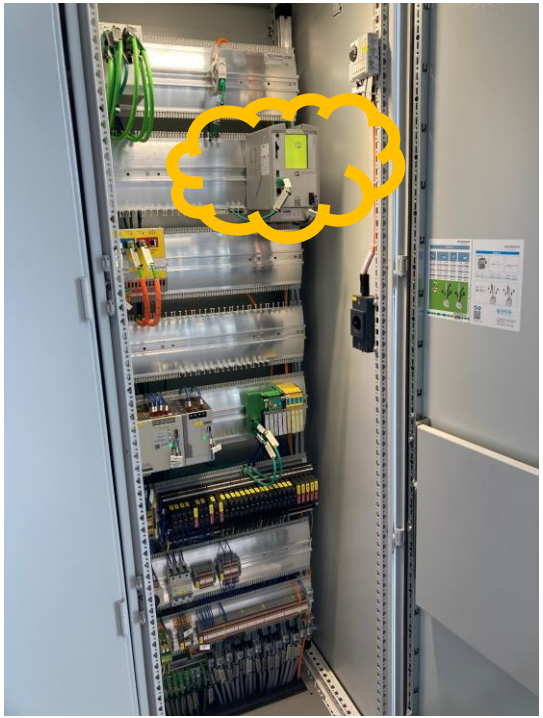
- Updates require downtime
- Delayed patching increases exposure

Inefficient

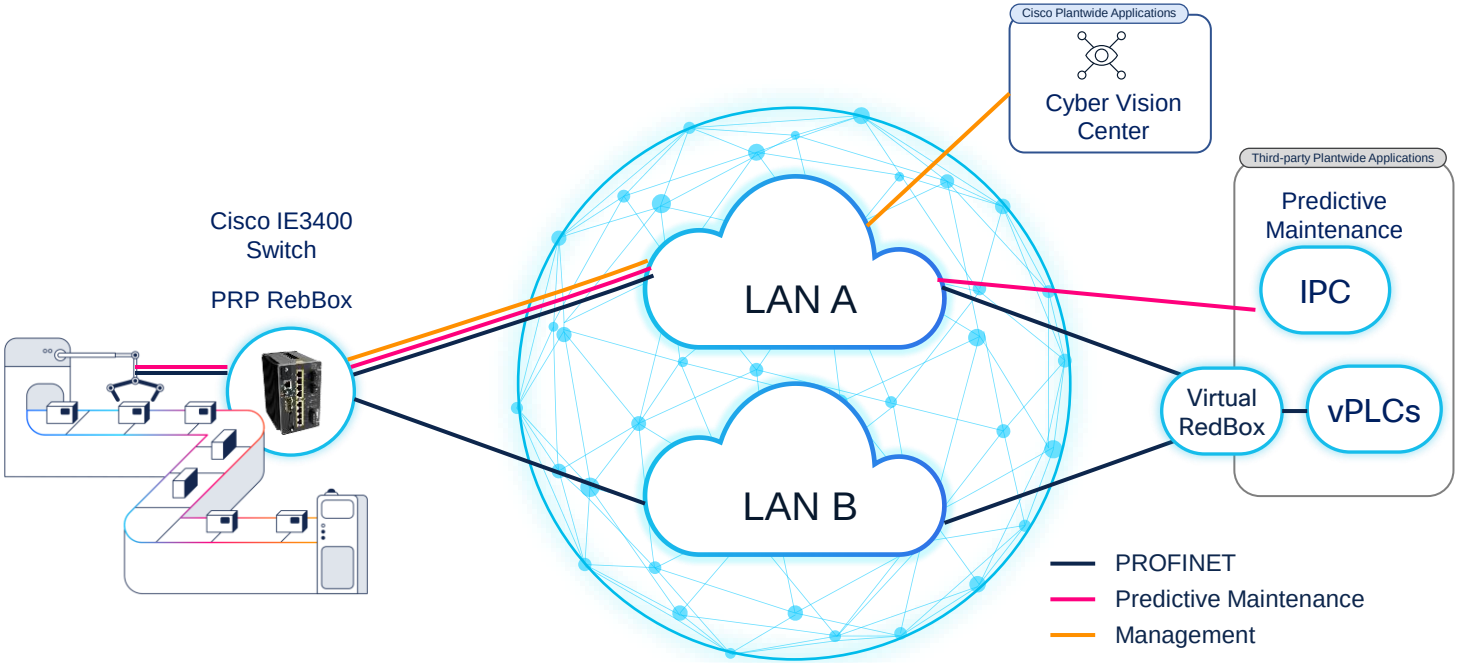
- Extra compute and energy use
- Harder to meet sustainability goals

A Look into Audi's Factory – Towards Virtualization





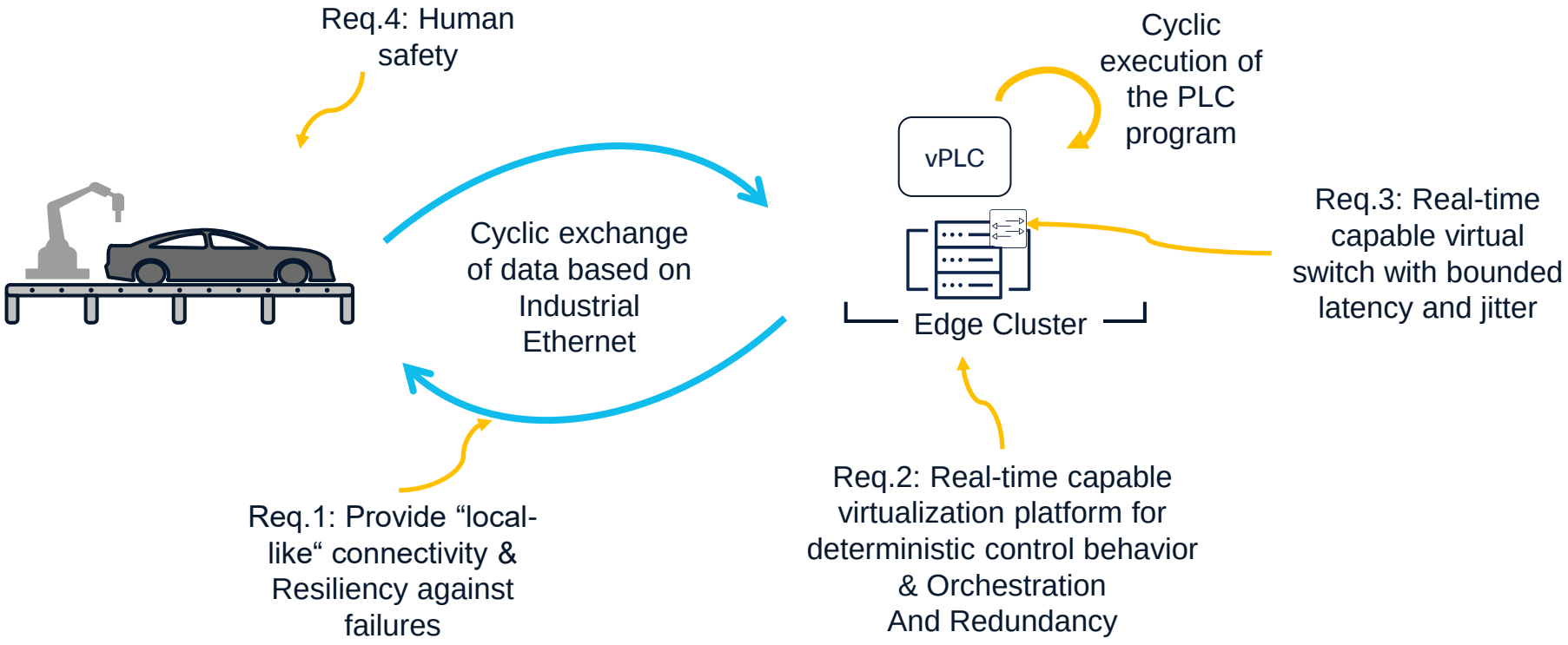
EC4P Simplified Architecture view



Network spanning industrial, enterprise, and data center (6-10 km, <100us)

✓ End-to-end security ✓ Consistent management & observability tools

Architecture Components & Requirements



The Network as the Nervous System of the Factory

See More, Fix Faster, Stay Secure

- Unlock operational efficiency by transforming your network into a sensor for complete visibility and proactive defense.

01

Comprehensive Visibility

Full view of devices, communication patterns, and traffic anomalies across the entire infrastructure.

The network becomes your "eyes and ears"—eliminating blind spots completely.

02

Smarter Troubleshooting

Proactively detect configuration issues and performance bottlenecks before downtime strikes.

Pinpoint errors to resolve root causes—no more finger-pointing.

03

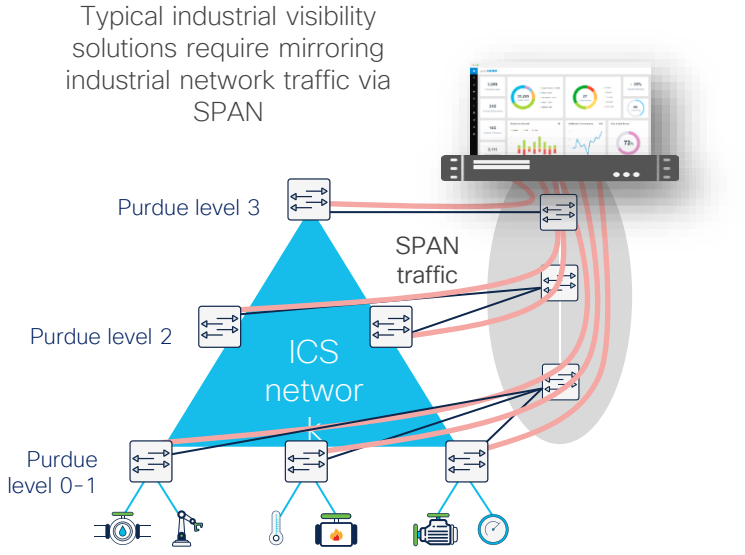
Enhanced Security

Identify all connected devices and automatically assess their vulnerabilities in real-time.

Use the network as a sensor to stop anomalies—no extra devices needed.

Cyber Vision

Alternative OT visibility solutions can’t scale because of high cost of implementation



- An order of magnitude **more assets** in OT than typically found in IT
- Traffic mirroring for visibility requires out-of-band collection switches and **expensive** cabling
- IT unwilling to deploy and maintain **high OpEx SPAN** based solution selected by CISO

Cyber Vision helps gain comprehensive visibility at scale

OT visibility built in, not bolted on

- Visibility sensor is a software feature running in switches and routers
- No additional appliances needed
- No out-of-band collection network needed
- Active discovery requests see pass NAT
  and firewall boundaries

Deep Packet Inspection & Active Discovery
built into your network infrastructure

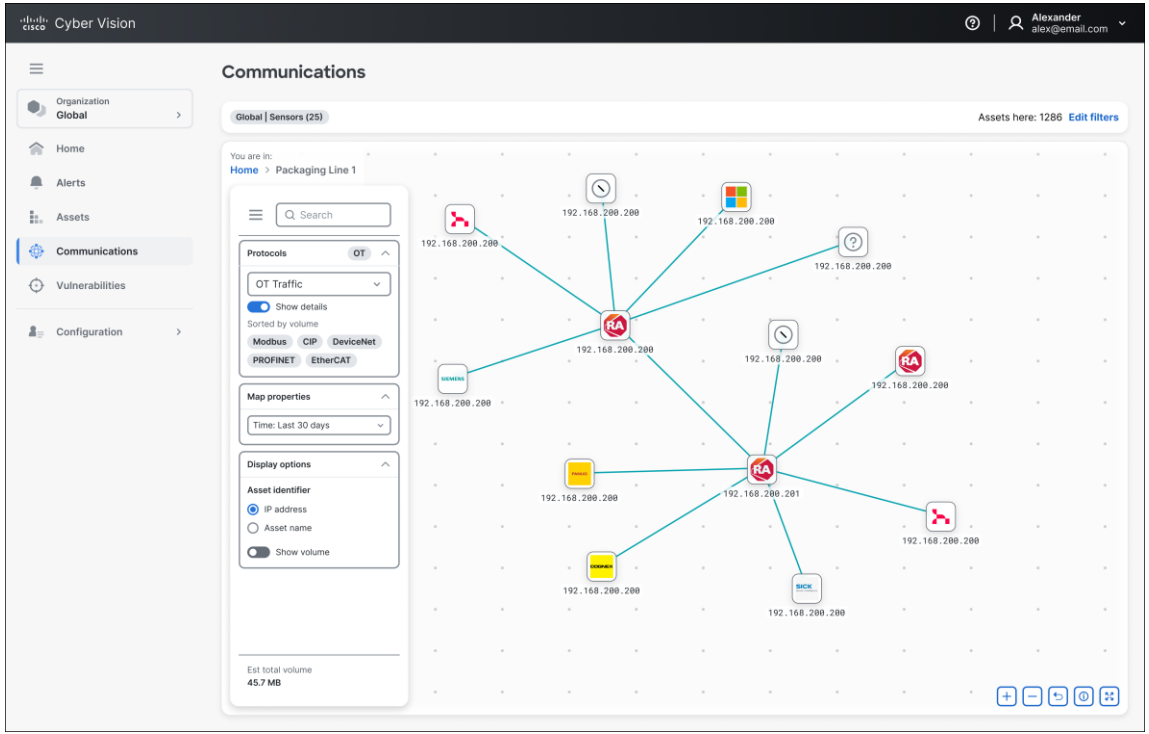
Cisco Cyber Vision

Visibility & Security Platform for the Industrial IoT

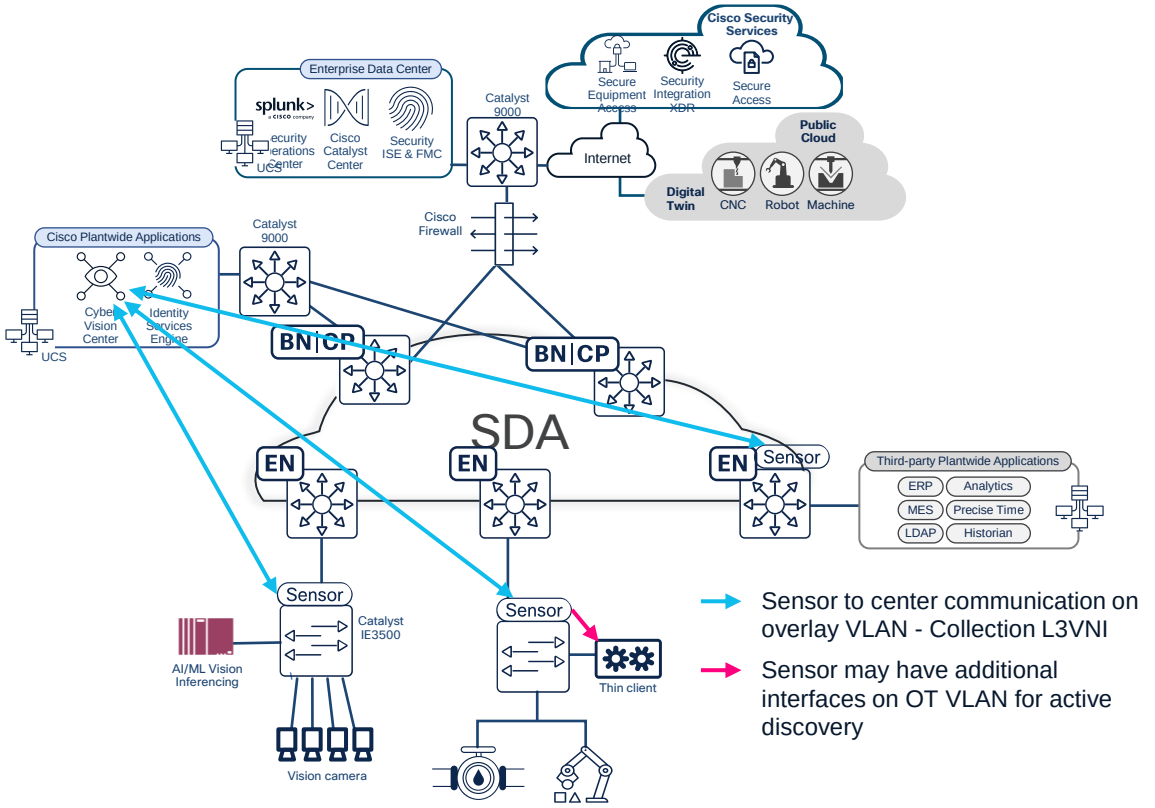
Visibility

Security Posture

Zone Segmentation



Add Visibility to the OT Network with Cyber Vision – SDA



- Cyber Vision Center is deployed outside the SDA Fabric
- Cyber Vision sensors may be deployed in fabric edge nodes (Cat9300, IE9300)
- Cyber Vision sensors on extended nodes/non-SDA IE switches (IE9300, IE3500, IE3400, IE3300)
- Cyber Vision sensors are deployed in the overlay using Cyber Vision Management extension

Sensor Deployment on Fabric Edge: Configuration Example

CLI or Template Configuration

1. Enable iox

```
C9300#format usbflash1: ext4
C9300#config t
C9300(config)#iox
```

2. Configure capture interface VLAN

   This IP is local to the switch and not routed, used for ERSPAN only

```
C9300(config)#vlan 2
C9300(config-vlan)#int vlan 2
C9300(config-if)# ip address 169.254.1.1 255.255.255.252
C9300(config-if)#no sh
```

3. Configure AppGigabitEthernet interface as trunk

```
C9300(config-if)#interface AppGigabitEthernet1/0/1
C9300(config-if)#sw mode trunk
C9300(config-if)#
```

4. Configure Monitor Session

   Define which traffic is sent to the sensor, use VLANs or interfaces

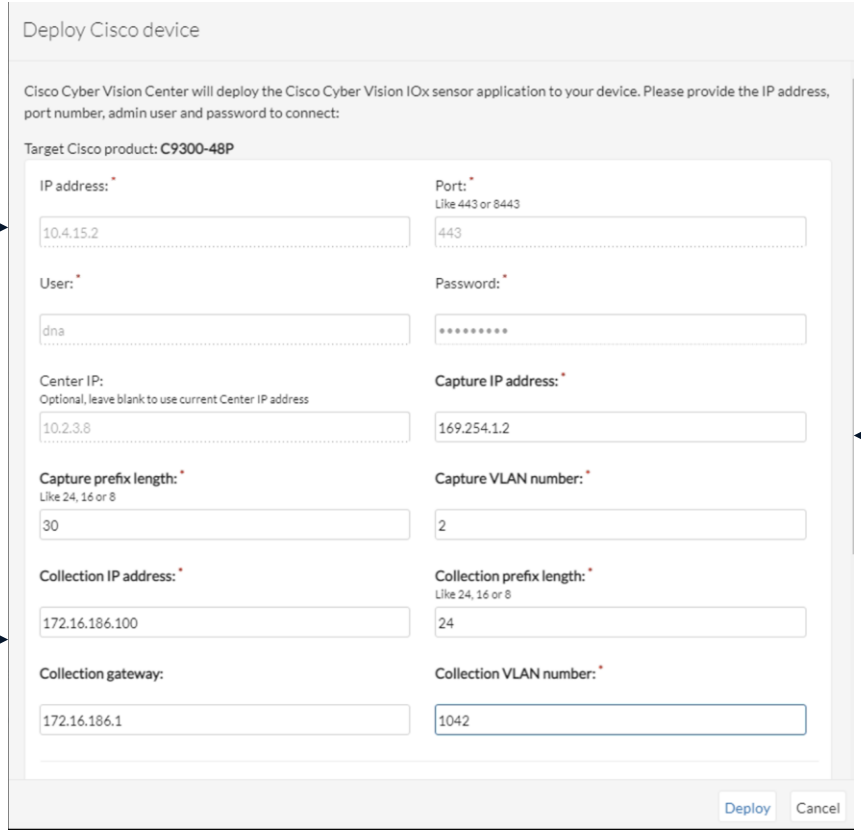
```
C9300(config-if)#monitor session 1 type erspan-source
C9300(config-mon-erspan-src)#source interface Gi1/0/1 - 2 both
C9300(config-mon-erspan-src)#no shutdown
C9300(config-mon-erspan-src)#destination
C9300(config-mon-erspan-src-dst)#erspan-id 2
C9300(config-mon-erspan-src-dst)#mtu 9000
C9300(config-mon-erspan-src-dst)#ip address 169.254.1.2
C9300(config-mon-erspan-src-dst)#origin ip address 169.254.1.1
C9300(config-mon-erspan-src-dst)#end
```

Sensor Deployment via Cyber Vision Management Extension

FE Loopback interface and credentials

Collection IP must match an IP pool configured for the fabric.

Use anycast gateway as collection gateway

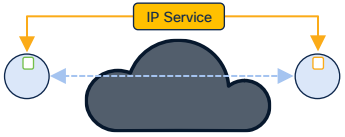


Capture interface and VLAN

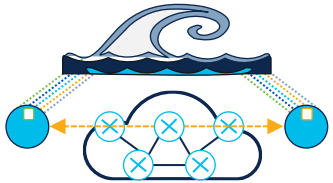
Must match configuration via template

Cisco Provider Connectivity Assurance - how to measure with microsecond precision

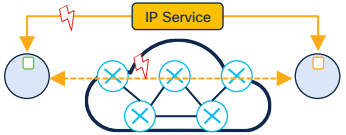
It all starts with visibility and the ”right” data and insights



How is the network performing?
Is my service healthy?



How is the quality of experience?
Is my service meeting SLAs?

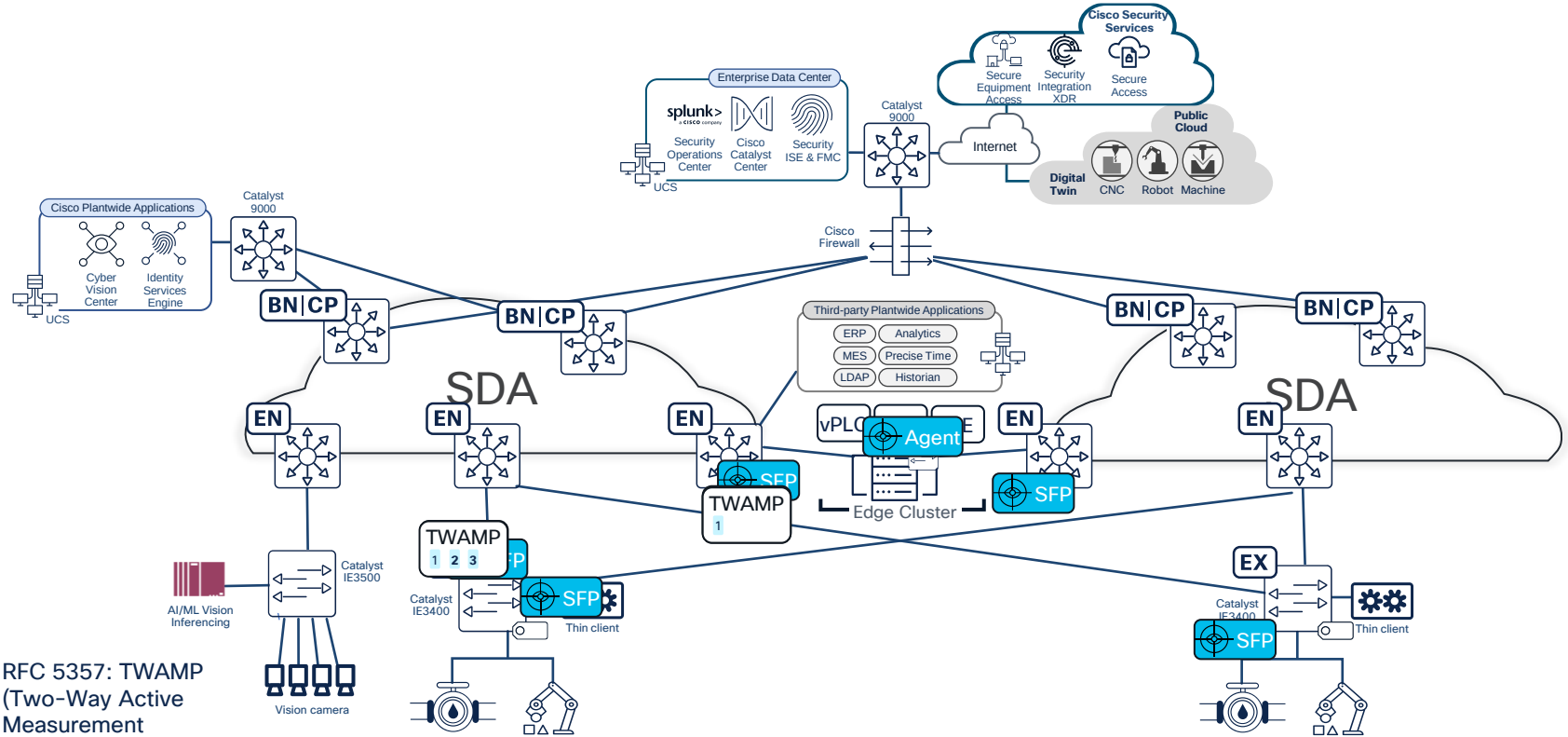


Service is degrading!
Where is the problem?

Challenge	Requirement	How
Visibility	Network and end-to-end service visibility	Continuous real-time monitoring with precision
Insight	Actionable service quality insight	Performance, telemetry and device data is correlated, analyzed and visualized
Action	Take remedial actions and drive efficiencies	Enriched insight feeds into orchestration and automation platforms

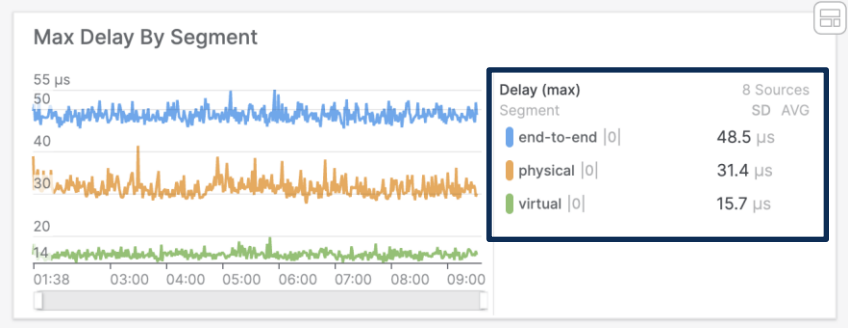
Monitoring Network Performance

Leveraging TWAMP with Cisco Provider Connectivity Assurance

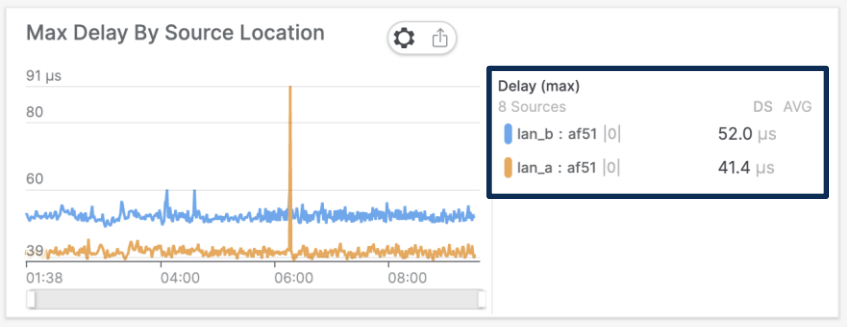


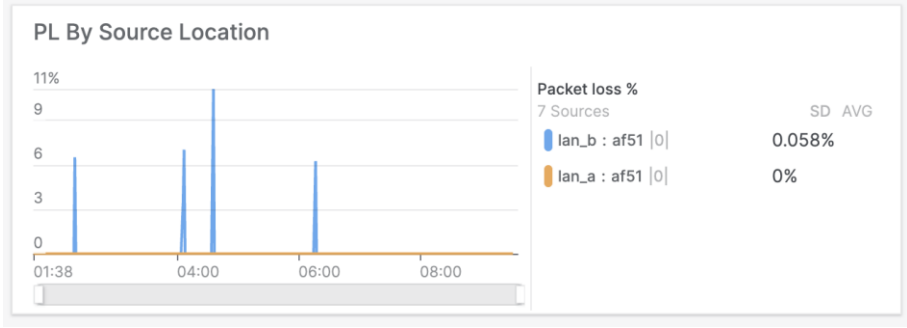
RFC 5357: TWAMP (Two-Way Active Measurement Protocol)

Assurance reporting and analytics



- Identify performance issues affecting critical traffic
- Compare latency, jitter, and loss across traffic types
- Visualize network behavior with contextual insights
- Use metadata to understand traffic intent





Overcoming Industrial Network Challenges

#1 Prioritizing Critical Traffic

Scenario: Auto manufacturer is sending mission critical traffic through a converged IT/OT infrastructure.

The Challenge: Enterprise and other traffic can interfere with PROFINET traffic

The Solution: Prioritize PROFINET traffic in low latency queues

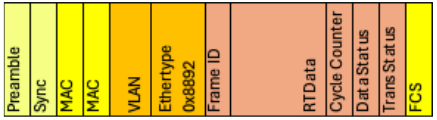
Key Feature: Quality of Service

Quality of Service

Templates are used to deploy this configuration

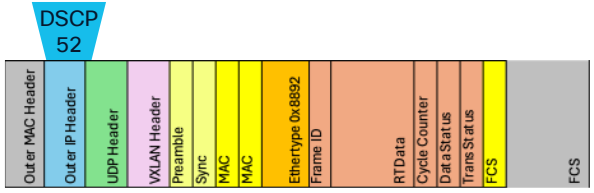
1. QoS in the industrial switch prioritizes PROFINET EtherType.

2. Frame gets classified based on EtherType (0x8892) and mapped to a custom DSCP value (i.e., 52)



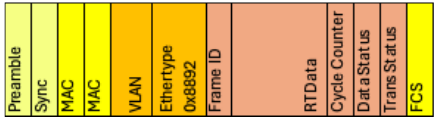
PROFINET Frame

3. Custom DSCP value is added to VXLAN header



PROFINET frame encapsulated in VXLAN

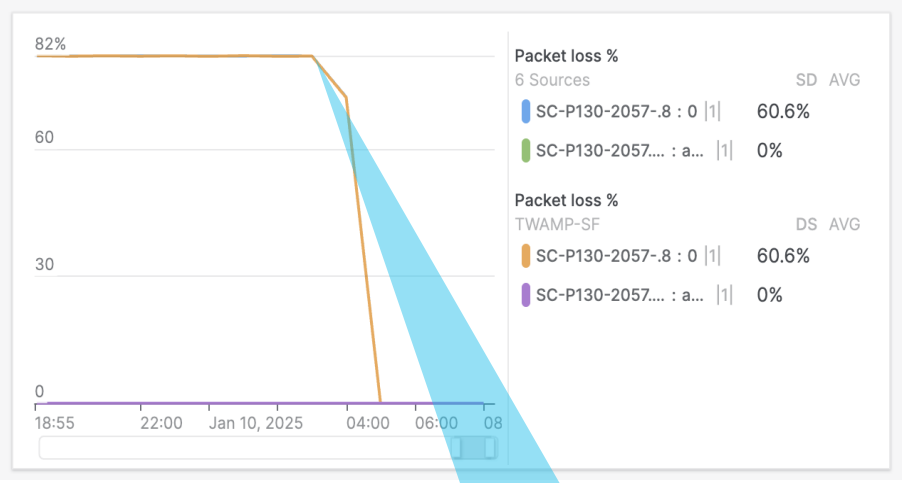
4. Packets with the custom DSCP value 52 are put in a priority queue



PROFINET Frame

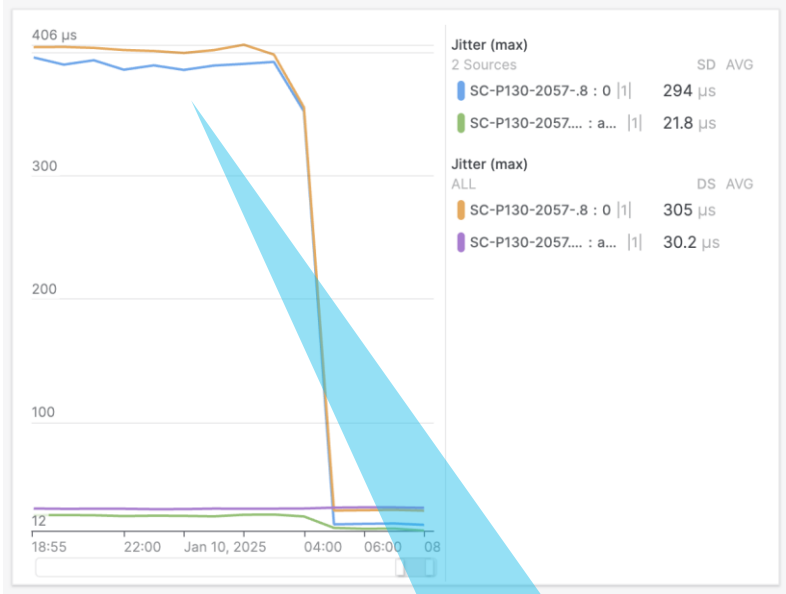
5. The DSCP value is used to mark the frame before removing the VXLAN encapsulation. Frame is put in a priority queue at egress.
COS 6 is re-added to the frames.

Monitoring QoS with Provider Connectivity Assurance



Congested Network

Priority traffic has 0% loss, even in highly congested scenario where other classes have 82% loss



Congested Network

Jitter for priority traffic is <32μs. Jitter for other classes has a max of 406μs during congestion

#2 Segmenting The Network

Scenario: Bob, a Nullbyte Ventures employee, connects to the network using a compromised laptop. This puts the network at risk.

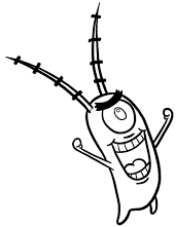
The Challenge: a compromised device has the potential to affect the whole network

The Solution: Create micro segmentation policies to contain threads to a small area

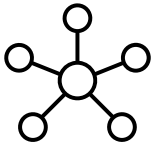
Key Technology: TrustSec

A well-tailored email causing a user to click....

Which goes to a questionable website....



Which downloads malware to the users' machine....



Who connects into the OT network ....

Which causes unusual activity in the OT.... Puts Nullbyte Ventures at risk

OT Segmentation Differences from Campus Networks

Zone-Based Segmentation Adequacy:

Segmentation within a zone is typically unnecessary and availability is a priority.

IEEE 802.1X Limitations in OT Devices:

Most OT devices lack support for IEEE 802.1x, and profiling accuracy is often limited.

Process-Centric Privilege:

Privilege levels in OT scenarios are often tied to processes or locations rather than device types.

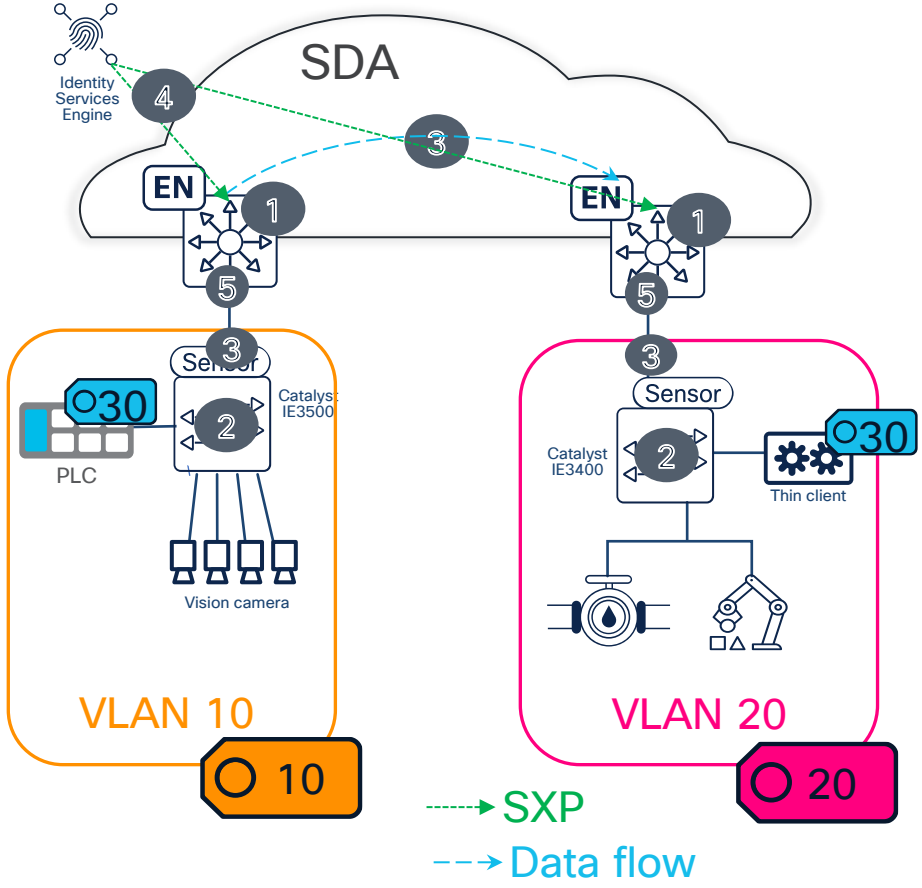
OT Endpoints and VLANs:

OT endpoints cannot be moved to another VLAN; they often use static IP addressing.

TrustSec Variability in OT Networks:

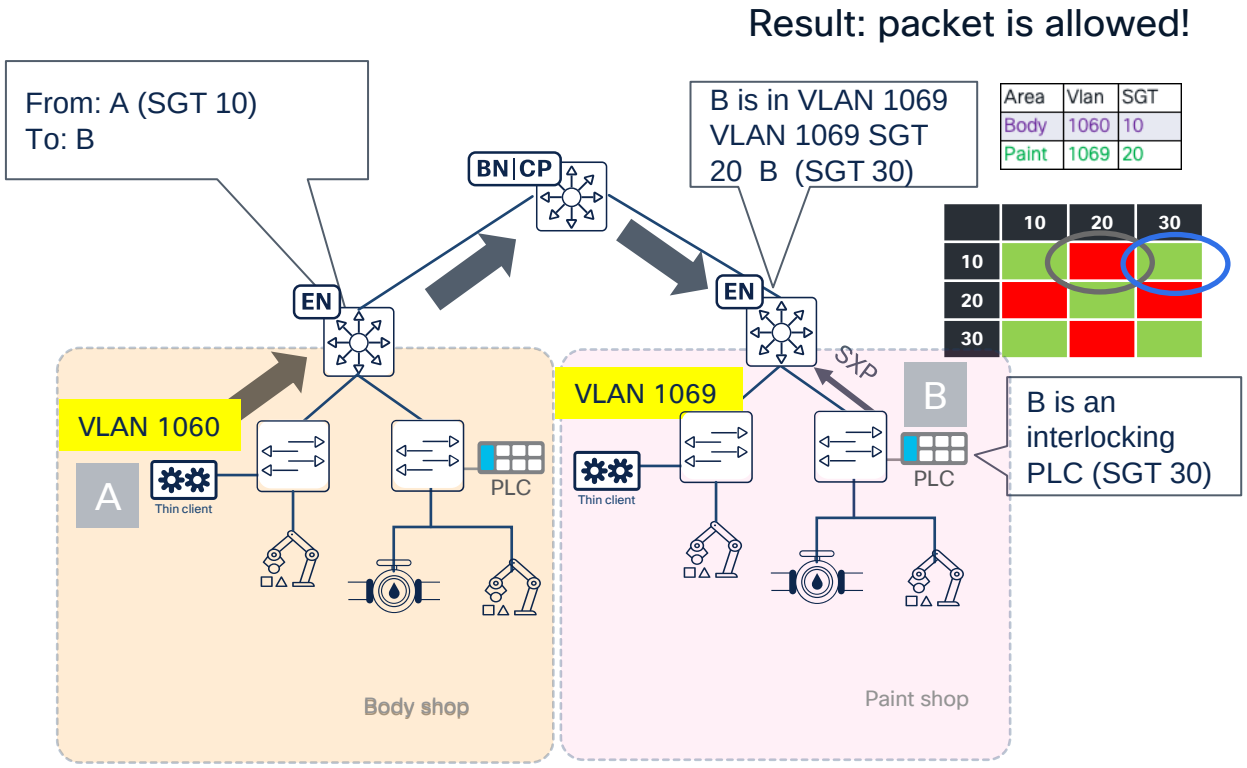
Industrial switches in cell area zone may not have full TrustSec support.

Classification, Propagation and Enforcement for OT



1. Classification is static for most endpoints. (i.e. VLAN 10 > SGT 10)
2. Classification is dynamic for some endpoints at authorization (i.e. interlocking PLC > SGT 30)
3. Source SGT is propagated on data plane
4. Destination SGTs need to be propagated to enforcement points to avoid incorrect enforcement (i.e. Fabric edge needs to know interlocking PLC is SGT 30)
5. Policies are enforced on egress port at egress of fabric edge

What if the Destination Has a Dynamic Tag?



- SXP propagation is required when enforcement is not at the access & dynamic authentication is used. Needed for enforcement device to learn about destination tag
- SXP can be from ISE to FE (centralized) or from access switch to FE (distributed)
- SXP is configured via templates

#3: Integrate Machines with Duplicated IPs

Scenario: Machines arrive with duplicate IP ranges

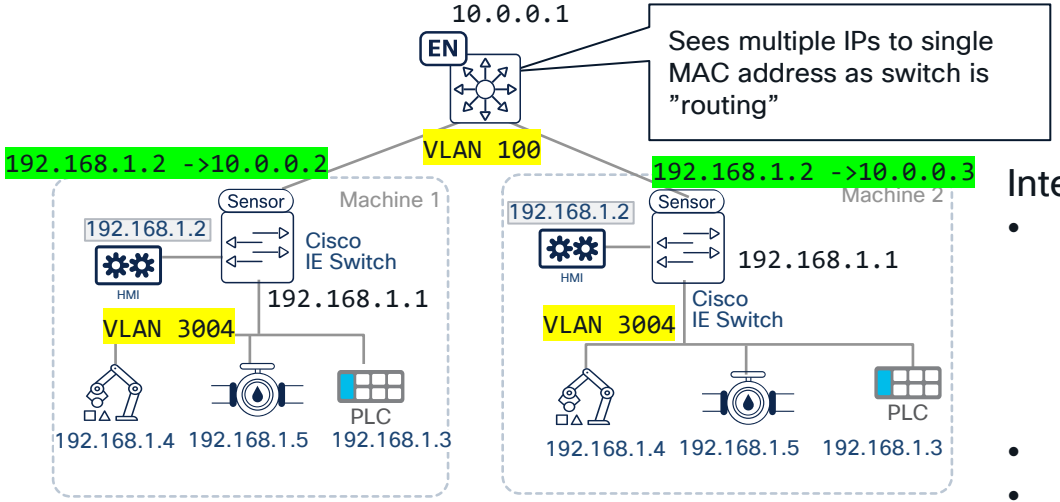
Challenge: They must coexist on the same network

Solution: L2NAT on Cisco IE switches

Key Feature: Catalyst Center “multiple IP-to-MAC” support

Multiple IP to MAC Address Example

L2NAT with inter-VLAN routing



Inter-VLAN routing:

- Eliminate machine to machine Broadcast:
  - Different VLAN ‘inside’ from ‘outside’
  - VLAN 3004 inside machine
  - VLAN 100 outside machine
- IE switch ‘routes’ between VLANs.
- IE switch is L3 GW for 192.168.1.x

- Configure multiple IP to MAC address in IP pool to support L2NAT with Inter-VLAN routing **(To comply with SISF policy)**
- Host behind the NAT can present as silent in the fabric until they have routed communication (more on this later)
- NAT support:
  - IE3105, IE3300, IE3400: Support Layer 2 NAT with or without inter-VLAN routing
  - IE9300, IE3500: Support Layer 2 NAT (without routing) and Layer 3 NAT

#4: Empowering OT with Catalyst Center

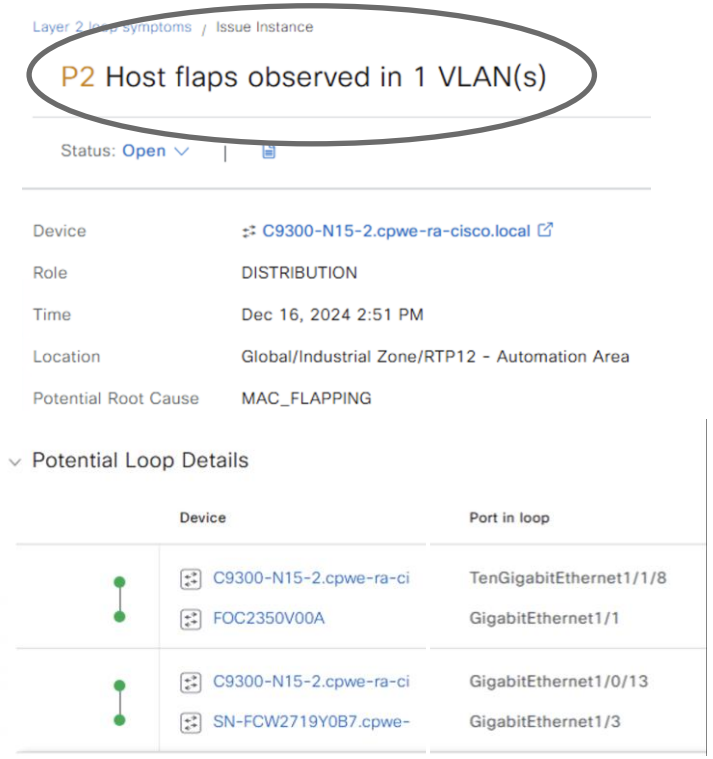
Scenario: Production stops; the root cause is unclear

Challenge: Operator assumes a switch failure and replaces it

Result: Unnecessary downtime and delays

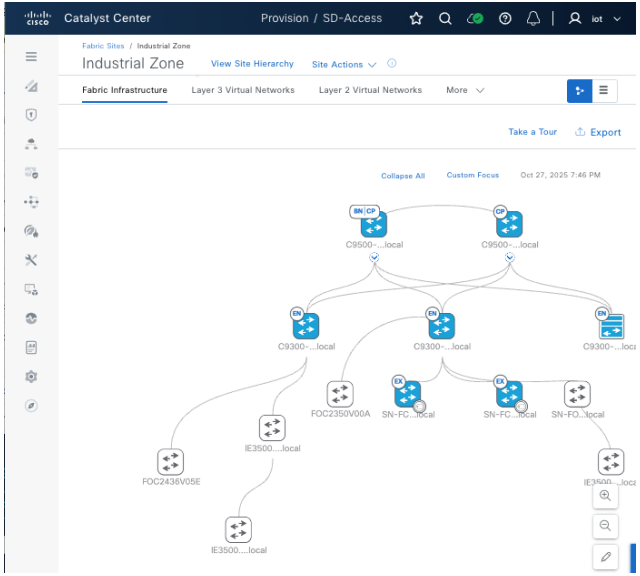
Solution: Catalyst Center Assurance pinpoints the real issue—a network loop

Key Feature: Site-based RBAC gives OT safe visibility and insights

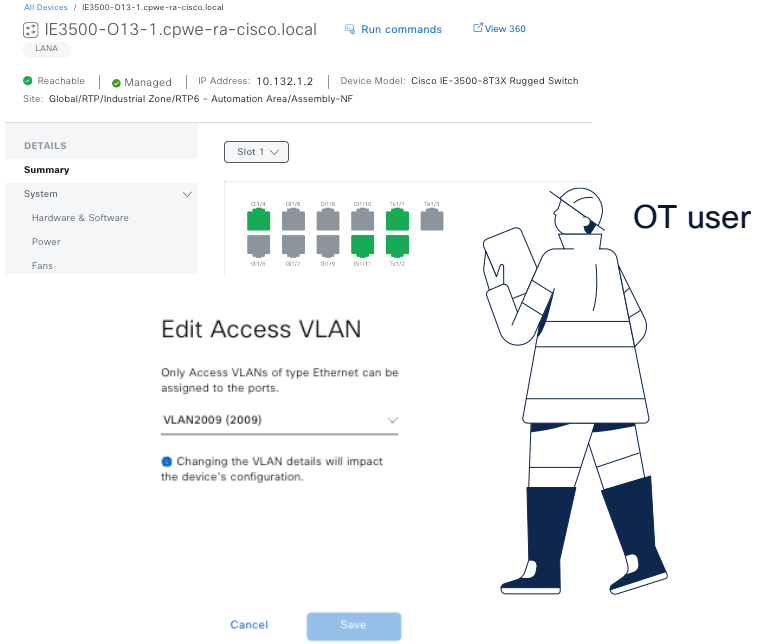


Catalyst Center Enables Safe Collaboration with Site Based RBAC

IT & OT Teams can safely work in the same Catalyst Center instance.



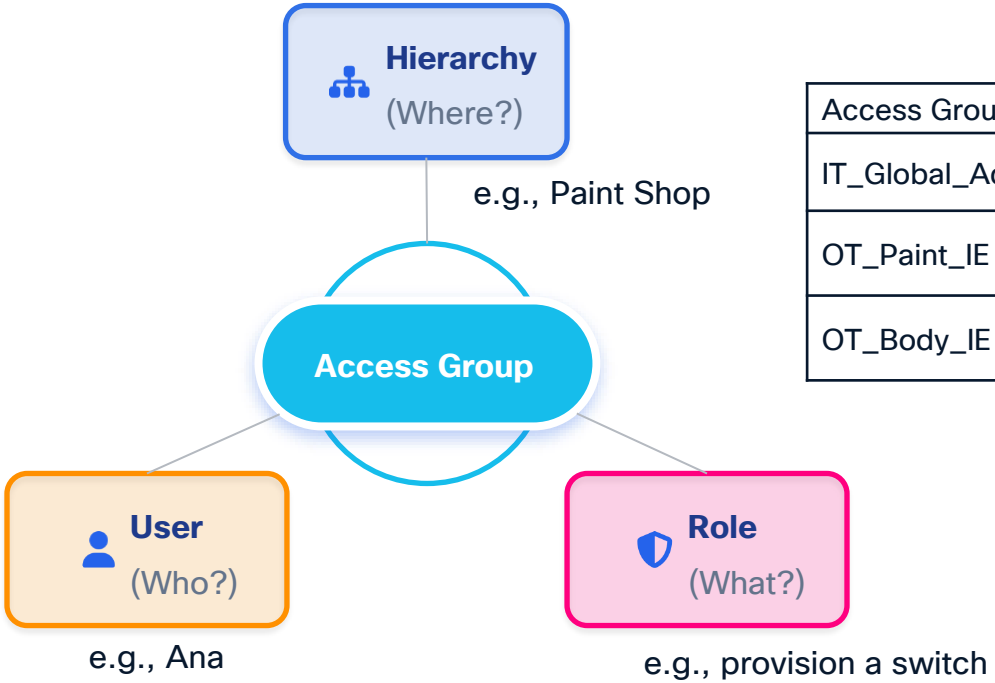
IT user



OT user

Making RBAC Site-Aware

The Access Group glues together who you are, what you can do, and where you're allowed to do it.



Access Group	Role	Site Scope	User
IT_Global_Admin	Network Admin	Global	Alex_IT
OT_Paint_IE	OT Network Operator	Paint Shop	Ana_OT
OT_Body_IE	OT Network Operator	Body Shop	Ben_OT

Example workflow

Alex

IT Network Admin

Designs SDA fabric

Onboards new switches, upgrades software

Monitors performance across all sites (Global View)

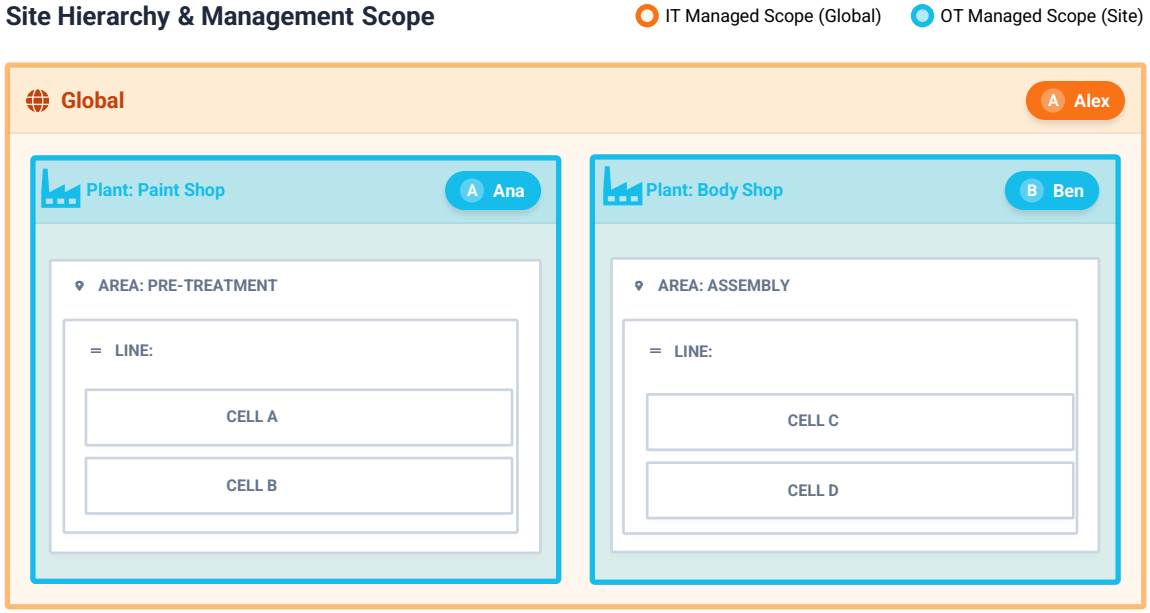
Ana & Ben

OT Engineers

Configure access ports on IE switches via Catalyst Center

Enable/disable ports for maintenance activities

View assurance data for their specific plant/area only



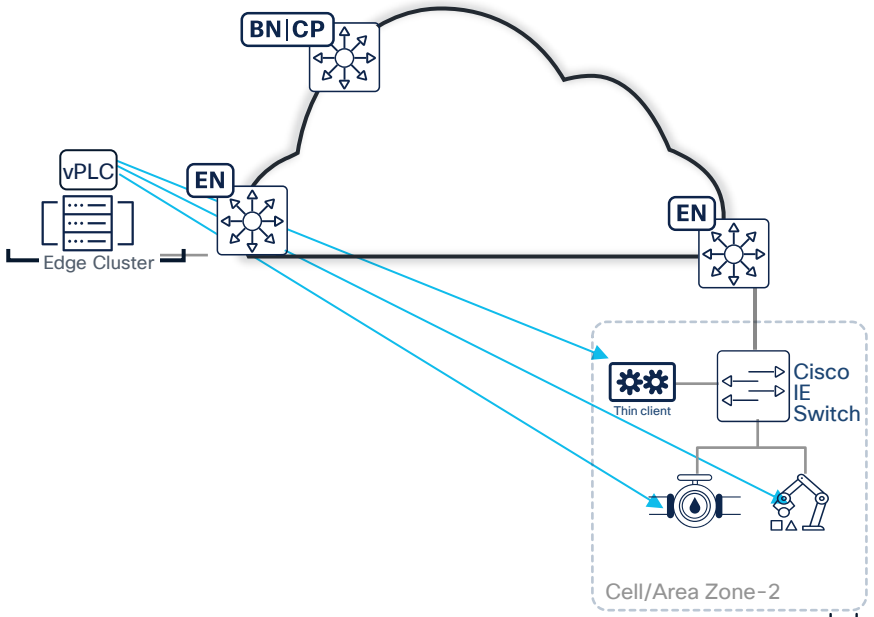
#5 Enabling Multicast Traffic Over SDA

Scenario: vPLCs send Discovery and Basic Configuration Protocol (DCP) multicast packets to discover and identify PROFINET devices

The Challenge: multicast is not forwarded by default on SDA fabrics

The Solution: enable multicast forwarding on the OT VLAN

Key Catalyst Center Feature: Layer 2 flooding



Layer 2 Flooding

Default Behavior: Broadcast, Unknown-Unicast, and Link-Local Multicast traffic are not forwarded.

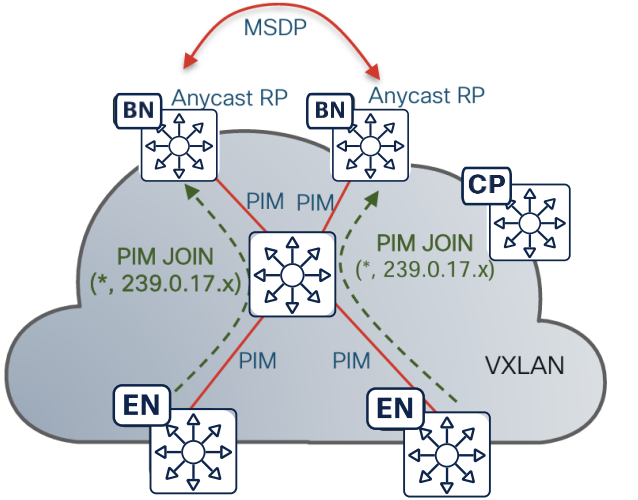
Solution: L2 Flooding encapsulates subnet broadcasts in an underlay multicast group (239.0.17.x).

How It Works:

Edge nodes subscribe to the underlay multicast group.

Underlay PIM ASM builds the multicast distribution tree.

Use Cases: Silent hosts, Layer 2 handoff, and Layer 2 Fabric require L2 Flooding.



Edge nodes configured with Anycast RP rp-address

```
instance-id 8203
  remote-rloc-probe on-route-change
  service ethernet
   eid-table vlan 2223
   broadcast-underlay 239.0.17.1
   flood unknown-unicast
   database-mapping mac locator-set rloc_xxxx
   exit-service-ethernet
```

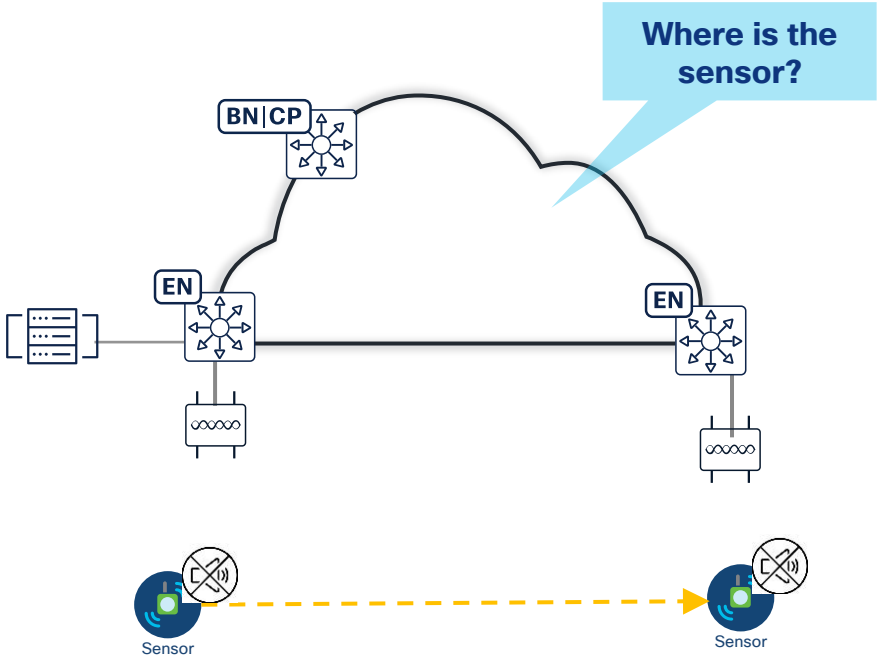
#6 Dealing with Silent Hosts

Scenario: Static-IP sensors stay silent on the network

Challenge: The fabric cannot locate or onboard them

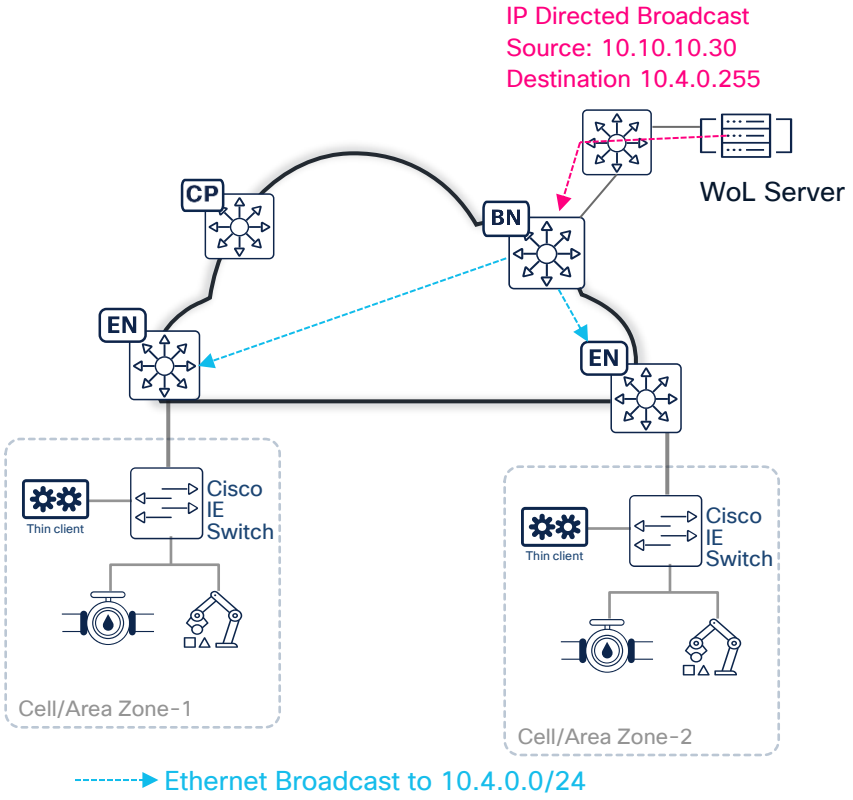
Solution: Trigger responses from the endpoints

Key Feature: IP Directed Broadcast



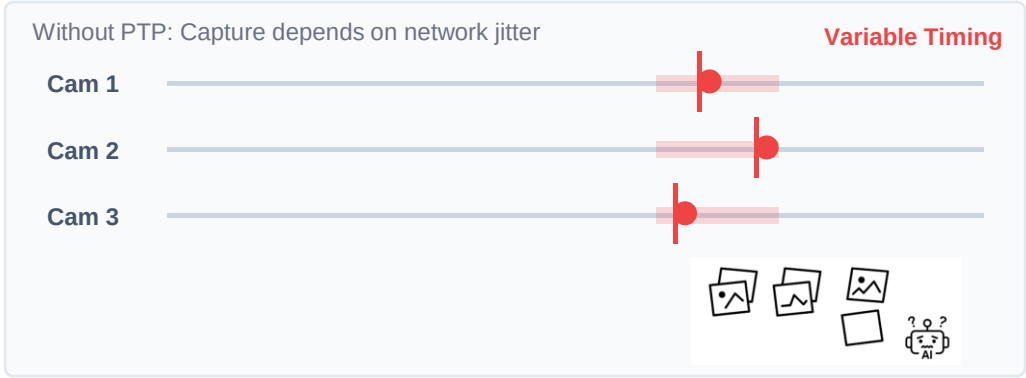
IP Directed Broadcast Use-Case

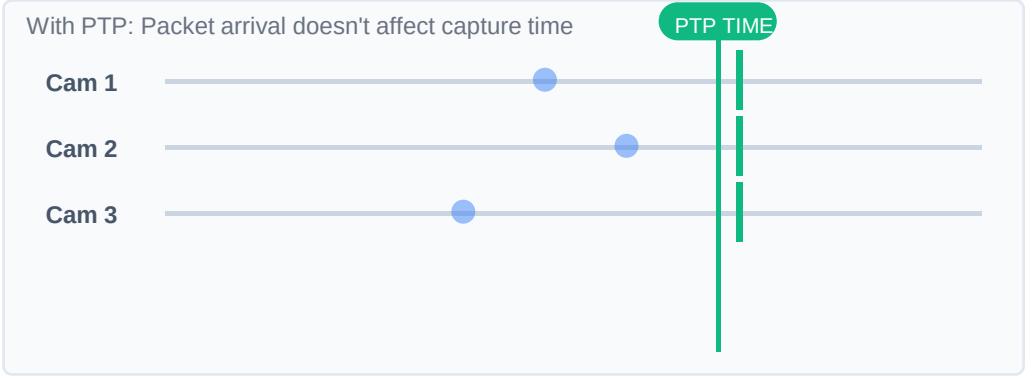
- Devices that stay idle **become invisible** to the fabric
- Without traffic, their location remains **unknown**
- **Directed broadcasts** bring silent endpoints online
- Border Nodes convert **IP Directed Broadcast** to Ethernet broadcast for Wake-On-LAN
- **Remember the L2NAT case:** endpoints in a different uplink VLAN may stay silent – this feature wakes them up



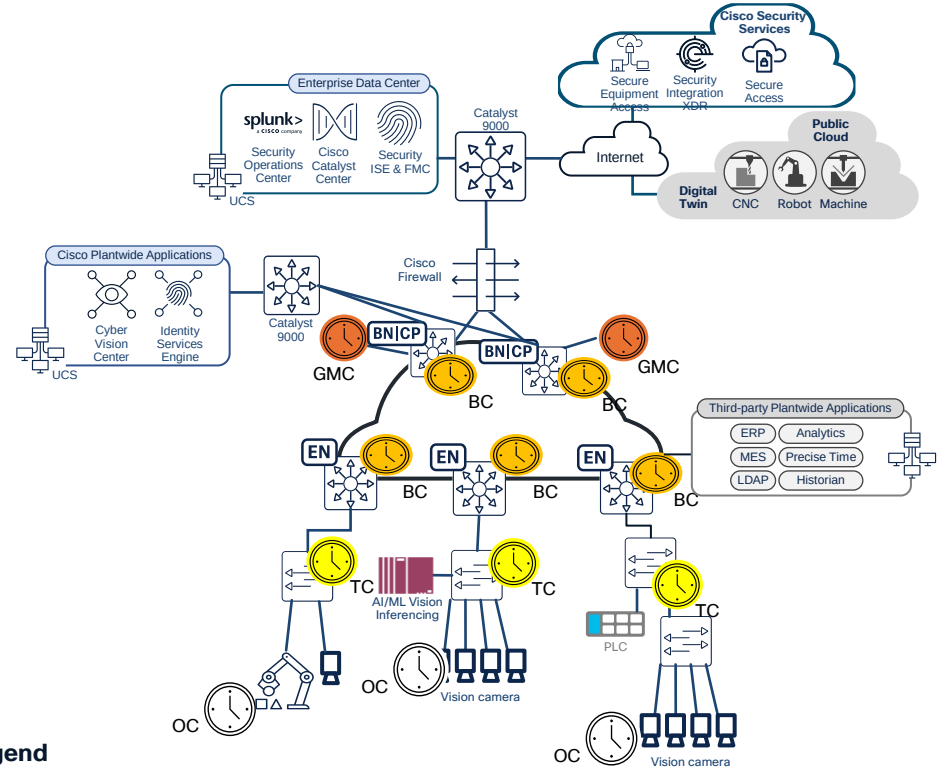
#7 Dealing with Time-Critical Workloads

- **Scenario:** Multi-camera vision systems require precise, synchronized capture
- **Challenge:** Without common understanding of time, images cannot be processed
- **Solution:** A common fabric-wide time reference
- **Key Feature:** PTP





PTP in SDA Fabric



Legend
- **GM** – Grandmaster Clock
- **BC** – Boundary Clock
- **TC** – Transparent Clock
- **OC** – Ordinary Clock

- Runs globally on fabric nodes (BN/CP/EN) using Boundary Clock mode.
- Operates in the underlay (L3) — never across the VXLAN overlay.
- Fabric = Boundary Clocks; IE switches = Transparent / Ordinary Clocks.
- PTP is propagated to access VLAN at the SDA Edge.
- Validated with observed offset ~100ns
- Default PTP profile only, not verified in dual-fabric topology

When deploying PTP check hardware support and feature interaction

PTP Configurations on Network Devices

Reference Slide

Border/Control Node (Boundary Clock with L3 uplink to GM):

```
interface TenGigabitEthernet1/0/33
no switchport
ip address 10.254.1.137 255.255.255.252

ptp transport ipv4 udp
ptp mode boundary delay-req
ptp priority1 100
ptp priority2 101
```

Border/Control Node (Boundary Clock with L3 uplink to GM):

```
ptp vlan 120
! Default to E2E Transparent mode
```

Edge Node (Boundary Clock + VLAN propagation on access port):

```
ptp transport ipv4 udp
ptp mode boundary delay-req
ptp priority1 102
ptp priority2 103

!On access Interface
interface GigabitEthernet1/0/10
 switchport
 switchport mode access
 switchport access vlan 120
 ptp vlan 120
```

Tips:

- The following configurations help with stability :

```
ptp utc-offset 37

time-property persist infinite
```

- Always check platform dependent PTP support

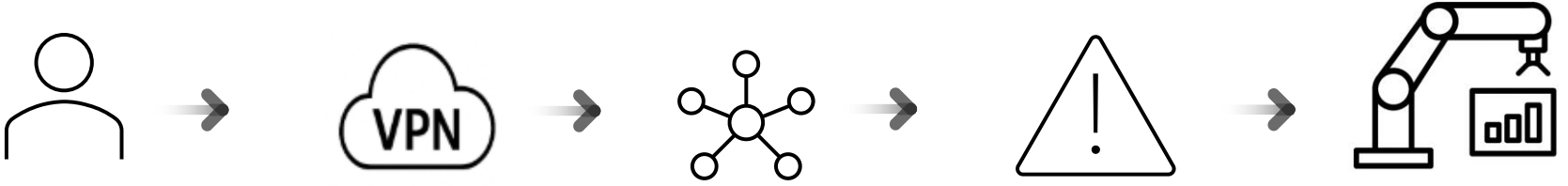
#8 Providing Secure Remote Access to OT Assets

Scenario: machine builders need remote access to machine for troubleshooting

The Challenge: traditional OT remote access methods create **security gaps** (VPN overreach, ad-hoc tools, cellular gateways). IT requires **zero-trust control**, while OT needs **simple, per-asset access**.

The Solution: deploy Cisco Secure Equipment Access **(SEA)**

Key Feature: SEA application for industrial switches and Catalyst9300



A remote machine builder initiates access...

...using traditional VPN or ad-hoc remote access methods...

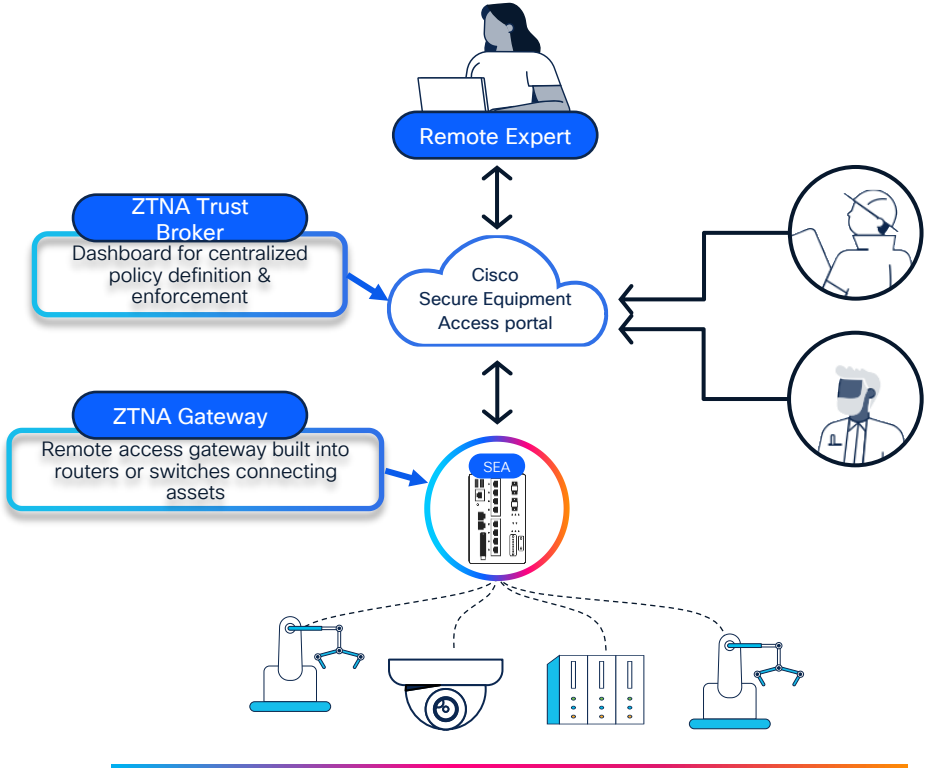
...which unintentionally gives reach into the OT network...

...increasing the chance of unintended changes or compromise...

...and making PLCs, robots, and machines reachable without zero-trust boundaries.

OT self-service remote access with ZTNA control

- Combined Application: **One appliance provides both visibility (CV) and secure remote access (SEA)–**no extra hardware.
- Multi-Overlay Access: SEA supports **multiple SDA overlays** (VNs/VRFs) to reach different OT networks from a single deployment.
- **Segmented Connectivity**: Each SEA interface maps to a specific overlay for least-privilege, per-zone access (machines, cells, production lines).
- Proxy Architecture: **Cyber Vision Center acts as the SEA proxy**, delivering secure remote access and unified management for OT assets.



One-click zero trust remote access to any OT asset connected to Cisco industrial network

Current Challenges

OT Requirements vs Current SDA Support

Requirement	Current limitation	Available workaround
Tolerance to network outages: 1-100ms	Failure on the underlay may produce outages > 200ms	Dual fabric with PRP
Layer 2 multicast is used for producer/consumer messages	IGMP has not been validated	
Resiliency protocols in industrial networks: PRP, MRP, DLR, HSR, REP	Only REP is supported in Catalyst Center today	Keep L2 resilient topologies outside of the fabric
QoS: Priority queue needs to be reserved for high priority traffic. May need COS values	Application policy is based on enterprise profile and Application policy does not support for COS	Use templates
L2NAT	Not supported by Catalyst Center workflows	Use templates

Closing

New CVD: Dual Fabric Architecture for vPLC and Manufacturing Applications

Modernizing industrial control with dual fabric architecture

Reality in Plants Today

PLCs on Factory Floor

Controllers traditionally deployed **locally near machinery**, increasing hardware footprint.

High Reliability Needs

Control systems **require extremely reliable** and predictable network connectivity.

Centralization Risks

Centralizing PLC logic increases the potential **blast radius** of failures.

What the CVD Changes

Dual Fabric Architecture

Architecture designed to host virtualized PLCs and **preserve Layer 2 connectivity**. (VXLAN component of SDA)

Local-Like Connectivity

Network design delivering **low-latency** performance indistinguishable from local PLCs. (High performance network)

Validated Resiliency

Proven resiliency models designed specifically for virtualized automation systems. (PRP for **zero loss**)

Benefit: adopt virtualization with confidence, reduce downtime, reduce cost

Our Final Thoughts: Enabling the Software-Defined Factory with SDA

01 **SDA supports critical use cases:** Converged IT/OT infrastructure, Layer 2 extension, and PLC virtualization.

02 **Customer-driven deployments**: An SDA deployment depends on unique customer requirements, including OT control traffic localization, operational workflows, and IT/OT infrastructure ownership.

03 **IT and OT collaboration**: Strong collaboration between IT and OT teams is vital for successful SDA deployments.

04 **TrustSec and automation**: While SDA is not required for TrustSec, it simplifies automation and policy enforcement.

Complete your session surveys

Complete your surveys in the Cisco Events App.

Complete a minimum of 4 session surveys and the overall event survey to receive a unique Cisco Live t-shirt.
(from 11:30 on Thursday, while supplies last)

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Visit the Technical Solutions Clinics to discuss your technical questions

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at CiscoLive.com/On-Demand

Contact me at: www.linkedin.com/in/erikafranco/

Internet of Things Learning Maps

Future Proofing Industrial Networks

START

Tuesday, February 10 | 8:00 a.m.
BRKIOT-2115
Fabric Networks for OT: The History (IP MPLS), Today (SD-Access) and Emerging Trends (SRv6 and BGP EVPN)

Tuesday, February 10 | 12:00 p.m.
BRKIOT-2269
A Short History of Time in Industrial Systems - Synchronizing Critical Infrastructure Elements with PTP

Tuesday, February 10 | 3:45 p.m.
BRKIOT-3624
Advanced Techniques for Successful Cellular Connectivity Implementation

Wednesday, February 11 | 8:15 a.m.
BRKIOT-2644
Industrial Connectivity Excellence: When Ultra Reliable Wireless Backhaul Meets WiFi in Action

Wednesday, February 11 | 5:15 p.m.
BRKIOT-2876
A Day in the Life of Marty OT Administrator: Securing, Automating, and Assuring OT Operations with Cisco Catalyst Center

Thursday, February 12 | 8:30 a.m.
BRKIOT-2027
123 URWB: A Wireless Network Engineer's Guide

FINISH

Thursday, February 12 | 4:45 p.m.
BRKIOT-2990
5 Ways to Deploy Scalable , Secure AND Cost Sensitive Industrial IoT Solutions for Customers using Cisco Catalyst SD-WAN

Reimagine your IoT Applications and Use Cases

START

Tuesday, February 10 | 1:30 p.m.
IBOIOT-2114
Redefining Industrial Networking: SRv6 for Utilities and Distributed Automation

Wednesday, February 11 | 9:45 a.m.
BRKIOT-2746
AI at the Industrial Edge: Designing Networks that Deliver

Wednesday, February 11 | 11:15 a.m.
BRKIOT-2720
The Future of Manufacturing: Secure, Reliable, AI-Ready Network Architecture

Wednesday, February 11 | 1:45 p.m.
BRKIOT-2849
Factory-as-Code: Operational Excellence through Industrial Network Automation

Wednesday, February 11 | 3:00 p.m.
IBOIOT-1116
Expanding Cloud-Managed Switching to Ruggedized Environments with Meraki Dashboard

Wednesday, February 11 | 5:00 p.m.
IBOIOT-1117
No Ticket Required: AI-Powered Troubleshooting for OT Networks

Thursday, February 12 | 10:00 a.m.
IBOIOT-1116
Expanding Cloud-Managed Switching to Ruggedized Environments with Meraki Dashboard

Thursday, February 12 | 10:30 a.m.
BRKIOT-2808
Smart and Creative Use Cases of Industrial Networking Technologies

Thursday, February 12 | 1:30 p.m.
IBOIOT-1117
No Ticket Required: AI-Powered Troubleshooting for OT Networks

Thursday, February 12 | 5:30 p.m.
IBOIOT-2114
Redefining Industrial Networking: SRv6 for Utilities and Distributed Automation

FINISH

Friday, February 13 | 9:15 a.m.
BRKIOT-2299
The Software-defined Factory Enabled by SDA

Secure your Industrial IoT Environment

START

Tuesday, February 10 | 11:45 a.m.
BRKSEC-2096
Securing Industrial Networks: Where Do I Start?

Tuesday, February 10 | 2:00 p.m.
LTRSEC-2381
Stronger Together: Uniting IT and OT Security with Cyber Vision

Tuesday, February 10 | 5:00 p.m.
IBOIOT-1113
OT Security Made Simple: Your 101 Guide to OT Network Security Assessments

Tuesday, February 10 | 5:15 p.m.
BRKIOT-2846
Enhancing Splunk with OT context using Cisco Cyber Vision

Wednesday, February 11 | 9:30 a.m.
IBOIOT-1113
OT Security Made Simple: Your 101 Guide to OT Network Security Assessments

Wednesday, February 11 | 11:15 a.m.
BRKIOT-2720
The Future of Manufacturing: Secure, Reliable, AI-Ready Network Architecture

Wednesday, February 11 | 3:15 p.m.
BRKIOT-2029
The OT Security Journey: Network Visibility, Segmentation, and Investigation/Response

Thursday, February 12 | 1:00 p.m.
BRKIOT-2910
Securing Industrial Operations: From OT Asset Visibility to Zero-Trust Network Access

Friday, February 13 | 9:00 a.m.
LTRIOT-2110
IT/OT Collaboration: Deploying and Securing Industrial Automation Networks

FINISH

Friday, February 13 | 11:15 a.m.
BRKIOT-2588
From Chaos to Control: Practical Segmentation Strategies for Industrial Networks

Thank you

cisco Live !


CISCO