

The background features a vibrant, abstract design with a color gradient from dark blue on the left to bright yellow and white on the right. The design consists of overlapping, wavy horizontal bands and a radial pattern of lines emanating from a bright white point on the right side, creating a sense of motion and energy.

CISCO *Live!*

Let's go



The bridge to possible

Assessing Software-Defined Access (SDA) for Industrial Automation

Best Practices for a Successful Deployment

Ilan Nagalingam, Technical Leader
Erika Franco, Technical Leader

Agenda

- Introduction
- Design Considerations
- SDA for IA architecture
- Common Industrial Features
- SDA Features for IA networks
- Cyber Vision Sensor on SDA
- TrustSec for the OT
- A note on wireless options

Why Are We Here?

“Want to get the most of Cisco Live”

“We have heard the benefits of SDA and want to apply it to OT network”

“We already deploy SDA and want to learn best practices”

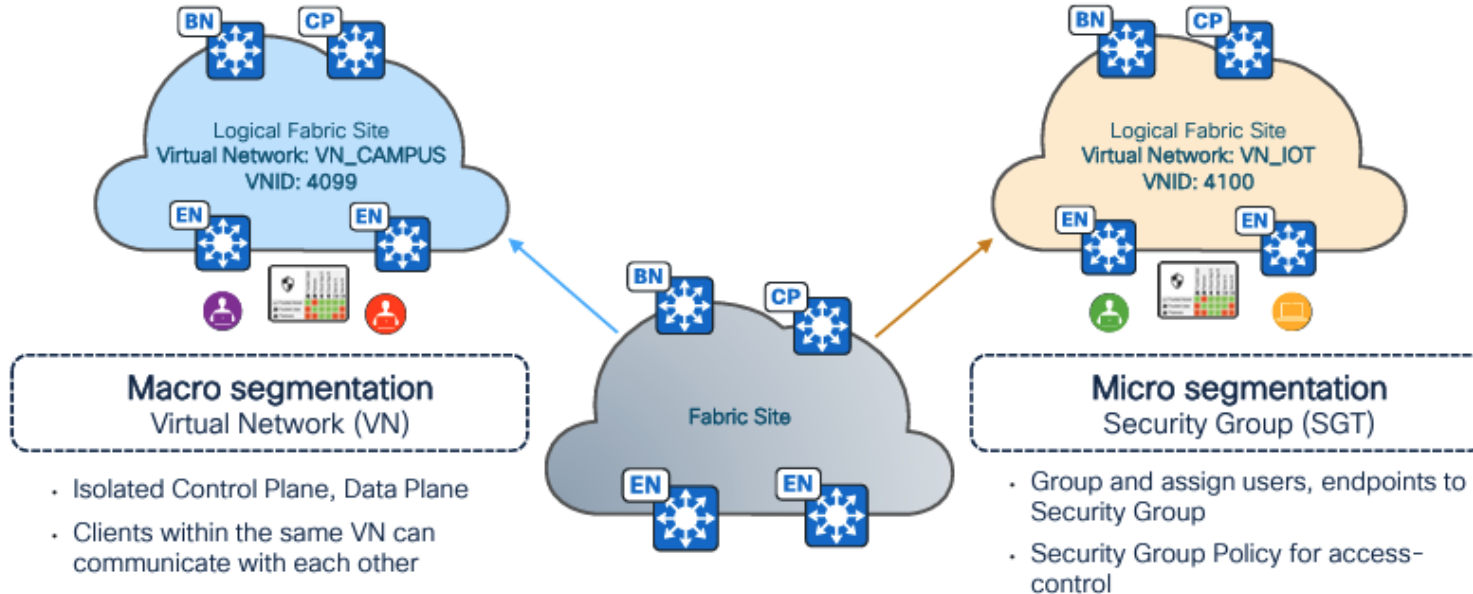
“Looking for an OT/IT converged network”

“I heard SDA is the way to apply micro-segmentation to the OT network”

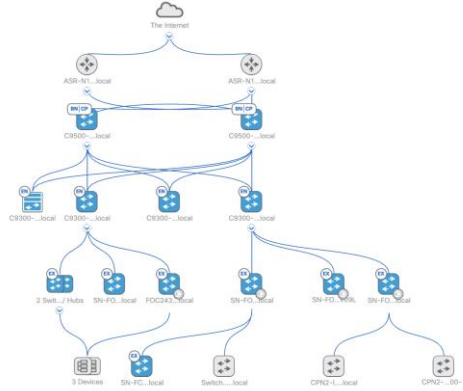
“Looking to migrate from an unmanaged network”

Cisco SD-Access

Multilevel Segmentation – VN, SGT



Benefits of SDA

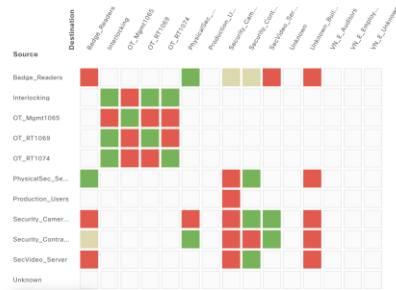


Automation and
Simplified
Management

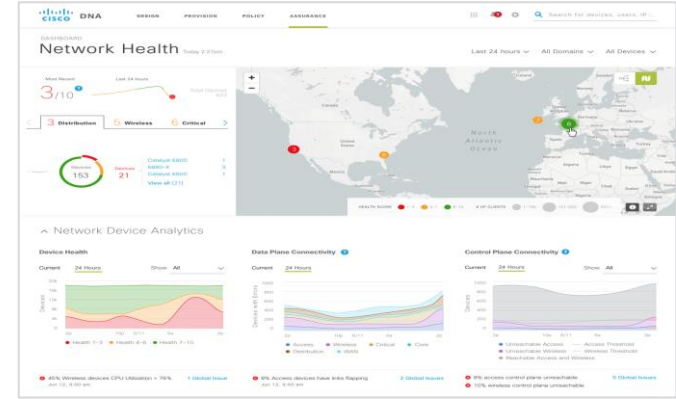
Policies (58) [Enter full screen](#)

[Filter](#) [Deploy](#) [Refresh](#)

☒ Permit ☐ Deny ☐ Custom ☐ Default



Policy-Based
Segmentation

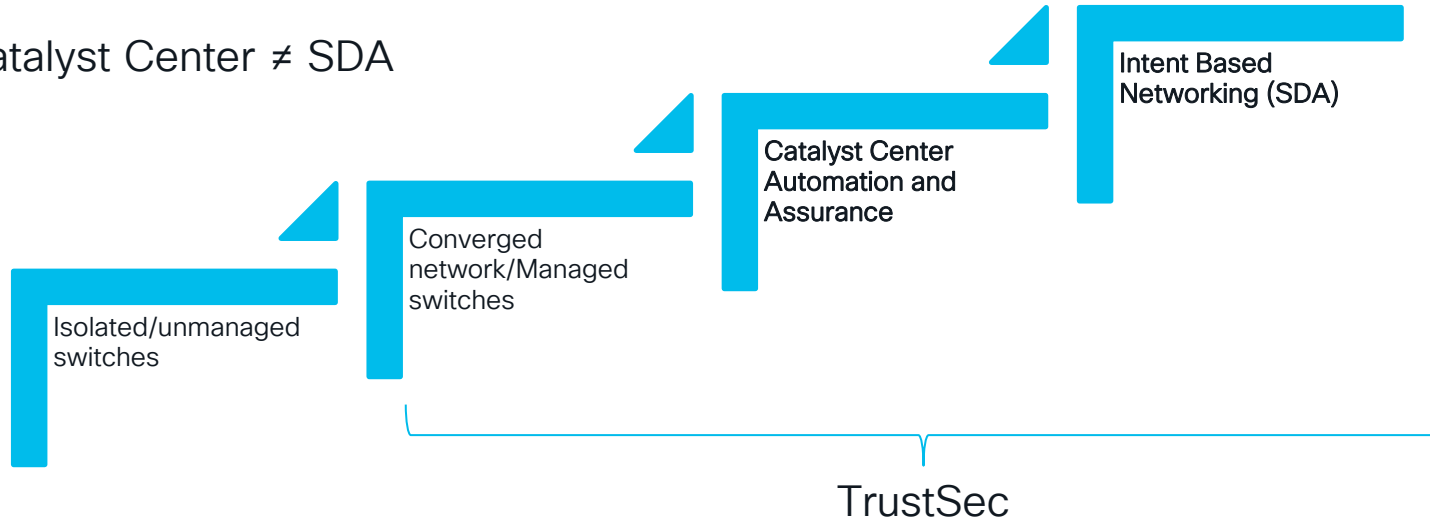


Centralized Control

Scalability and Flexibility

Clearing Common Misunderstandings

Catalyst Center $\neq$ SDA



SDA is not required to deploy TrustSec

Industrial Automation Requirements

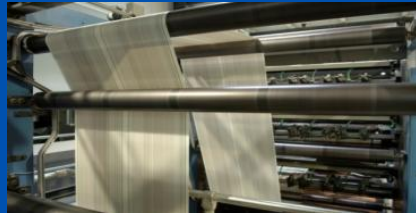
High Availability
Form Factor
Industrial Features
Ruggedization
Zero downtime
Different user persona
Security
Industry compliance
Support for duplicated IP addresses
Low Latency/Jitter

Performance Requirements

Industrial Automation & Control System Applications



For your
reference

	Process Automation	Discrete Automation	Loss Critical
Function	 Information Integration, Slower Process Automation	 Time-critical Factory Automation	 Multi-axis Motion Control
Comm. Technology Period	.Net, DCOM, TCP/IP	Industrial Protocols, CIP, Profinet	Hardware and Software solutions, e.g. CIP Motion, PTP
	1 second or longer	1 ms to 100 ms	100 μ s to 10 ms
Industries	Oil & Gas, chemicals, energy, water	Auto, food and bev, electrical assembly, semiconductor, metals, pharmaceutical	Utilities Subset of Discrete automation
Applications	Pumps, compressors, mixers; monitoring of temperature, pressure, flow	Material handling, filling, labeling, palletizing, packaging; welding, stamping, cutting, metal forming, soldering, sorting	Life/equipment safety, Synchronization of multiple axes: printing presses, wire drawing, web making, picking and placing

IT vs OT Requirements

CIA vs AIC



Protect the Data
CIA

Confidentiality

Integrity

Availability



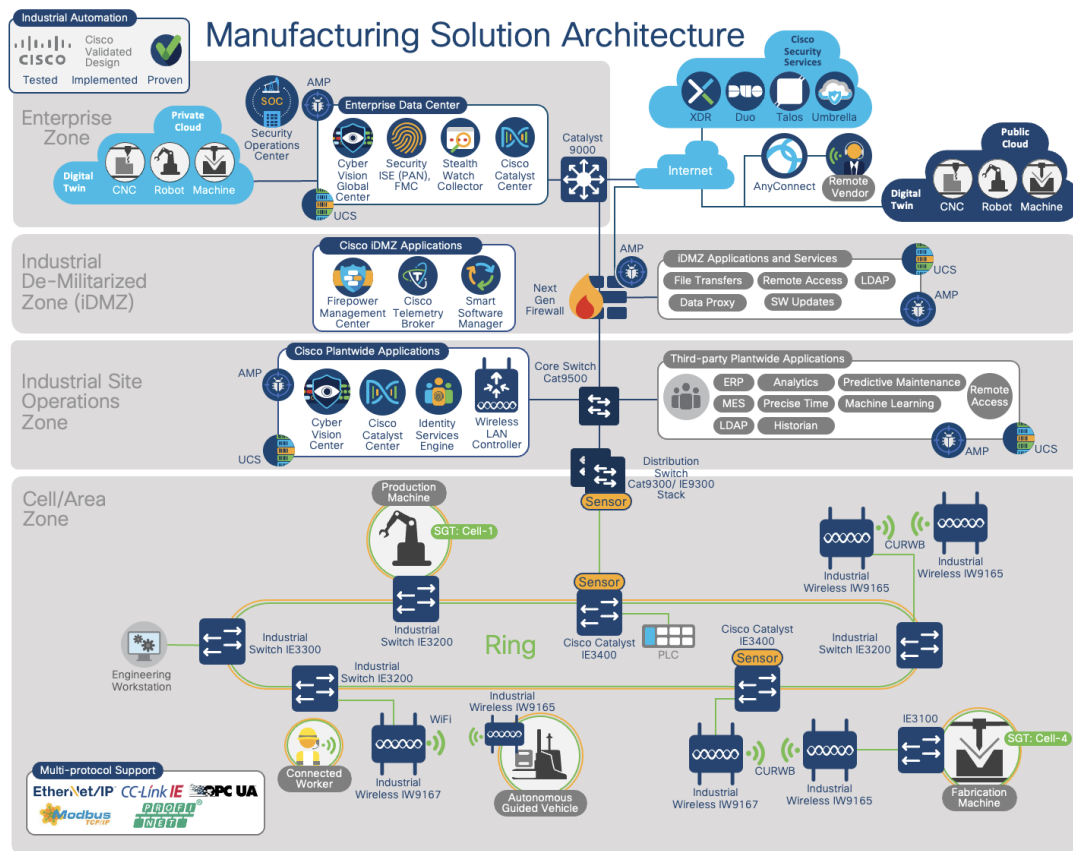
Protect the Process
AIC

Availability

Integrity

Confidentiality

Industrial Automation Non-SDA Architecture



Outcomes

- Improve uptime, OEE and asset utilization
- Reduce support effort and deployment errors
- Reduce risk from cybersecurity threats

Benefits

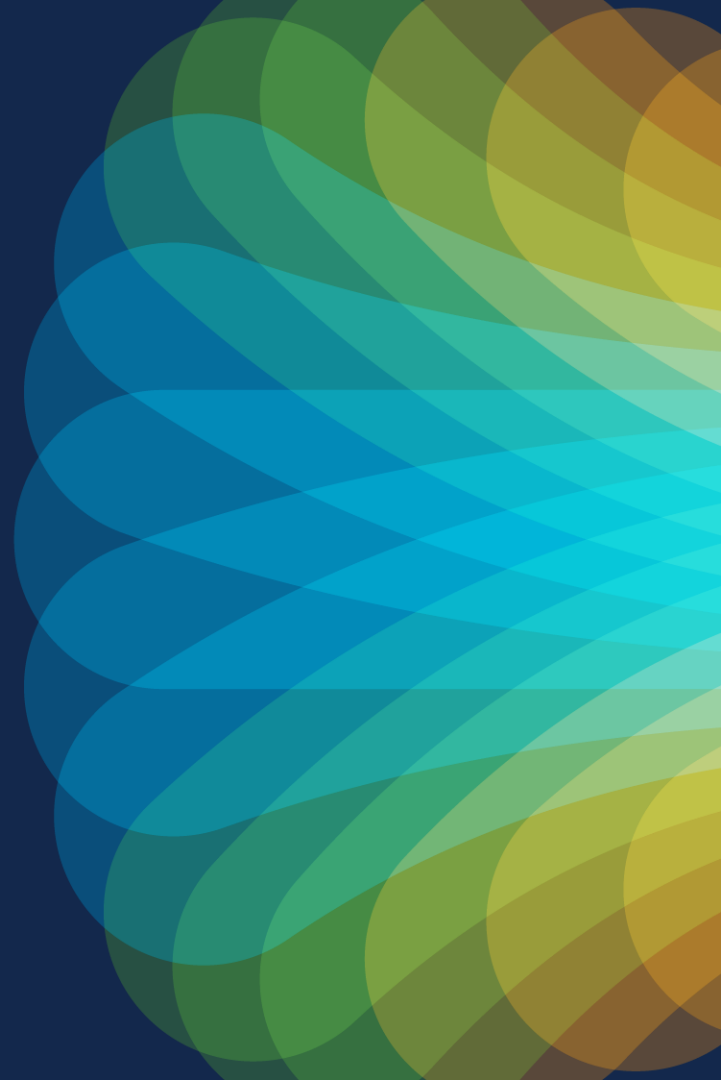
- Validated Design and Implementation guidance developed by Cisco engineering
- Tested against leading IACS vendor devices and applications
- Experienced Cisco services ready to apply to a customer scenarios

How to Transform Industrial Automation Architecture to SDA

Key design questions

- Could we apply the Purdue Model?
- Shared OT/IT network vs dedicated SDA network for OT
- Should SDA extend to the industrial access layer?
- Should IT and OT share Catalyst Center?
- Could we meet cell/area zone requirements in an SDA network?
- Is industrial wireless a requirement?

SDA and the Purdue Model



“The Purdue Model is dead. Long live the Purdue Model”

Forbes, “A Reimagined Purdue Model For Industrial Security Is Possible”, January 2022

Relevance of Purdue Model Today

Functional layers help address cybersecurity challenges unique to Industrial Automation Networks:

- IACS were built to last, not to evolve.
- Firmware updates are not always possible given stringent uptime requirements
- Increased requirements for cloud adoption and IT/OT convergence lead to less containment and isolation
- New sophisticated cyberattacks

A Decade After Stuxnet: How Siemens S7 is Still an Attacker's Heaven

Colin Finck | Tech Lead, Reverse Engineering & Connectivity, ENLYZE GmbH

Tom Dohrmann | Software Engineer, Reverse Engineering & Connectivity, ENLYZE GmbH

Date: Wednesday, December 6 | 1:30pm–2:10pm (ICC Capital Suite 4, Level 3)

Format: 40-Minute Briefings

Tracks: 🌐 Cyber-Physical Systems & IoT, 🔄 Reverse Engineering

 Security Magazine

Manufacturing is the top industry affected by ransomware in 2023

Ransomware in Q3 2023 was analyzed in a recent GuidePoint report. The report found a nearly 15% increase in ransomware activity since Q2 due...



CYBERSECURITY ADVISORY

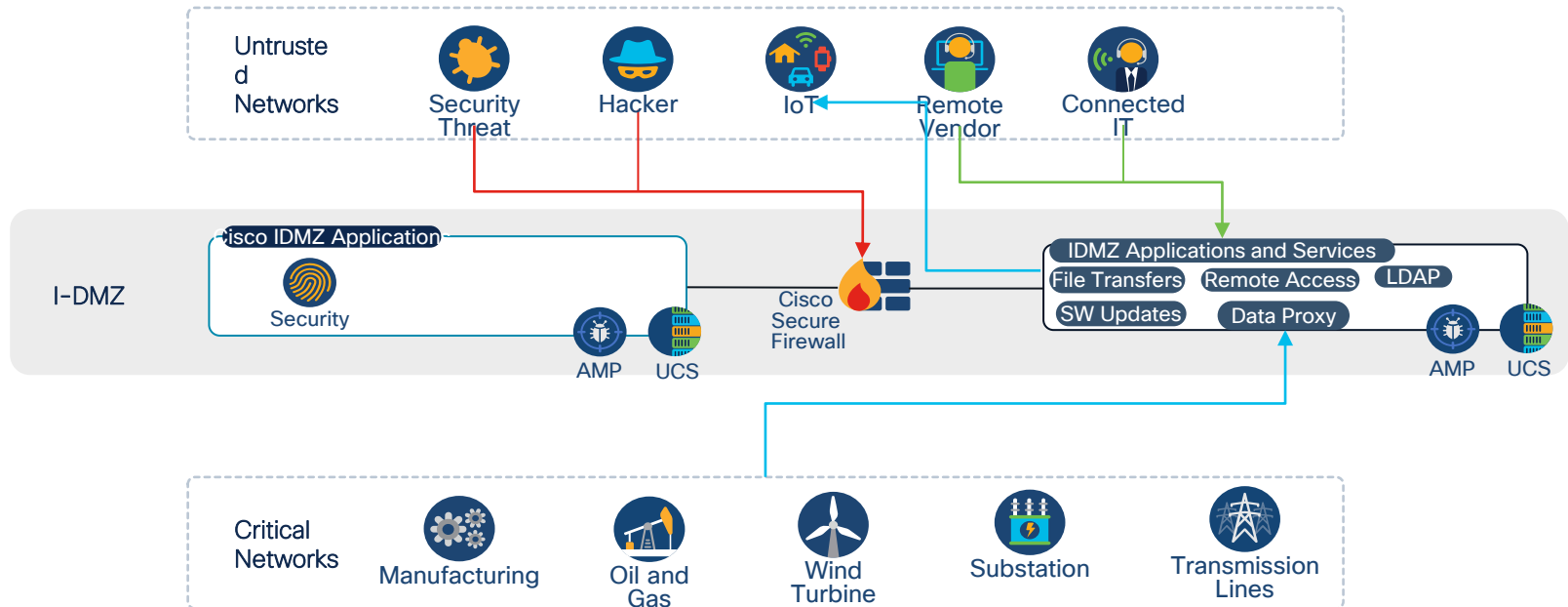
IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

Release Date: December 01, 2023

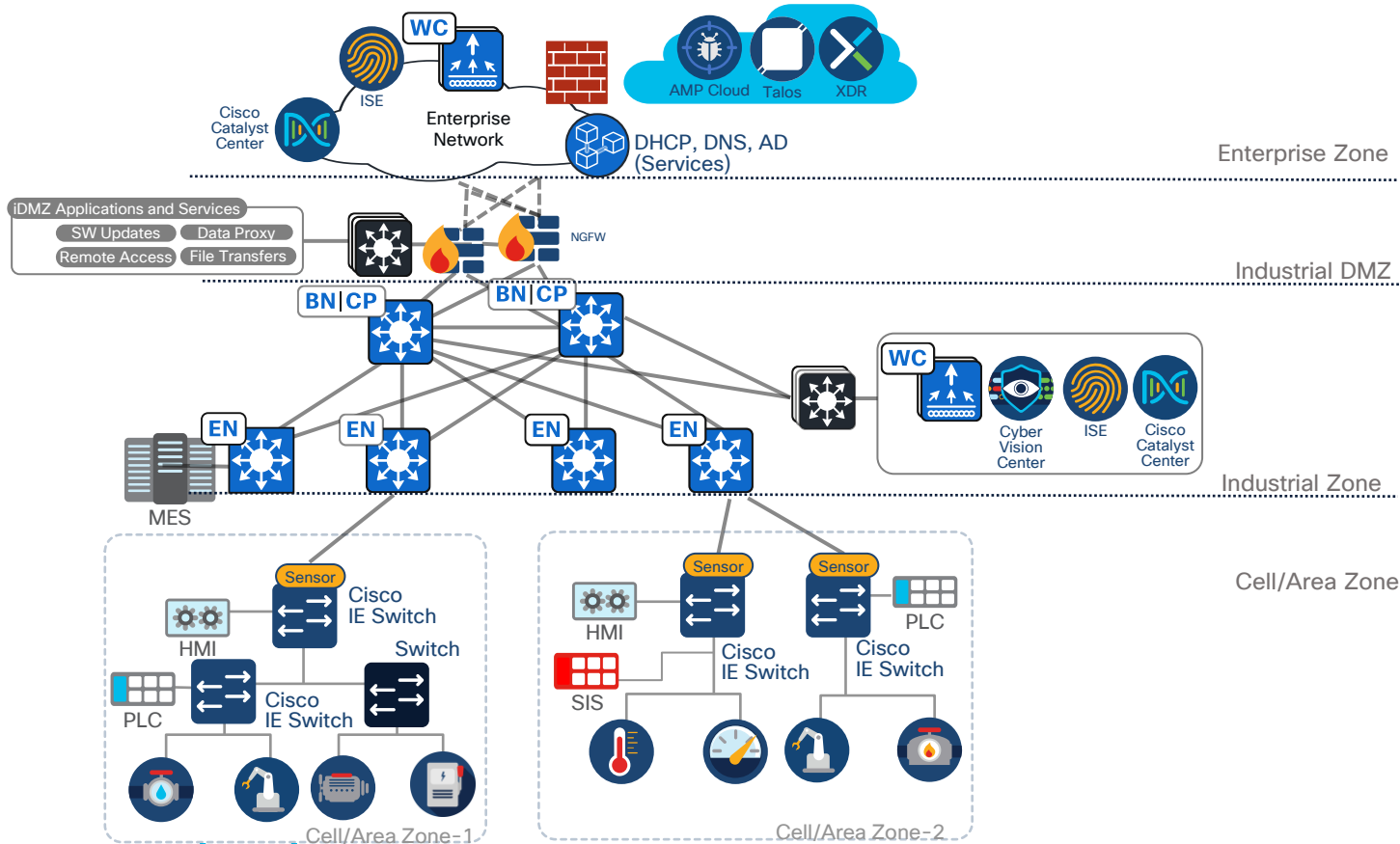
Alert Code: AA23-335A

IDMZ with Cisco Secure Firewall

Protects critical assets, limits inbound connections, serves as disconnection point



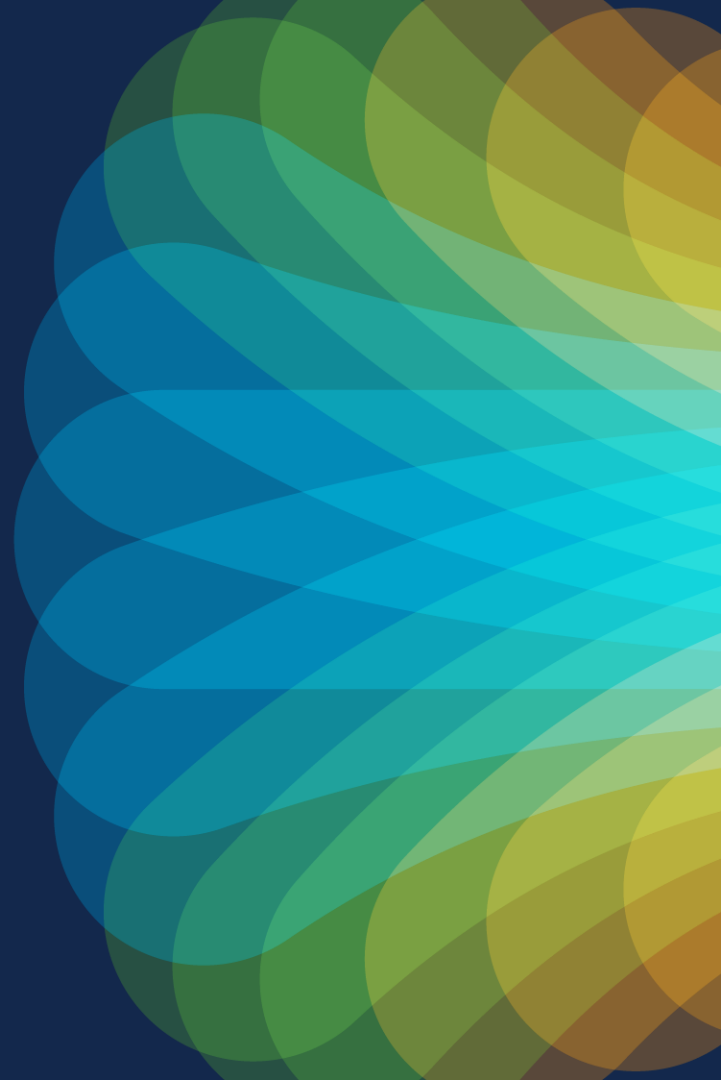
Industrial Automation SDA Architecture



- Peer device (a.k.a. Fusion) is a firewall
- Peer device connects to IDMZ service layer

ISE PSN, PxGrid, Cyber Vision, (optional Catalyst Center) for survivability

Should the Network for OT be Shared or Dedicated?



The Case for Dedicated OT SDA Network

A Dedicated OT SDA Network is Recommended

Isolation from IT Configuration Changes:

- **Benefit:** Prevents unintended consequences on OT systems due to IT configuration changes.

Custom Segmentation Policies:

- **Benefit:** Enables independent and tailored segmentation policies for OT network.

Tailored Quality of Service (QoS):

- **Benefit:** Facilitates the implementation of distinct QoS requirements, ensuring priority for critical OT processes.

Scalability for Large Industrial Deployments:

- **Benefit:** Meets the scalability demands of expansive industrial setups, supporting seamless growth without compromising performance.

The Case for Shared IT/OT SDA Network

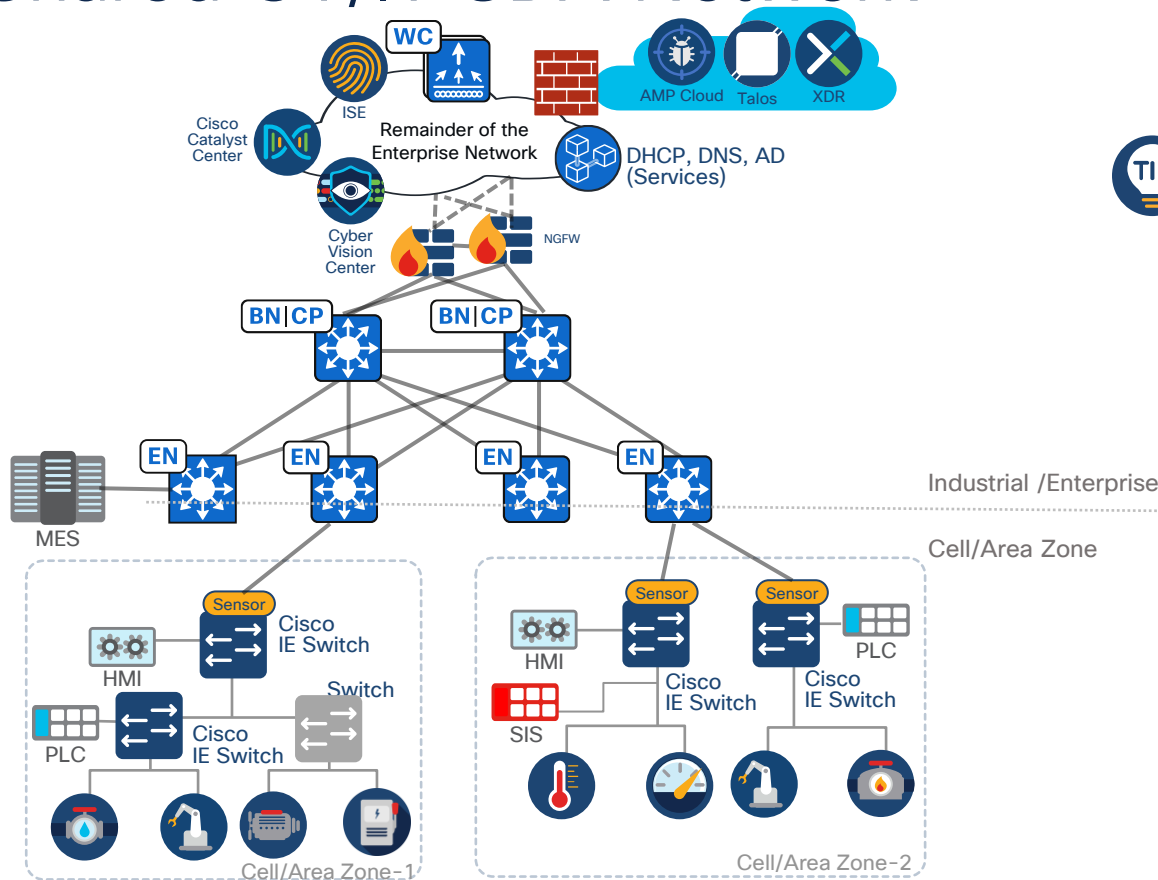
Cost-Efficient Infrastructure:

Benefit: Optimizes resource utilization and minimizes expenses.

Simplified Administration:

Benefit: Streamlines network management tasks, reducing the complexity of day-to-day administration for improved operational efficiency.

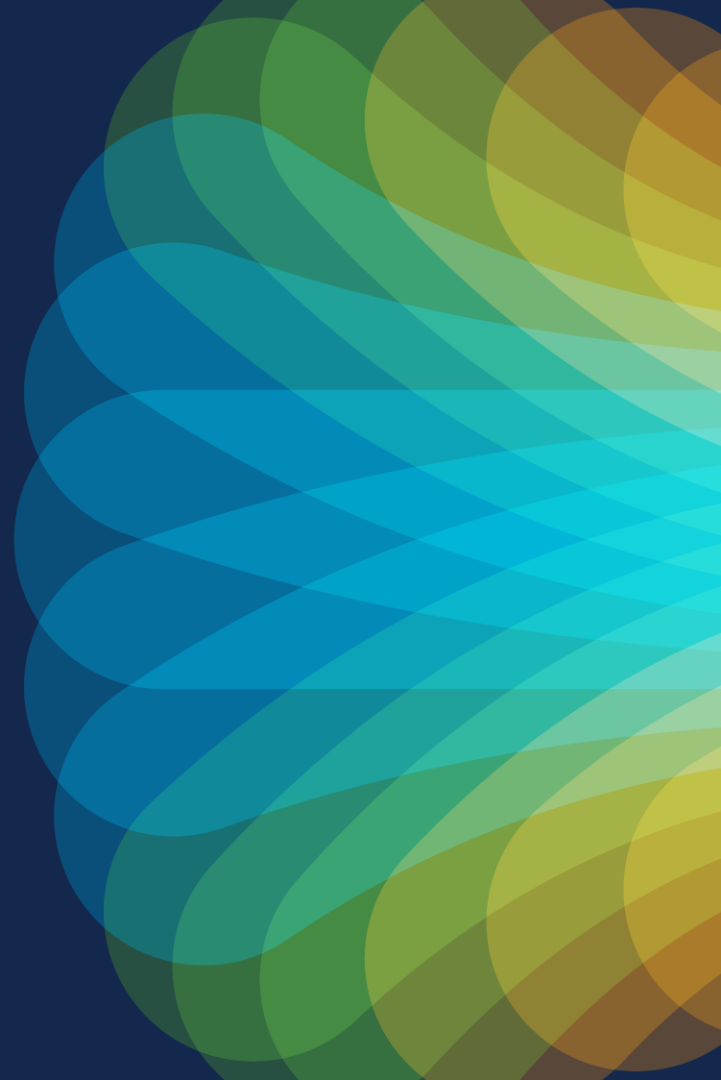
Shared OT/IT SDA Network



Create separate Virtual Networks for IT and OT.

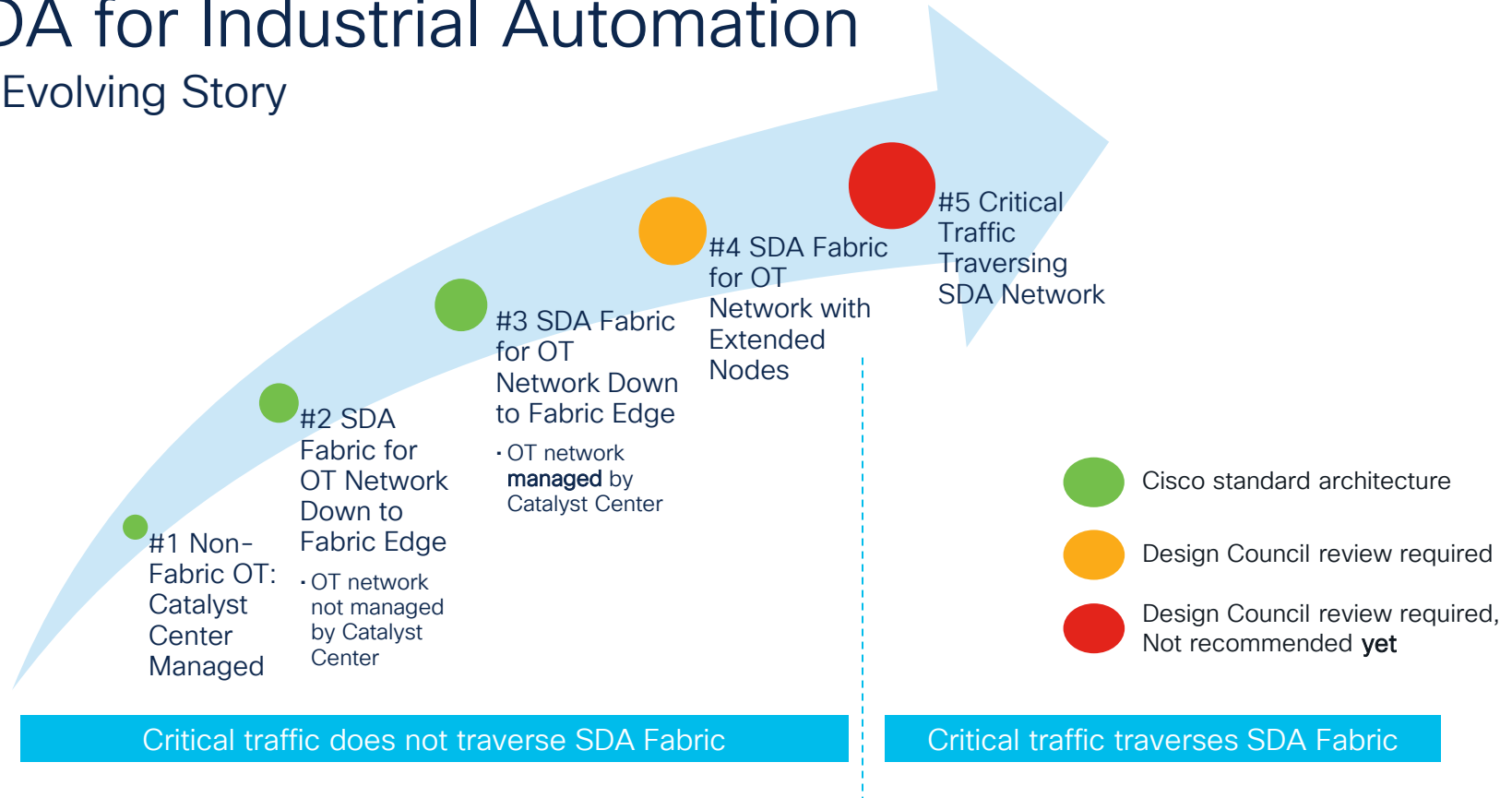
Configure Firewall acting as Peer Device with rules for OT connections

SDA to the Access?



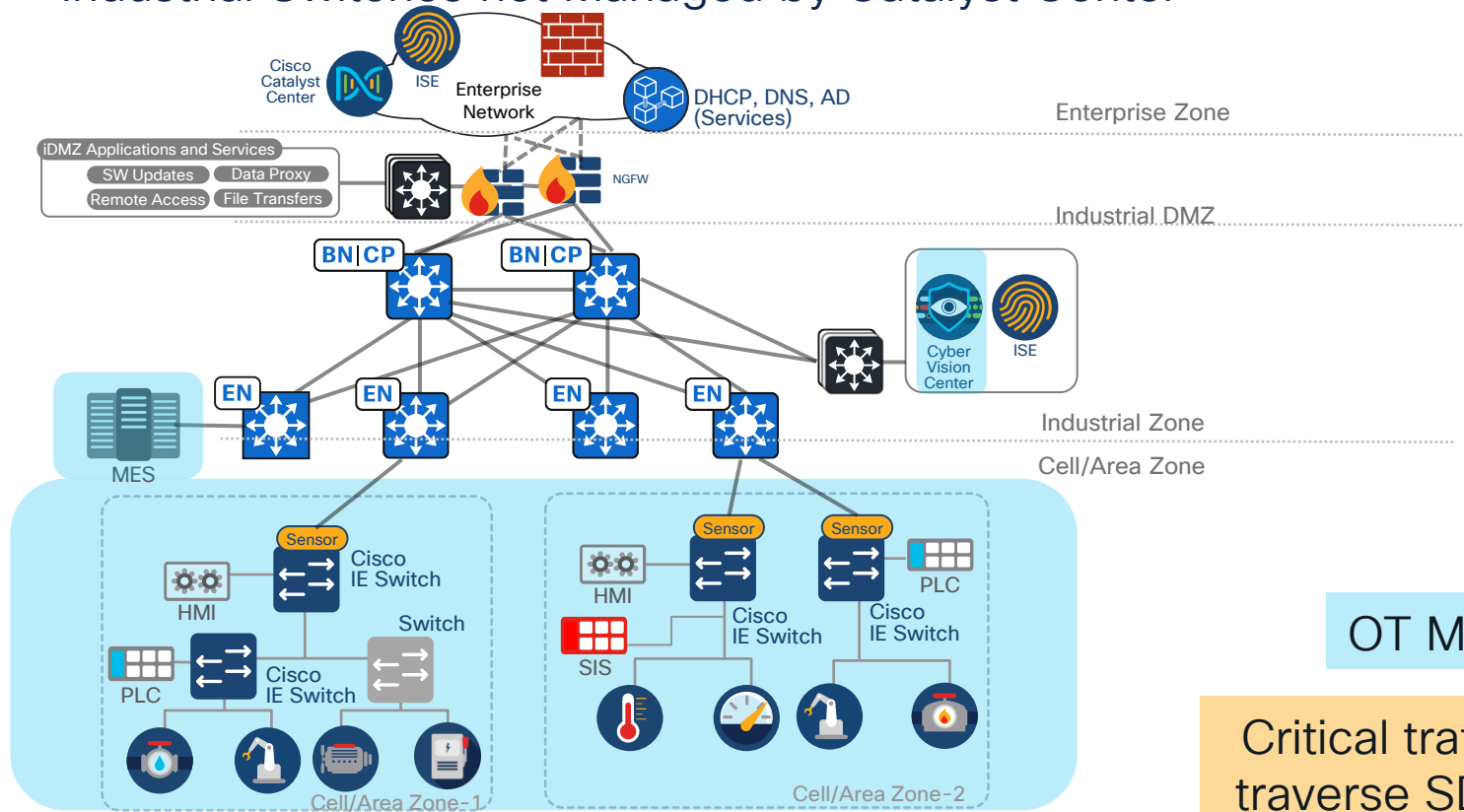
SDA for Industrial Automation

An Evolving Story



#2 SDA Fabric for OT Network Down to Fabric Edge

Industrial Switches not Managed by Catalyst Center



OT Managed

Critical traffic doesn't traverse SDA network

#2 SDA Fabric for OT Network Down to Fabric Edge

Industrial Switches not Managed by Catalyst Center



In favor

- Provides OT/IT separation.
- IT assigns IP pools and downlinks to OT.
- Easy transition for OT persona as no change in tools is needed.
- Cisco standard architecture



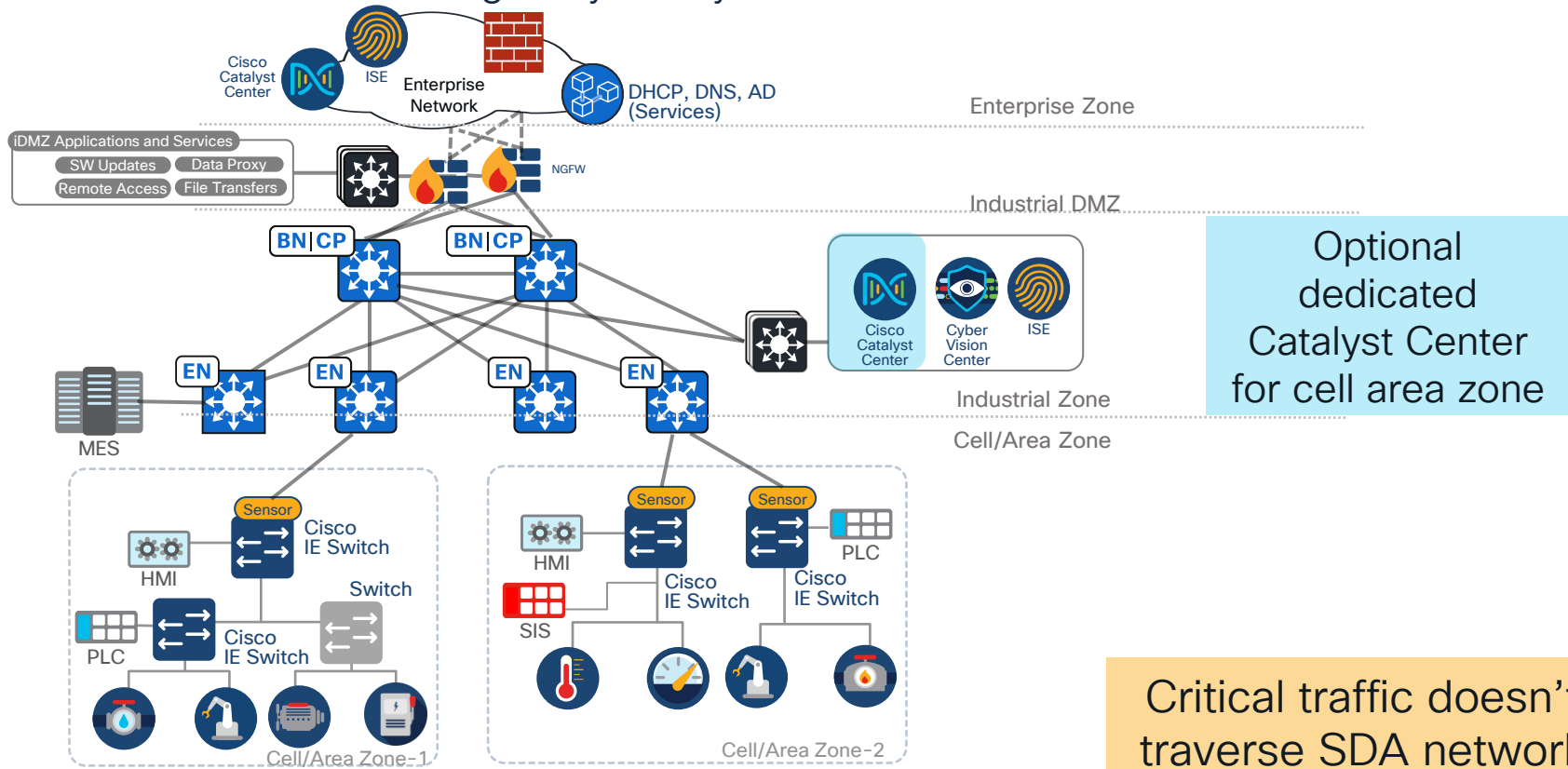
Possible cons ...

- Catalyst Center does not provide automation and assurance to the industrial switches.
- Dynamic segmentation policy not recommended in this architecture (More on this later)

Cell area zone network is operated independently by OT

#3 SDA Fabric for OT Network Down to Fabric Edge

Industrial Switches Managed by Catalyst Center



#3 SDA Fabric for OT Network Down to Fabric Edge

Industrial Switches Managed by Catalyst Center



In favor

- Catalyst Center provides automation and assurance to the industrial switches
- Allows for both options:
 - cell/area zone managed by OT persona using Catalyst Center
 - OT SDA network and cell area zone managed by same team
- Catalyst Center could be shared or dedicated to the OT
- Cisco standard architecture 

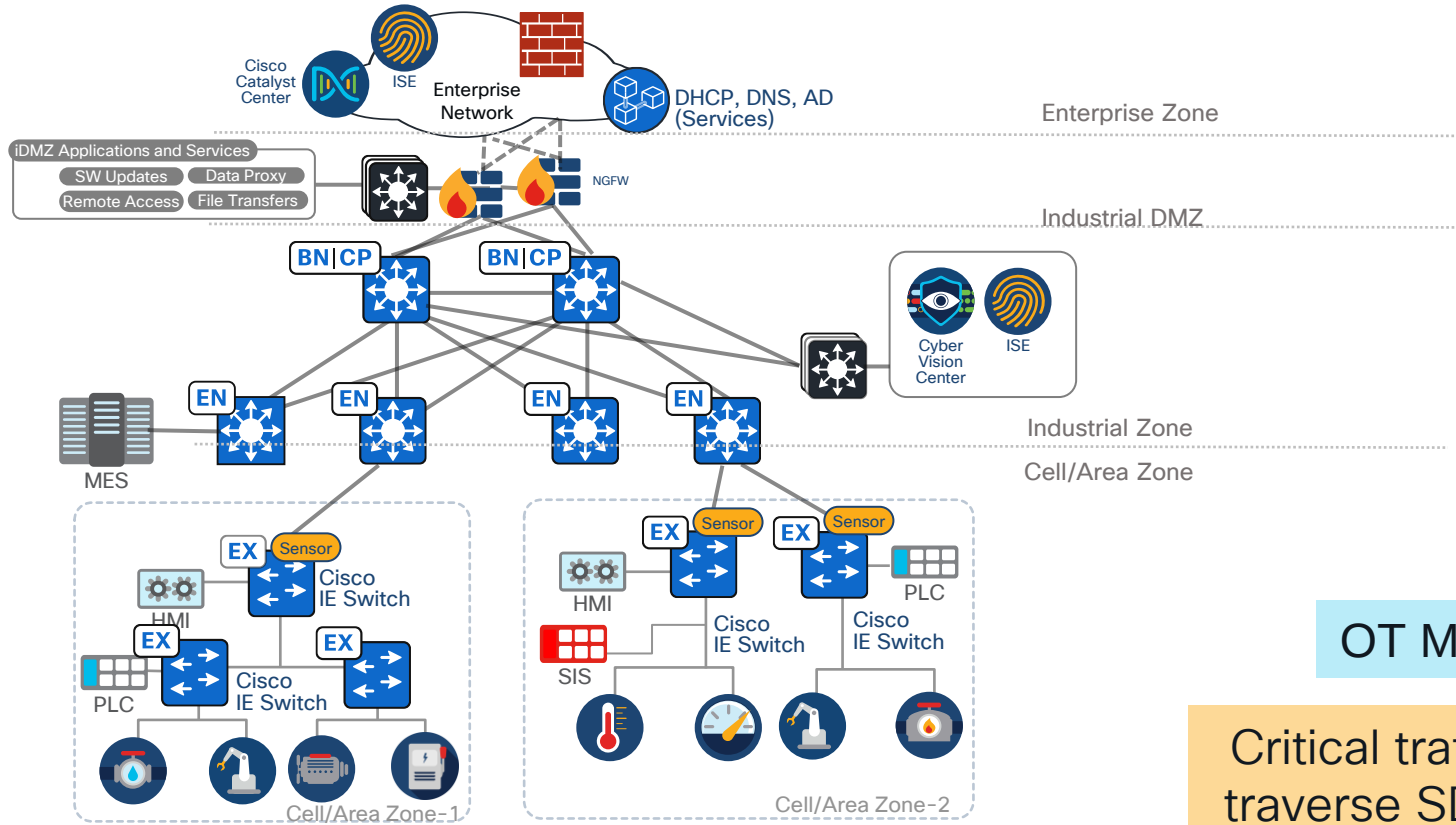


Possible cons ...

- IE switches don't benefit from SDA provisioning workflow (switches are provisioned using PnP and templates)

Cell area zone is managed by Catalyst Center

#4 SDA Fabric for OT Network with Extended Nodes



OT Managed

Critical traffic doesn't traverse SDA network

#4 SDA Fabric for OT Network with Extended Nodes



In favor

- No templates required for Industrial switches.
- Rich API support for industrial switch operations.



Possible cons ...

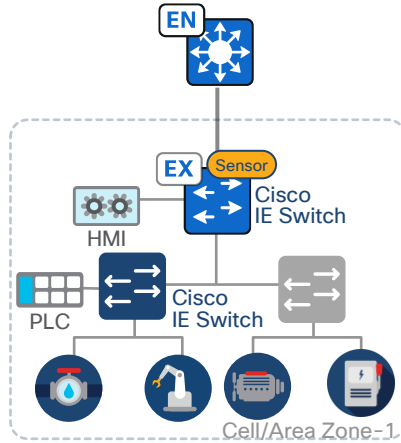
- OT SDA network and cell are zone managed by same team using a single Catalyst Center cluster
- Only REP or daisy chain topologies are supported
- Cannot mix PEN and EN in same daisy chain because of security policy
- No support for Brownfield switches, must be greenfield
- If templates are required for OT features, they need to be reviewed for conflicts



- All network devices on OT network benefit from SDA Automation

SDA Fabric for OT Network with Extended Nodes

Extended Node + Non-extended Nodes IE Switches



When should this be considered?

- Cell/area zone has Cisco Switches or IE switches with no EN/PEN support
- The EN/PEN switch acts as an aggregation layer with minimal modifications via template required but customization is needed on access switches
- Access switches need to be visible to PROFINET or CIP applications

Critical traffic doesn't traverse SDA network

Before Continuing...

Should IE switch be EN/PEN or Non-Fabric device?

EX



When to consider EN/PEN

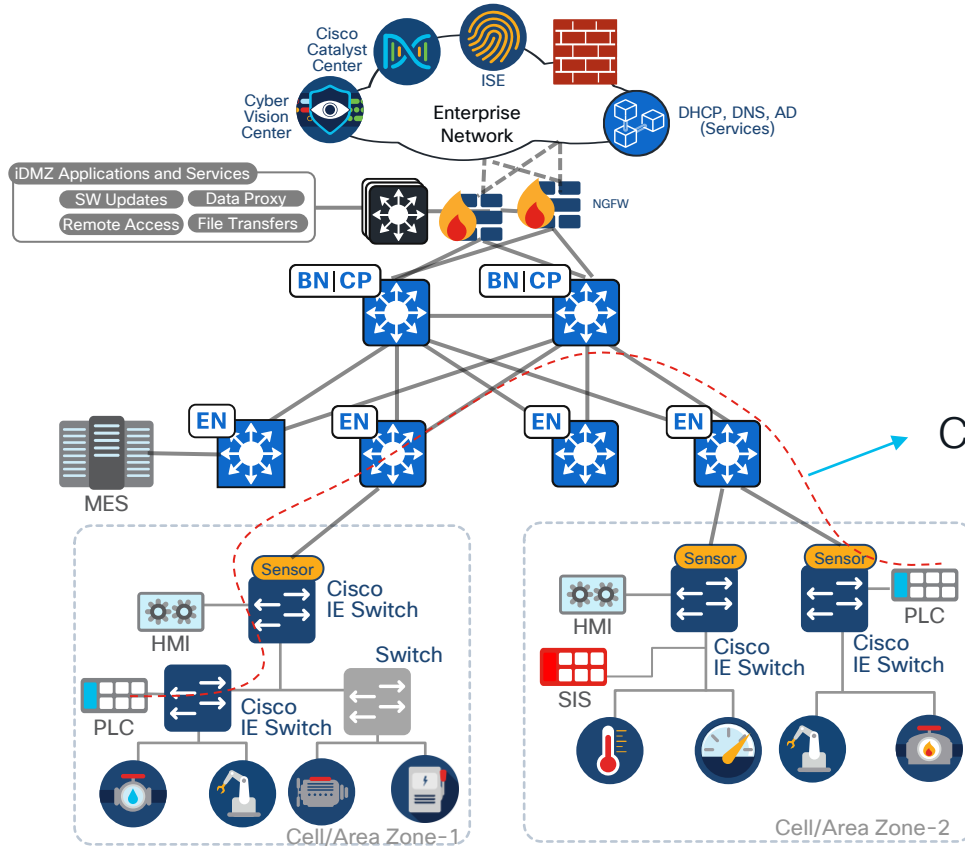
- Minimal modifications via templates are required
- Strong need of automation via APIs
- Same team is responsible for Core/Distribution and Cell area zone switches



When to consider Non-Fabric

- Templates required to support additional features (more on this later)
- Switch needs to be part of the overlay (i.e. visibility of switch in profinet topology)
- Different teams are responsible for Core/Distribution and Cell area zone switches
- Switch is configured by system integrator

Critical Traffic Traversing SDA Network



Not Recommended yet

If considering this design talk with Cisco account team.
Design Council review required.

Critical Traffic (i.e. Profinet, CIP, CC-link)

Looking into the future: PLC Virtualization

Replace large number of individual controllers by applications on the industrial data center reducing cost of ownership.

Dedicated Single-Purpose Hardware (PLC, I/O, IPC, SBC)



Decoupling of hardware and software by means of virtualization. Applications and services running on Commercial Off-The Shelf (COTS) Infrastructure



<https://www.controleng.com/articles/virtualized-programmable-logic-controllers/>

OT Requirements vs Current SDA Support

Tolerance to network outages: 10-80ms

Failure on the underlay may produce outages > 200ms

Layer 2 multicast is used for device discovery, producer/consumer messages

- L2 flooding enables multicast but broadcast domain is extended through the fabric
- IGMP has not been validated

Resiliency protocols in industrial networks: PRP, MRP, DLR, HSR, REP

Only REP is supported in Catalyst Center today

QoS: Priority queue needs to be reserved for high priority traffic

Application policy is based on enterprise profile

QoS: Profinet uses COS values

Application policy does not support for COS

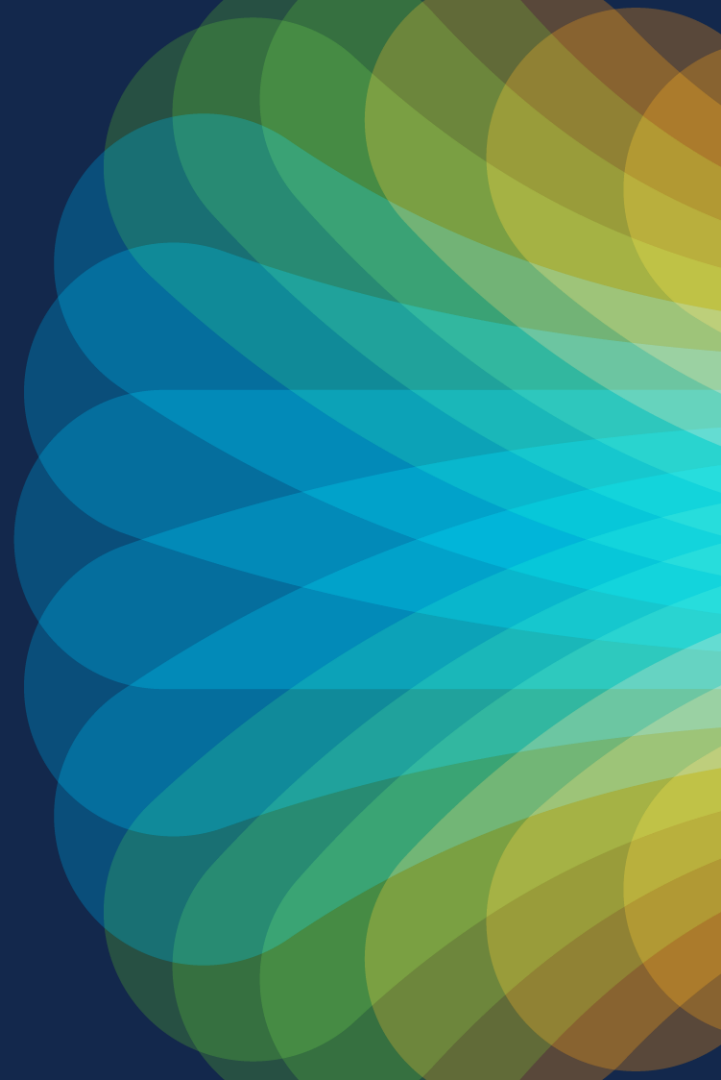
May require precision timing

Fabric nodes cannot be part of the PTP domain yet

L2NAT

L2NAT configured via template

Should IT and OT share Catalyst Center?



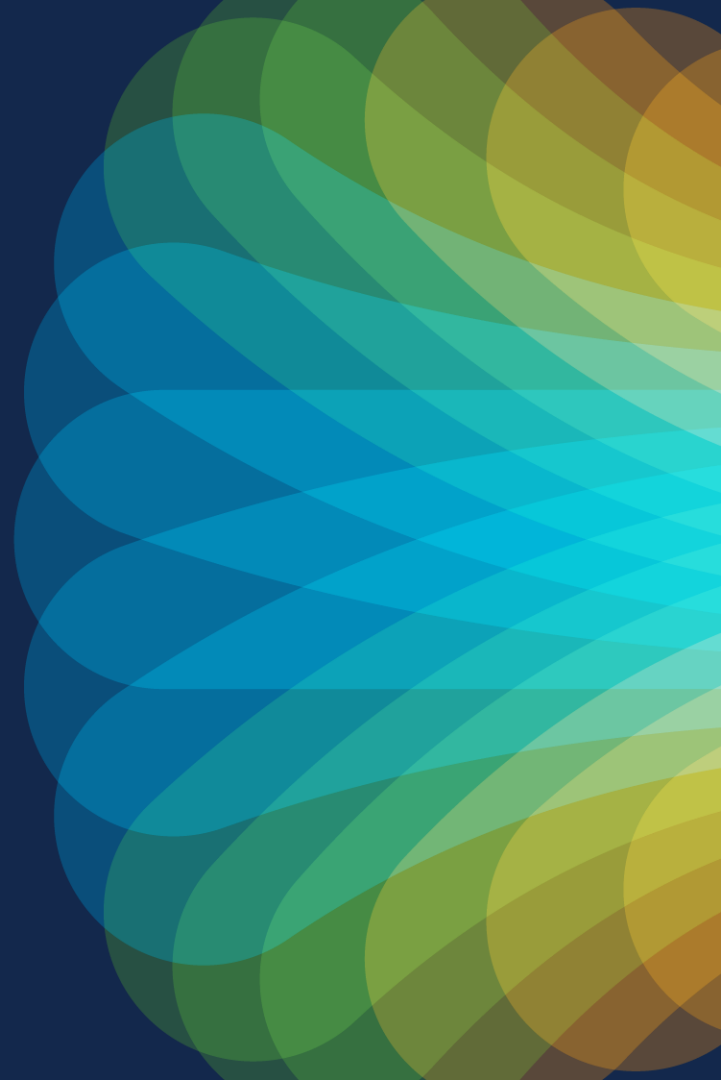
Catalyst Center deployment considerations

Role Based Access Control (RBAC) based on function globally*

Role	Description	Personas
System Administrator	Catalyst Center administrator	IT
Network Administrator	Network administrator (pushes templates, configures fabric, uses PnP, SWIM)	IT Possibly OT: needed if OT is upgrading devices, pushing templates, onboarding switches, etc
Observer	View-only access	IT and OT
Custom	Permit or restrict user access to certain functions globally	Possibly OT: Could create custom roles i.e. SWIM + view-only

*Site based RBAC is roadmap

Common Industrial Features



Common Industrial Features

Templates are Required to Apply Most Industrial Features

Feature	Description
Cyber Vision	Configure AppGigabit interface, configure monitoring sessions
Quality of Service	Configure industrial traffic for QoS policy
Profinet/CIP	Enable/disable, configure VLAN
Pruning VLANs/trunk configuration	Configure trunk options: VLANs, PNP startup VLAN, CTS
Resilient protocols	PRP, MRP, DLR, HSR
L2NAT	L2NAT instance, NAT entries and interface configuration
PTP	PTP mode, VLAN, interface configuration

L2NAT

Layer 2 NAT – Integrate Multiple Machines

Ethernet networks continue to grow

Each **machine**
adds another

5-10

EtherNet / IP enabled
devices

+

Every **line**
adds another

250-1,000

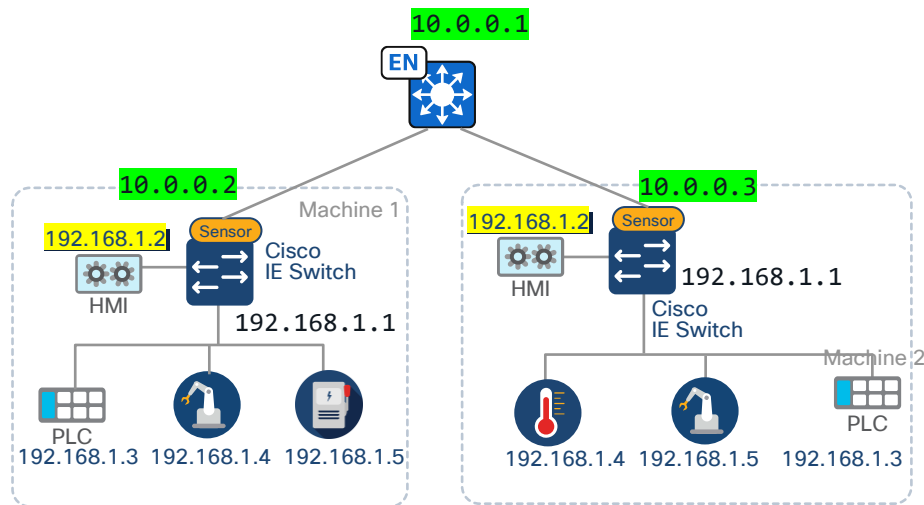
EtherNet / IP enabled
devices

=

How do I
connect all these
machines into a
plant network to
gain the
advantages?

Common OT Features That Require Templates Example

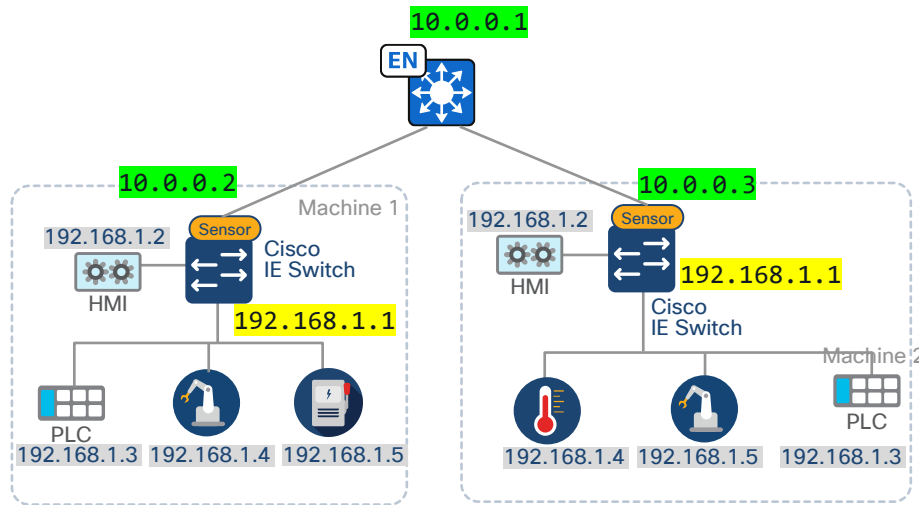
L2NAT: Allows IP Address Duplication in Different Machines



L2NAT has not been validated in EN/PEN*

Common OT Features That Require Templates

L2NAT



```
l2nat instance machine1
  instance-id 1
  permit all
  fixup all
  inside from host 192.168.1.2 to 10.0.0.101
  inside from host 192.168.1.1 to 10.0.0.2
```

```
interface GigabitEthernet1/1
  switchport trunk allowed vlan 100
  switchport mode trunk
  l2nat machine1 100
  !
Interface vlan 100
  ip address 10.0.0.2 255.255.255.0
interface Vlan3004
  ip address 192.168.1.1 255.255.255.0
```

PROFINET and CIP

Common OT Features That Require Templates

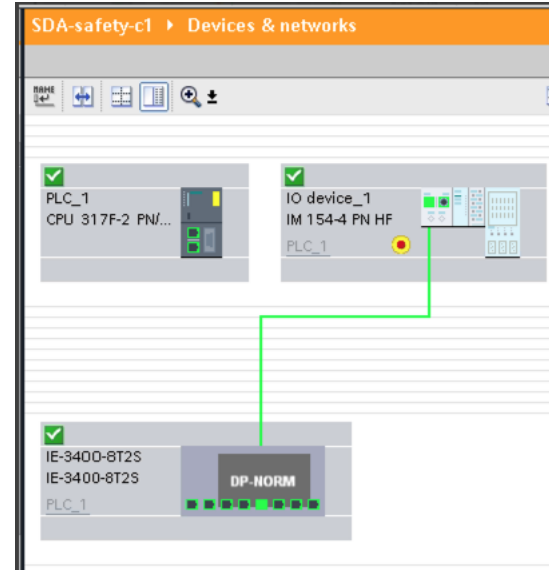
PROFINET and CIP

- IE switch needs to have an IP address on the OT overlay to be added to the topology on engineering application
- HMI can read information from the switch (i.e. alarms)

Template Example for PROFINET:

```
profinet
```

```
profinet profinet vlan 1069
```

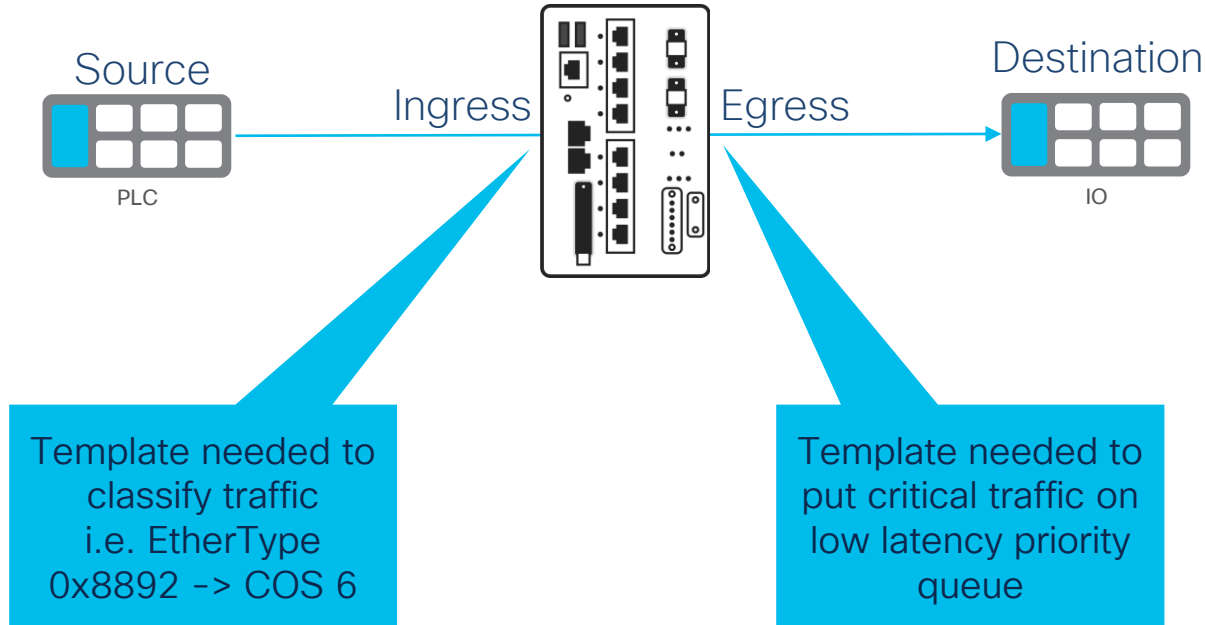


Quality of Service



Common OT Features That Require Templates

Quality of Service



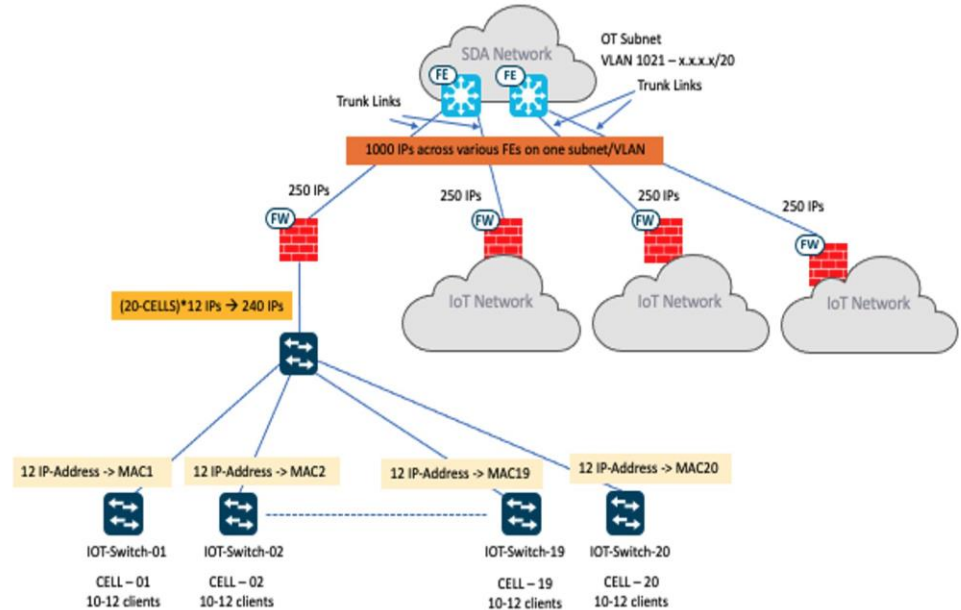
SDA Features for IA networks

SDA Features for IA networks

Feature	Description	Use case
Multiple IP-to-MAC addresses	Supports multiple IPs associated to a single MAC address.	Multiple IPs can be associated to a single MAC when L2NAT with connected routing is used on the industrial network
IP Directed Broadcast	An SD-Access Border switch can convert an IP-directed broadcast originated outside the fabric into an Ethernet broadcast and flood to all endpoints in the destination VLAN.	Silent hosts (An endpoint whose location in fabric is not known because it has not sent any packets or frames.)
Layer 2 Flooding	Floods all ethernet broadcast, unknown unicast and multicast to all switches connected to L2 network	Allows critical traffic based on multicast. i.e. DCP discovery from engineering station to cell area zone
Fabric zones	Fabric Zones are a way to localize Layer 2 Virtual Networks and Anycast Gateways to sections of a Fabric Site, for example to a production area.	Helps with scale Eases micro-segmentation implementation when VLAN to SGT is used
REP Workflow	Supports REP rings of extended nodes and Fabric Edge	Fault tolerant network. Convergence < 150 ms

Multi-IP to MAC Addresses

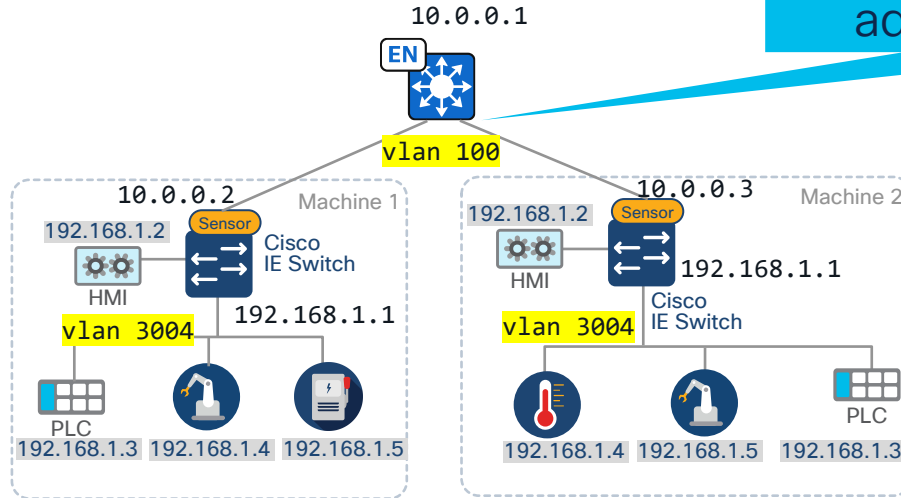
- Multi-IP to MAC Address feature can be enabled on an Anycast Gateway.
- A Wired endpoint in the associated VLAN can have the following number of IP Address to MAC mappings
 - 1000 IPV4 Addresses to a MAC
 - 1000 IPv6 Addresses to a MAC
- Wired and wireless endpoints hosting bridge network VM can also be connected to the associated VLAN.
- A Maximum of 20 Bridge network VMs can be hosted on a wireless endpoint connecting to the associated VLAN.



Multiple IP to MAC Address Example

L2NAT with inter-VLAN routing

Sees multiple IPs to single MAC address as switch is "routing"



Eliminate machine to machine Broadcast:

different vlan 'private' from 'public'

Vlan 3004 inside machine

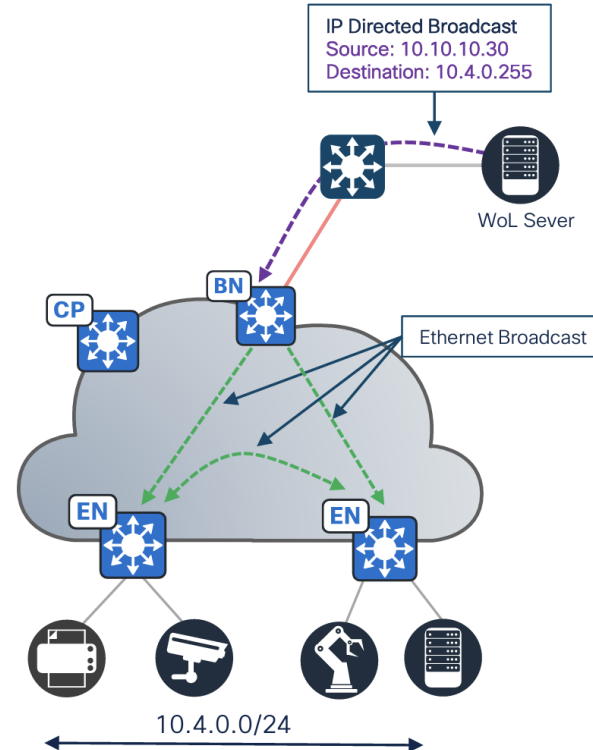
Vlan 100 outside machine

IE switch 'routes' between vlans.

IE switch is L3 GW for 192.168.1.x

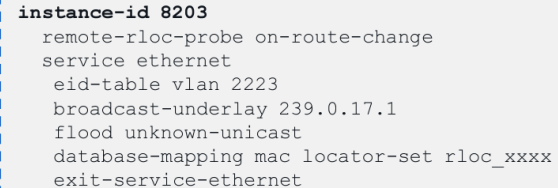
IP Directed Broadcast Use-Case

- An endpoint connected in the Fabric may move into passive/power saving mode(Silent/Sleeping hosts).
- An endpoint whose location in fabric is not known because it has not sent any packets.
- To onboard such clients, broadcast frame must be forwarded across the subnet across the edge nodes at a fabric site.
- In case, the Wake-On-LAN server outside the fabric, Border node can convert an IP Directed broadcast into an Ethernet broadcast and flood to all endpoints in the destination VLAN.



CISCO *Live!*

- 53



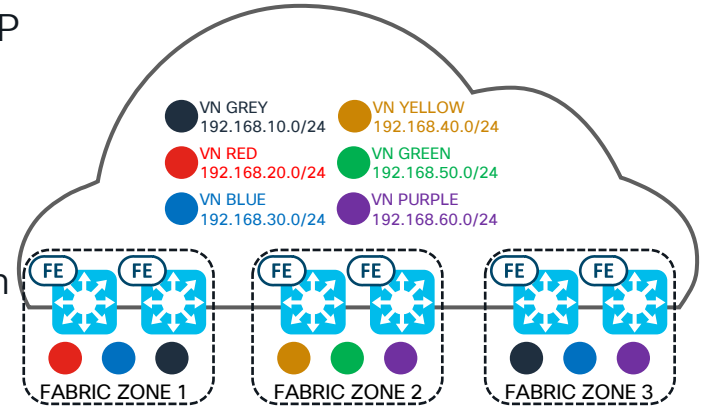
Fabric Zones

Use Case:

- Customers would like to restrict the VN/IP pool contained to a certain set of Fabric Edges.
- Customers requires the flexibility for granular control of IP Pool provisioning scope.
- Needed for compliance and security frameworks.

Feature Overview:

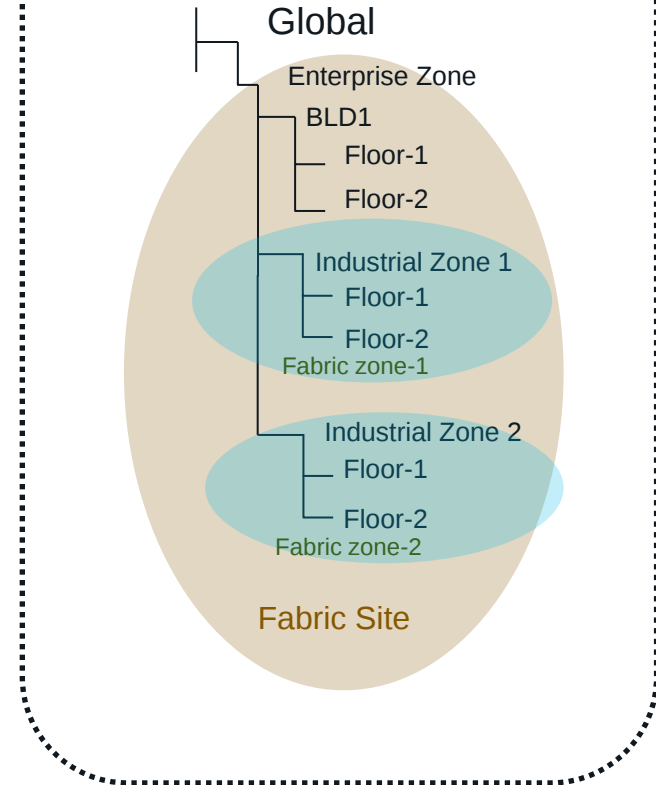
- Cisco SD-Access introduces an optional construct known as Fabric Zones
- Provides the flexibility to assign and map selective pools within the VN's to be provisioned at fabric edges.
- Device role that can exist in a fabric zone are only Fabric Edges, extended nodes, and policy extended nodes.



Fabric Zones Feature Overview

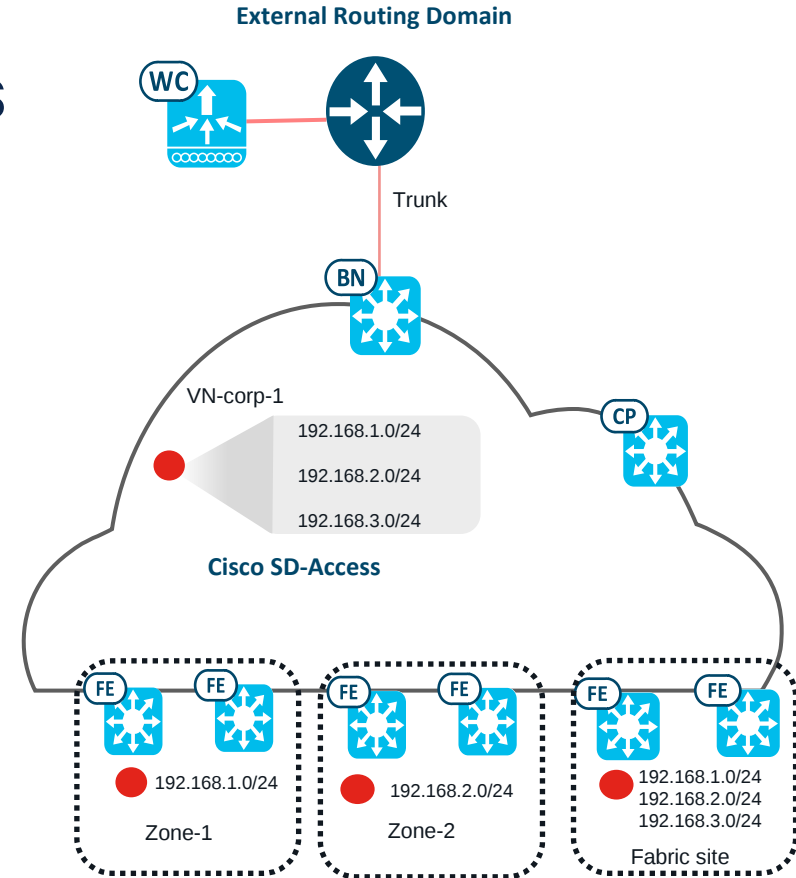
- By default, there is no fabric zone created in a fabric site.
- Fabric Zones are child sites of a parent fabric site
- Fabric zone can be enabled for Day-0 or a Day-N operation.
- A fabric zone can be created at a Building level or a floor level within a fabric site.
- A fabric zone is created at a building level, all the floors within the building become part of the same fabric zone.
- A pool enabled for wireless needs to be manually added to the fabric zone to allow seamless roaming.

Site Hierarchy



Fabric Zones Considerations

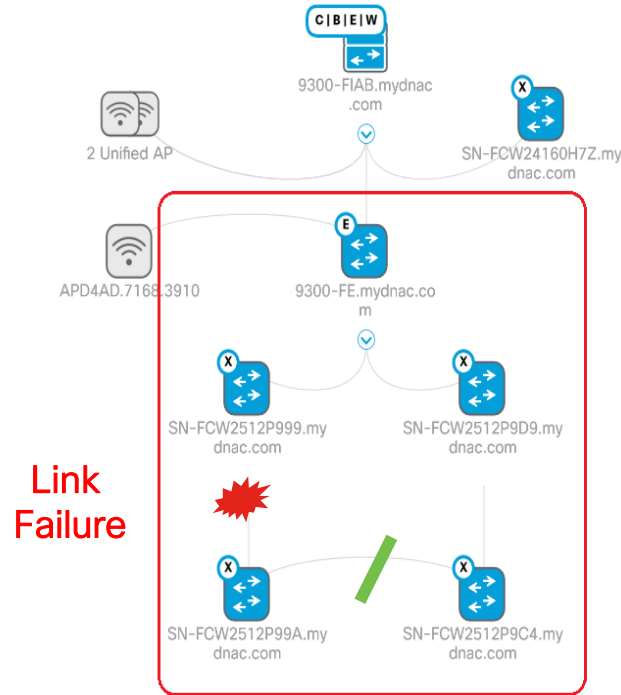
- Fabric zone can inherit all the pools within the VN or a selective pool within the VN by using the workflow on the Cisco Catalyst Center.
- All the properties of the Pool such as layer2 flooding directed-broadcast would be inherited on the fabric zone.
- The addition of CP/Border/WLC device is not allowed at the fabric zone. They need to be assigned at the parent fabric site only.
- When designing with a fabric zone , have the Border/CP and WLC at a site hierarchy layer where you don't intend to create a fabric zone.
- PEN/EN nodes within a fabric zone inherit the respective VLANs on the fabric zone.
- Any pool that is added to an existing VN in a fabric site, and if that pool needs to be used in a fabric zone will require explicit addition by using the workflow.



REP Ring Support

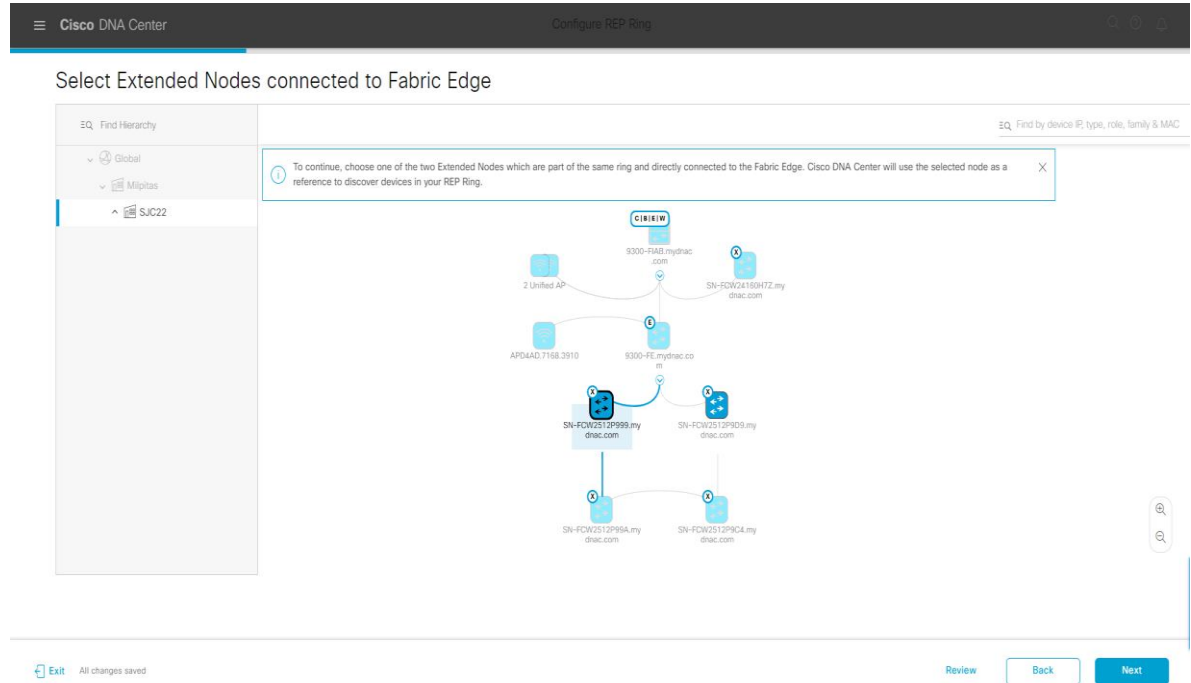
REP provides a way to control network loops, handle link failures, and improve convergence time

- Prerequisites:
 - STP Ring topology is already setup and devices are on-boarded in DNAC via PnP flow
 - Devices onboarded and provisioned successfully



REP Ring Workflow

1. Go to the fabric site and select Edge node where the ring is connected. Click REP Rings tab and Create REP Ring button
2. Select first adjacent extended nodes from the topology and go Next
3. Select last adjacent extended nodes from the topology and go Next
4. Review Selection



REP Ring Workflow Verification

User can see the status of the process

The screenshot displays the 'Configure REP Ring' interface in Cisco DNA Center. The page title is 'Configure REP Ring'. Below the title, the section 'REP Ring Configuration Status' is visible. A warning message states: 'Do not change any configuration on devices while REP Configuration is in progress.' Below this, the 'Ring-1' configuration details are shown. The 'RING DETAILS' section includes: Fabric Site (SJC22), Fabric Edge (9300-FE.mydnac.com), and Extended node devices connected to Fabric Edge (SN-FCW2512P999.mydnac.com, SN-FCW2512P909.mydnac.com). The 'PROGRESS DETAILS' section shows a progress bar at 50% and a list of steps: 'Start Ring Discovery' (completed), 'Discover Ring Members' (completed), and 'Configure Devices' (in progress). At the bottom, there is an 'Exit' button with the text 'All changes saved' and 'Back' and 'Next' buttons.

Cisco DNA Center

Configure REP Ring

REP Ring Configuration Status

View detailed step by step REP Ring Configuration progress

⚠ Do not change any configuration on devices while REP Configuration is in progress.

Ring-1

RING DETAILS

Fabric Site	SJC22
Fabric Edge	9300-FE.mydnac.com
Extended node devices connected to Fabric Edge	SN-FCW2512P999.mydnac.com, SN-FCW2512P909.mydnac.com

PROGRESS DETAILS

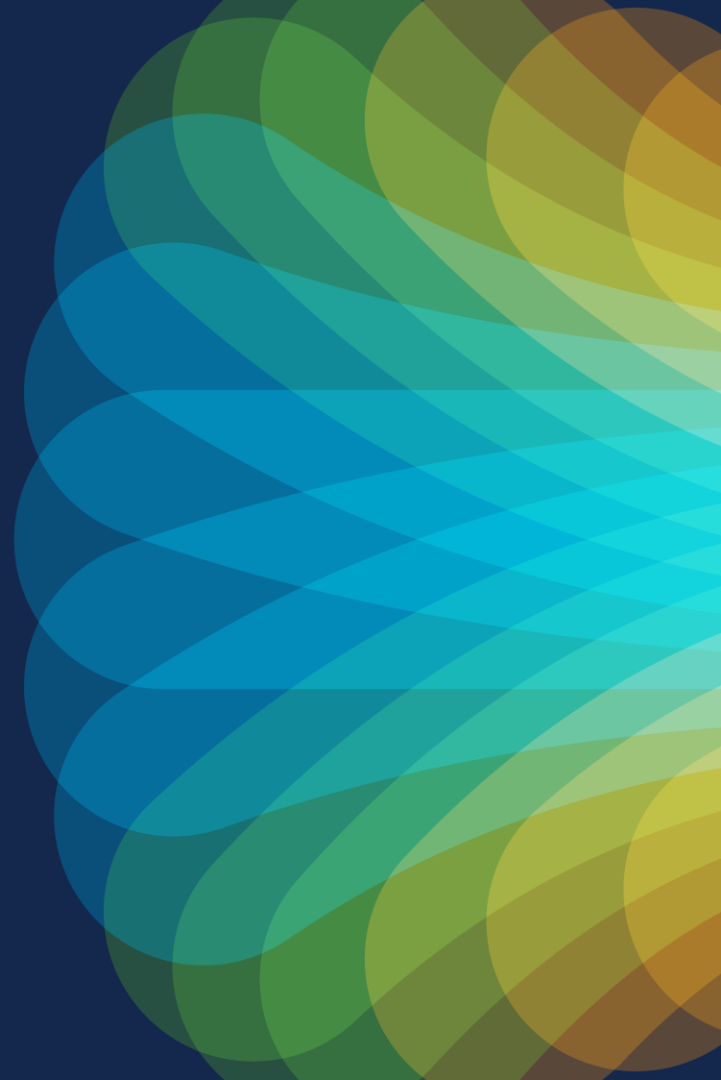
50%

- > Start Ring Discovery
- > Discover Ring Members
- > Configure Devices

Exit All changes saved

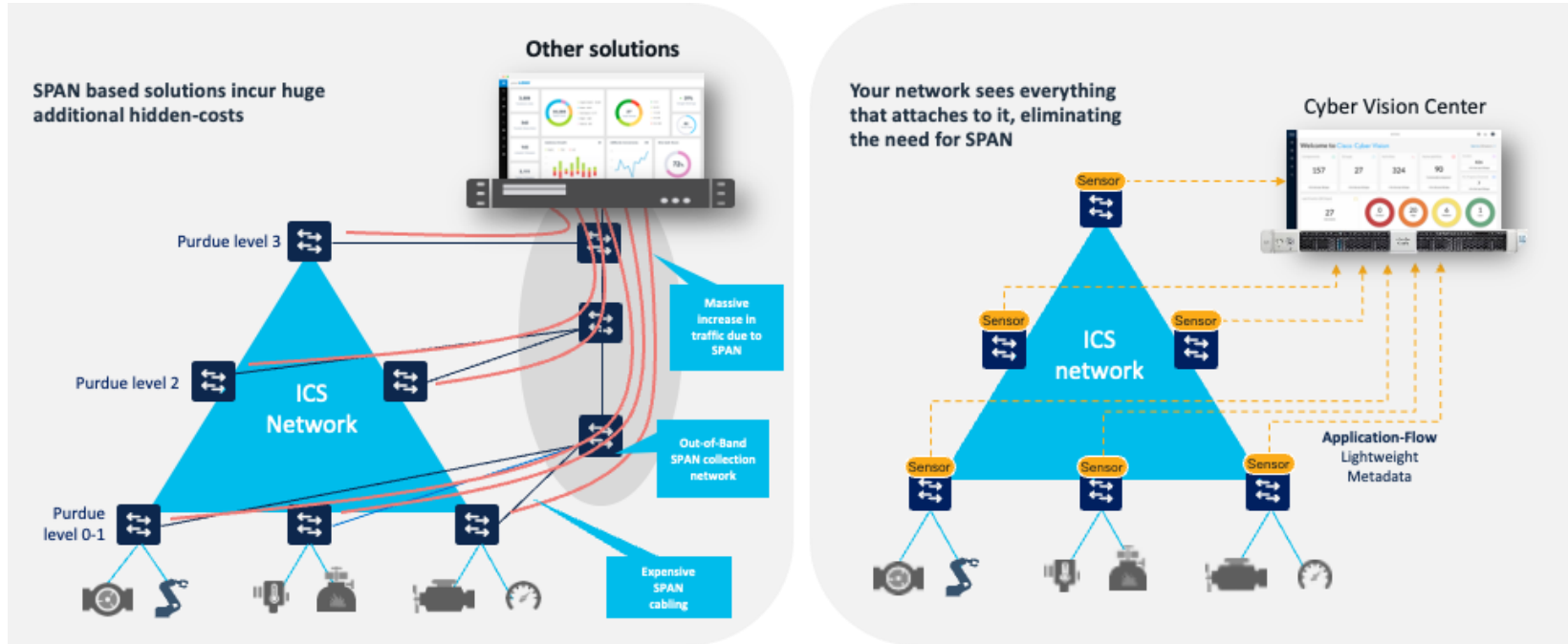
Back Next

Cyber Vision Sensor on SDA

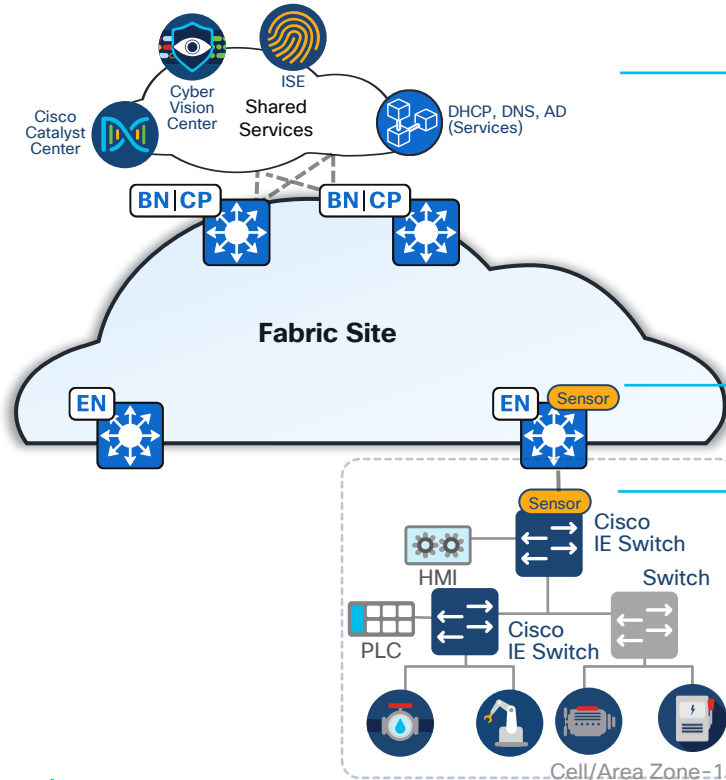


What is Network as a Sensor?

Discover endpoints and visualize application relationships



Cyber Vision on SDA Network



Cyber Vision Center is deployed at Shared Services

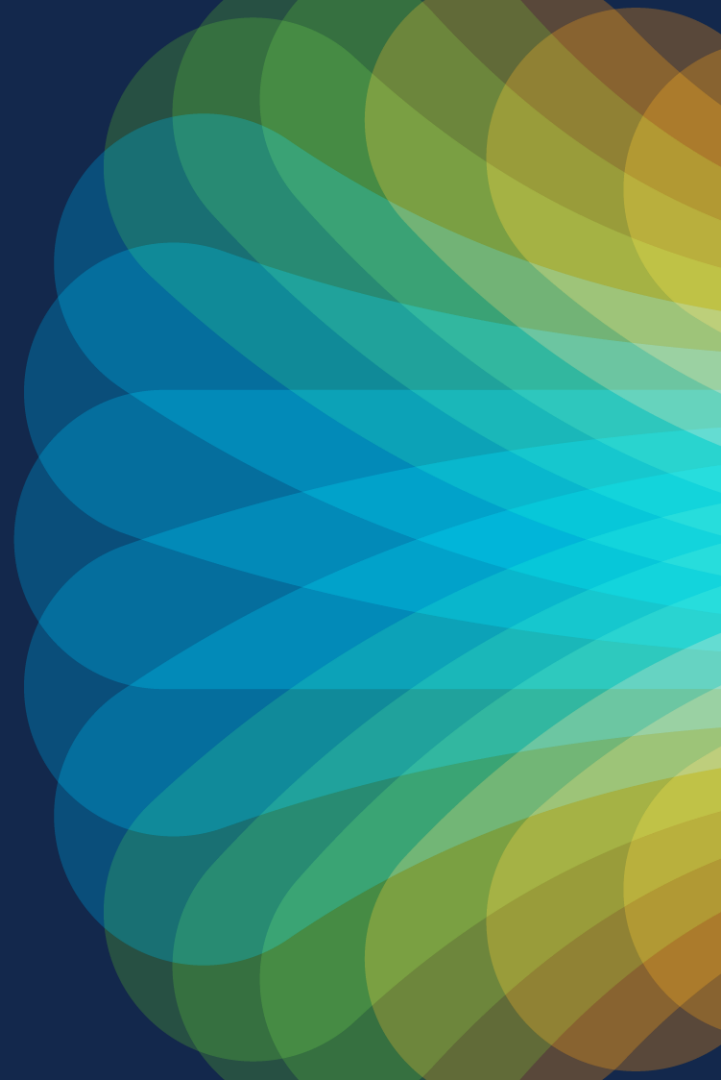
Cyber Vision may be deployed in FE (Cat9300, IE9300). Sensor collection IP needs to be part of the underlay

Cyber Vision on extended nodes/non-SDA IE switches (IE9300, IE3400, IE3300)

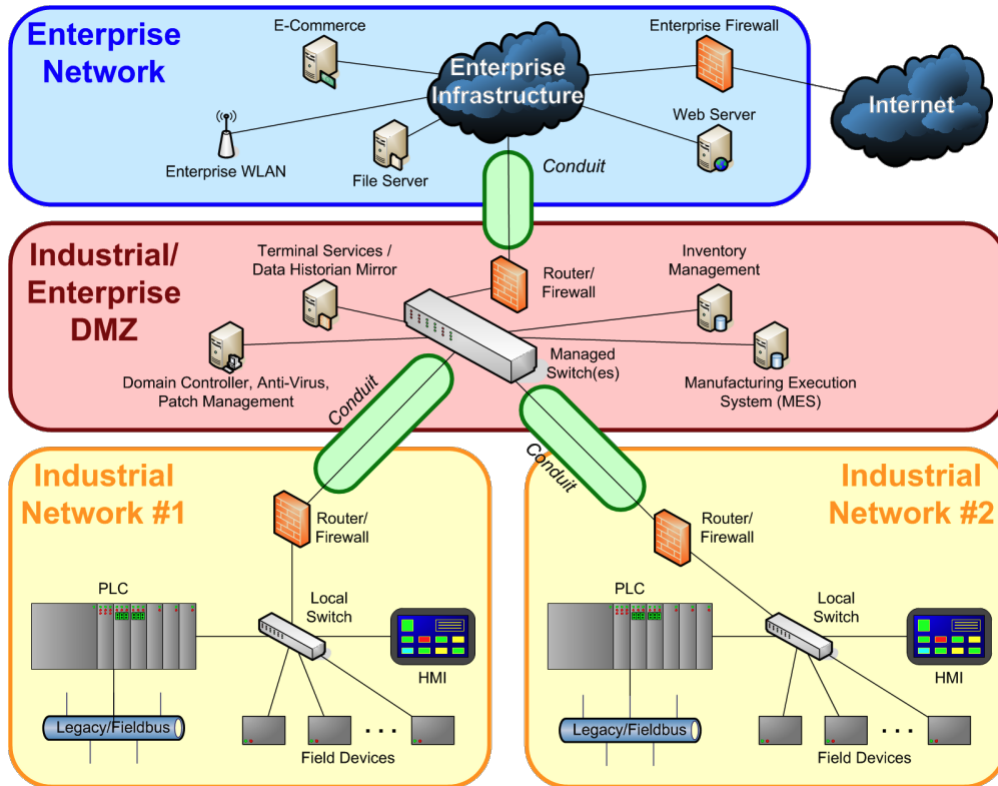
Cyber Vision Deployment

- Cyber Vision Sensor installation is not supported through Application Hosting on Catalyst Center. It is recommended to **deploy using sensor management extension** on Cisco Cyber Vision Center
- Templates on Catalyst Center could be used to configure ERSPAN, AppGig interface, monitoring sessions and exclude ERSPAN VLAN from trunks
- It is required to prune ERSPAN VLAN from all physical interfaces
- For sensors deployed on PEN/EN/Non-SDA industrial switches, configure separated VN for the collection network
- Sensors deployed on Fabric Edge should use a collection interface on the underlay.

TrustSec for the OT

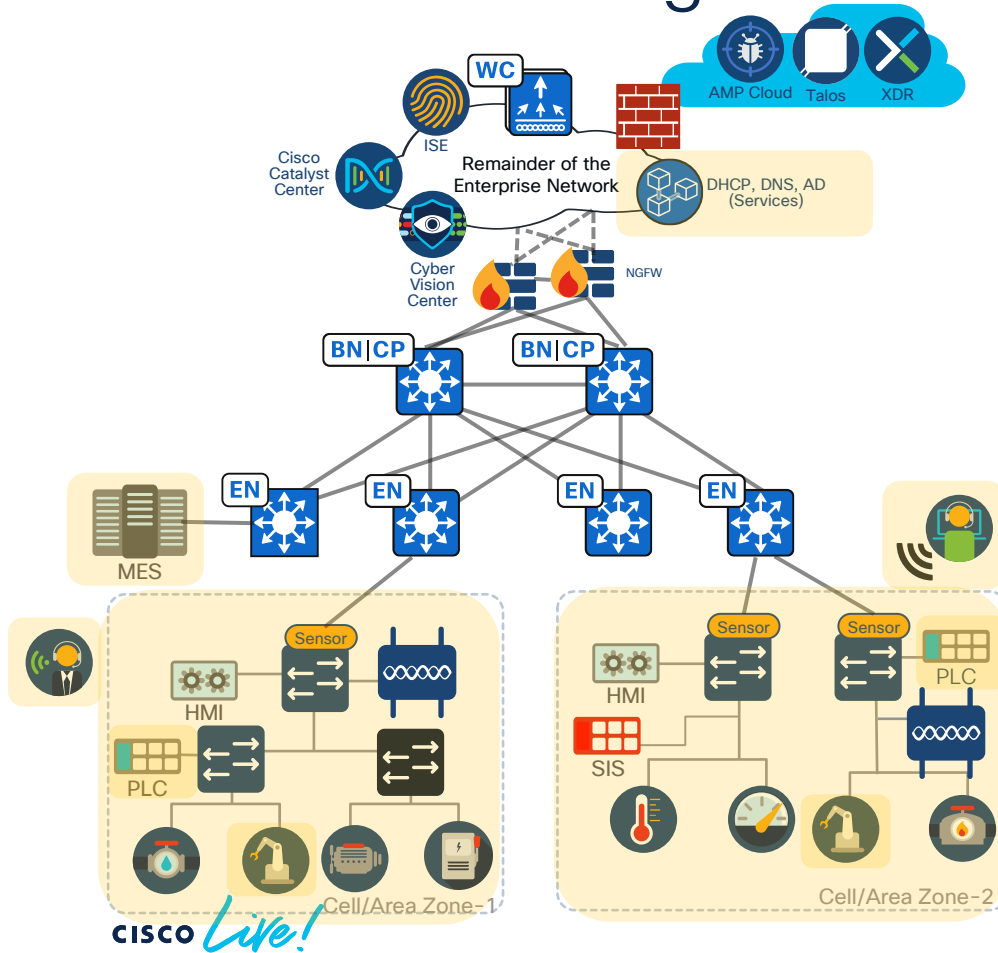


IEC 62443 Zones & Conduits



- **Zone:** Collection of entities that represent a partitioning of a System under Consideration (SUC) based on their functional, logical and physical (including location) relationship that share common security requirements
- **Conduit:** Physical or logical grouping of communication channels, intermittent or permanent, between connecting a zone with another zone or with the outside that share common security requirements
- The intent is to identify those assets which share common security characteristics in order to establish a set of common security requirements that reduce cybersecurity risk

OT Common Segmentation Requirements



1. All devices to the other devices within a zone
2. Interlocking devices between zones
3. ME applications to devices in specified zones
4. IT Applications to all zones
5. Robotic application to robots
6. Network admin to all devices
7. Mobile worker to all devices in specified zones

OT Segmentation requirements takeaways

Zone-Based Segmentation Adequacy:

Segmentation within a zone is generally unnecessary. Zones, defined by logical or functional groupings, inherently provide sufficient isolation. If a device in a zone is compromised, the process stops.

802.1x Limitations in OT Devices:

Most OT devices lack support for 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, reducing the necessity for extensive device profiling.

OT Endpoints and VLANs:

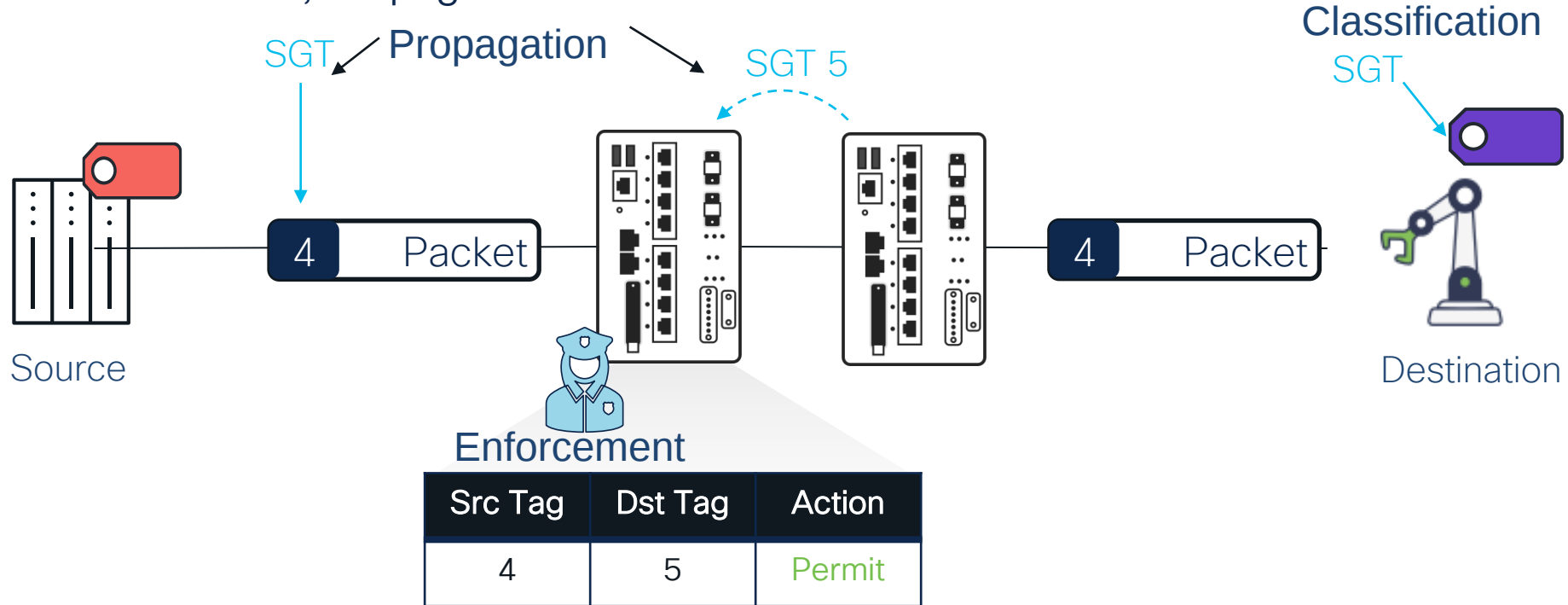
OT endpoints cannot be moved to another VLAN; they use static IP addressing.

TrustSec Support:

Industrial switches may not have full TrustSec support

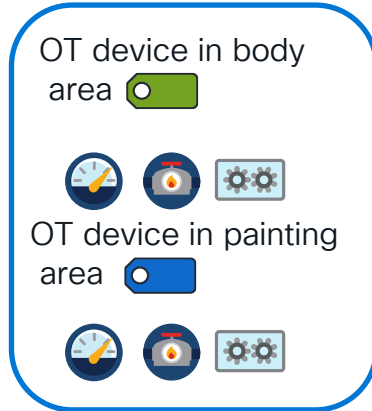
Cisco TrustSec – Key Concepts Review

Classification, Propagation and Enforcement



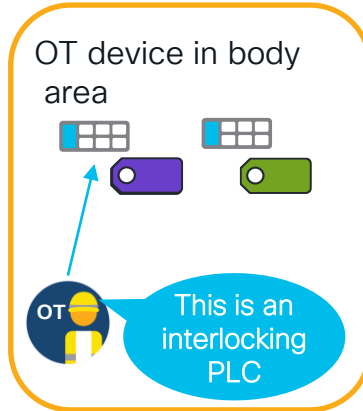
Classification in OT network

Static assignment based on location



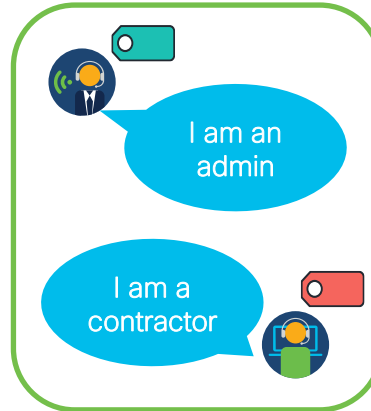
Use the network to answer: "Where are you?" (VLAN or Subnet)

Assignment for "named" devices



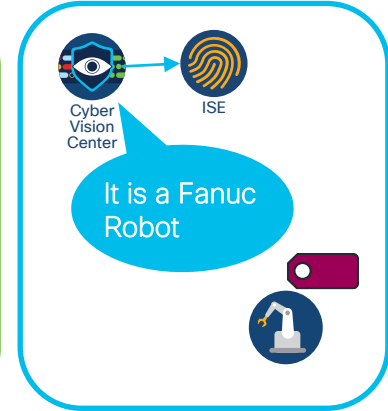
Use Cyber Vision to "promote"/change device tag

Dynamic assignment for users



Use credentials to confirm identity (802.1x)

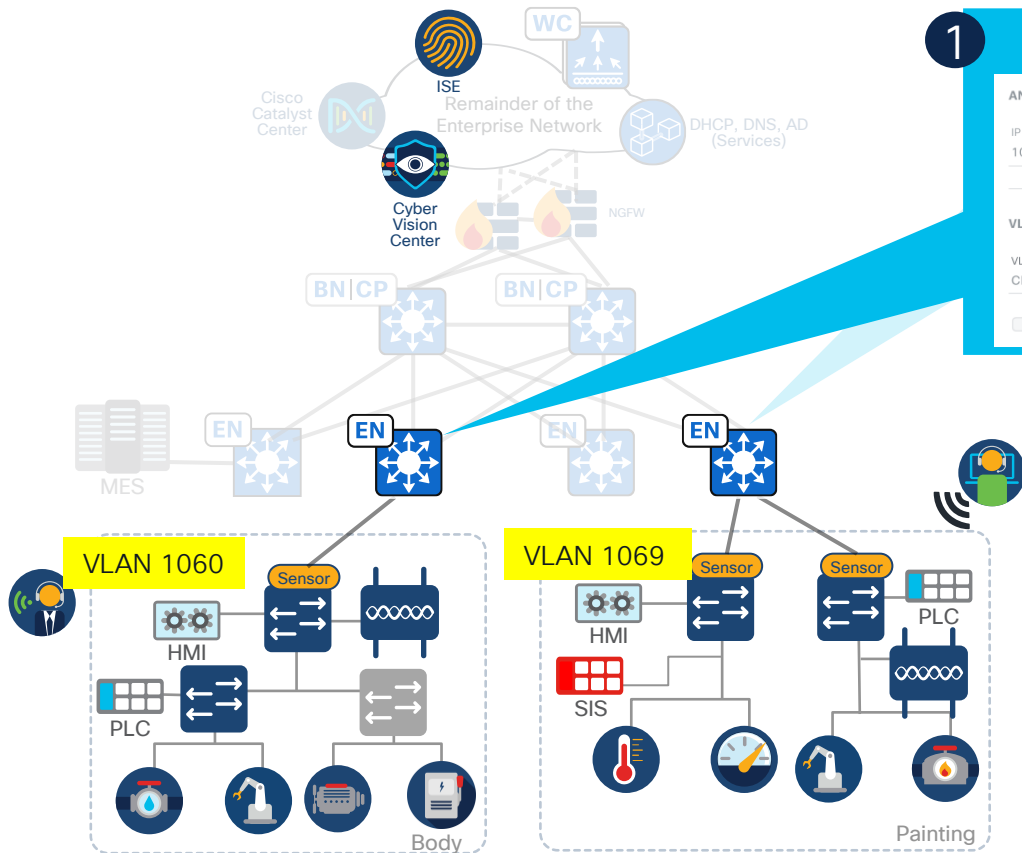
Dynamic assignment for OT devices



Use device attributes (ISE) and communication patterns (Cyber Vision) to profile device*

*Less common

Requirements for Classification in OT



1

Use Vlan to SGT:

ANYCAST GATEWAY

IP Address Pool*

100.0.8.0/21



☐ IP-Directed Broadcast

☐ Intra-Subnet

VLAN

VLAN Name

CPN-Data-Scale

VLAN ID

1069

Traffic Type



Data



Voice

Security Groups

OT_RT1069



☐ Auto generate VLAN name

2

Open authentication on access ports
(Dynamic tags overwrite Vlan to SGT)

3

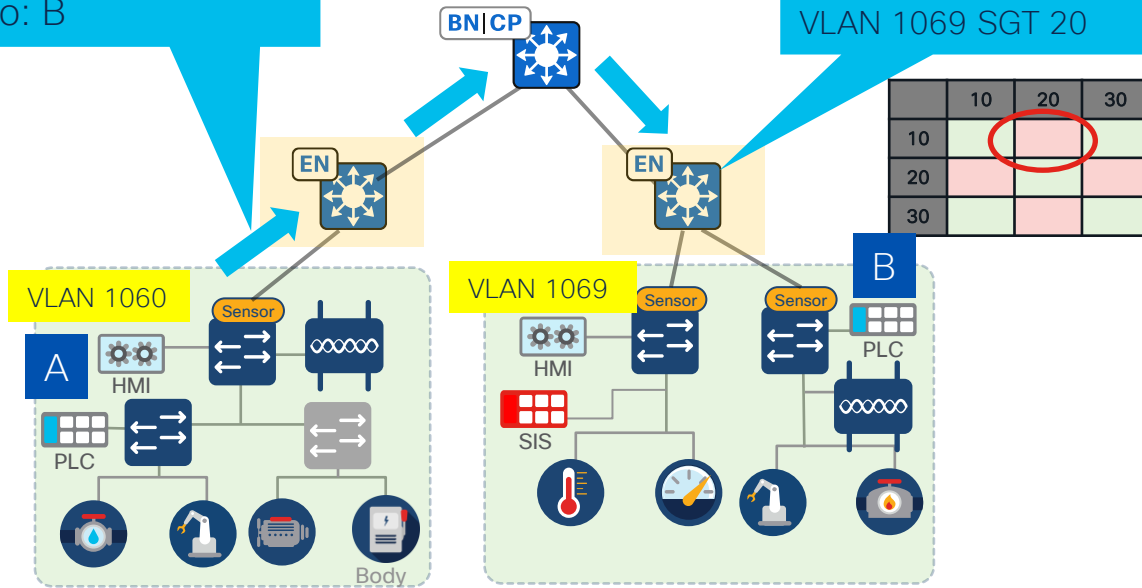
Use Cyber Vision for context /grouping

Enforcement in the OT

Recommendation is to enforce at the L3 boundary (Fabric Edge)

From: A (SGT 10)
To: B

B is in VLAN 1069
VLAN 1069 SGT 20



1. Connectivity over Security within the zone (enforcement inside the zone may not be desirable)

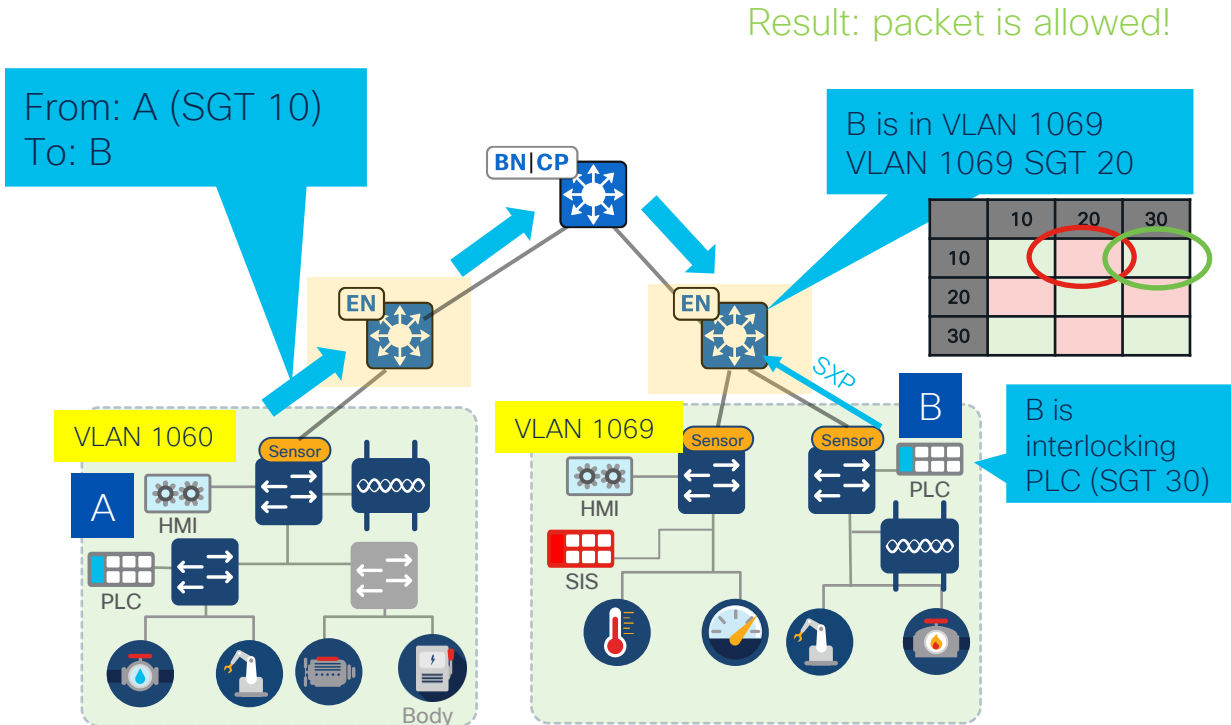
2. Least Privilege across zones (enforcement between zones is required)

3. TrustSec support may not be available on IE switches

Result: packet is denied!

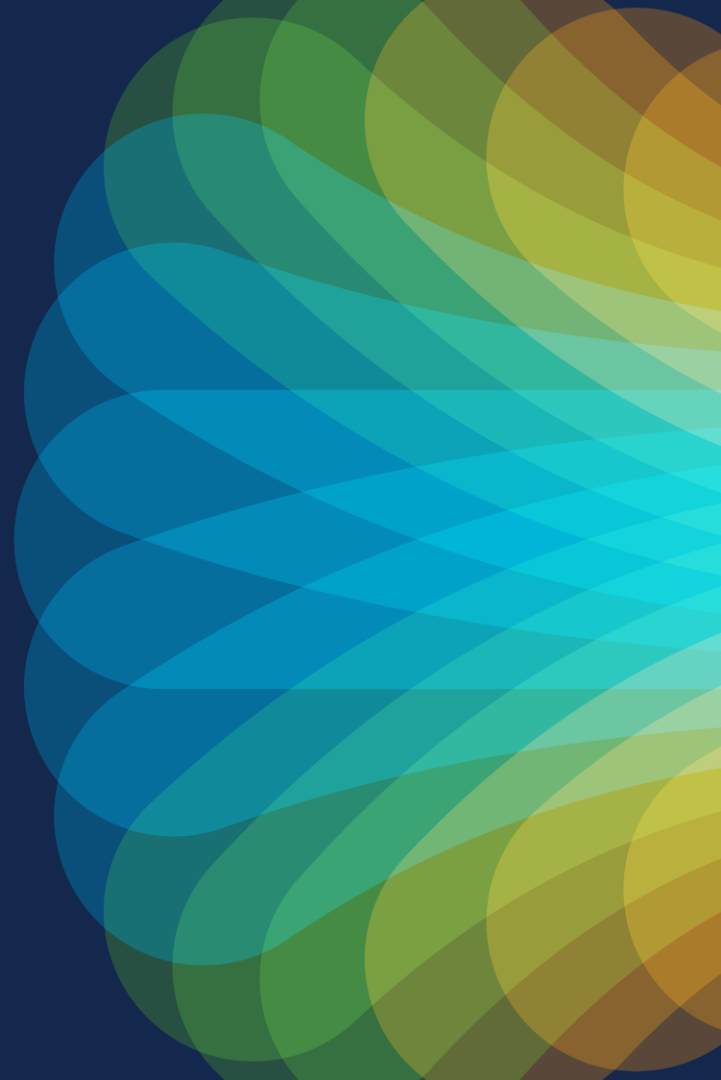
What if Destination Has a Dynamic Tag?

Propagation Example



- 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

A note on wireless options



A Note on Wireless Options

Option	SDA advantages	L2 Protocol support (i.e Profinet)	Mobility	MPO "PRP like"	Normal Endpoint Support	Managed by Catalyst Center	Local switching	Use Case
SDA centralized	Yes	No	WGB: roaming time < 100 ms	No	Yes	Yes	No	- Normal endpoints support - Stationary OT endpoints < 10-30ms - OT Mobility when critical requirements are not high
OTT centralized	No	No	WGB: roaming time < 100 ms	No	Yes	Yes	No	- Normal endpoints support - Stationary OT endpoints < 10-30ms - OT Mobility when critical requirements are not high - Used as migration step on when there is no support for SDA wireless
OTT Flex Connect Local Switching	No	Yes	WGB: roaming time < 100 ms	No	Yes	Yes	Yes	- Normal endpoints support - Stationary OT endpoints < 10-30ms - OT Mobility when critical requirements are not high - OT L2 protocol support
Cisco URWB	No	Yes	Zero millisecond handoff	Yes	No	No	No	- Critical traffic on AGV, AMR - OT protocols - Not suitable for normal endpoints - Good for point-to-point connectivity. i.e remote switch connected to underlay via wireless

Strong IT/OT relationship is required

Let's go

Join us for the ultimate
Cisco Live experience

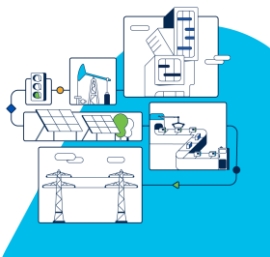
Anticipation | February 5-8, 2024

Let's come together to gain knowledge, cultivate a vision,
build community, share experiences, and explore the
possibilities of IT.

Please note: Registration closes on January 30 at midnight CET,
or sooner if we reach max capacity. Onsite registration will not be
available at this year's event.

Register Now

Ciscolive.com



IIoT Sessions at Cisco Live 2024

Technical Seminar

NEW ADVENTURES IN WIRELESS: THE JOURNEY OF WI-FI 6E AND PRIVATE 5G NETWORKS FOR THE ENTERPRISE - TECSPOT-2432

Mathias Fekner, Distinguished Architect, Cisco Systems, Inc. - **Distinguished Speaker**
Robert Barton, Distinguished Engineer, Cisco Systems, Inc. - **Distinguished Speaker**
Piero Rodriguez, Technical Solution Architect, Cisco Systems, Inc.

Schedule Monday, Feb 5 | 2:00 PM - 3:30 PM CET

Segmenting industrial networks with Trustsec and Cisco Identity Services Engine - TECSEC-3503

Andrew McPhee, Industrial Security Solution Manager, Cisco Systems, Inc.
Gyorgy Acs, Technical Solutions Architect, Cisco Systems, Inc.

Schedule Monday, Feb 5 | 2:15 PM - 3:45 PM CET

Dive into the depths of Industrial Resiliency Protocols - TECIoT-2201

Albert Mitchell, Technical Marketing Engineer, Cisco Systems, Inc.
Erika Franco, Technical Leader, Cisco Systems, Inc.

Schedule Monday, Feb 5 | 2:00 PM - 3:30 PM CET

Package Prices

	Early Bird Last November 14, 2023	Standard November 16, 2023 - January 25, 2024	Last January 28, 2024
Full Conference Participate in all Cisco Live has to offer	Not available	EUR 2,500 + VAT* or 36 Learning Credits**	EUR 3,000 + VAT*
IT Leadership Designed for IT leaders looking to grow knowledge and network skills	Not available	EUR 2,500 + VAT* or 42 Learning Credits**	Not available
Explorer Experience highlights, innovation talks, and the fun of Cisco Live	Not available	EUR 1,000 + VAT* or 15 Learning Credits**	EUR 1,200 + VAT*

Registration closes on January 30 at midnight CET. Onsite registration will not be available at this year's event.
*Prices include the full Cisco Live experience, including access to all sessions, networking opportunities, and more.
**Prices include the full Cisco Live experience, including access to all sessions, networking opportunities, and more.
***Prices include the full Cisco Live experience, including access to all sessions, networking opportunities, and more.

Explorer/Full Conference Pass

Automotives driving Cutting-edge network technology powered by Cisco - CSIOI-1686

Russ Vickers Vickers, CEO, Future Mobility Campus Ireland
Pete Kavanagh, Principal Architect, Cisco Systems, Inc.

Schedule Wednesday, Feb 7 | 10:45 AM - 11:30 AM CET

Empowering Network Engineers: A Deep Dive into AI, Automation, and Cybersecurity Trends - PARNW-1470

Danilo Wieding, Vice President, Strategy & Product Management, Springer

Schedule Tuesday, Feb 6 | 1:45 PM - 2:00 PM CET

Fueling the Future: Reinventing Gas Stations for Tomorrow - DEVLIT-1027

Sebastian Scharf, Solutions Engineer, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 2:00 PM - 2:30 PM CET

How Harbor secures their OT and IoT technologies to ensure a consistent sweet taste worldwide - CSSEC-1813

Andre Diering, Head of Corporate IT Operations Network & Security, HARBOR IT Dienstleistungs GmbH & Co. KG
Markus Wieding, Senior Specialist - IoT, Cisco Systems, Inc.

Schedule Wednesday, Feb 7 | 9:30 AM - 10:15 AM CET

Unlock New Revenue Streams With Cisco Mobility Services - PSOSP-1727

Andreas Christy, Director Product Management, Cisco Systems, Inc.

Schedule Wednesday, Feb 7 | 12:30 PM - 1:30 PM CET

Technical Seminars

Technical Seminars are available on Monday, February 5, 2024. Technical Seminars carry an additional fee and cannot be purchased without a Full Conference or Explorer Learning Pass. Fees are per person and subject to change without notice.

	Cost
One (1) 4-hour Technical Seminar	EUR 100 + VAT* or 15 Learning Credits**
One (1) 8-hour or Two (2) 4-hour Technical Seminars	EUR 180 + VAT* or 27 Learning Credits**

Full Conference Pass

~40°C Industrial Networking: Where Enterprise Products Fear to Go - BRKIOT-2104

Albert Mitchell, Technical Marketing Engineer, Cisco Systems, Inc.
DJ Cole, Technical Marketing Engineer, Cisco Systems, Inc.
Svenner Tjellum, IoT Wizardry, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 4:45 PM - 6:15 PM CET

5 ways to improve outcomes with digital transformation for roadways - IBOIoT-2471

Angela Murphy, Product Marketing Manager, Cisco Systems, Inc.
Pete Kavanagh, Principal Architect, Cisco Systems, Inc.

Schedule Thursday, Feb 8 | 11:45 AM - 12:45 PM CET

8 Tips for Deploying Indoor Wireless Mobility with Cisco Industrial Wireless - BRKIOT-2601

DJ Cole, Technical Marketing Engineer, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 11:45 AM - 1:15 PM CET

Assessing Software-Defined Access (SDA) for Industrial Automation: Best Practices for a Successful Deployment - BRKIOT-2299

Erika Franco, Technical Leader, Cisco Systems, Inc.
SAMI Nasrallah, TECHNICAL LEADER SOFTWARE ENGINEERING, Cisco Systems, Inc.

Schedule Friday, Feb 9 | 9:15 AM - 10:45 AM CET

Connected Factory Architecture - BRKIOT-2720

Anu Siddeswaran, Director, Solution Engineering, Cisco Systems, Inc.

Schedule Wednesday, Feb 7 | 10:30 AM - 12:00 PM CET

Connecting and Securing Renewable Energy - Enabling Green Technologies with Cisco IoT - BRKIOT-1203

Markus Smith, Utilities & Renewable Energy Solution Manager, Cisco Systems, Inc. - **Distinguished Speaker**

Schedule Thursday, Feb 8 | 10:45 AM - 1:45 PM CET

Connecting moving assets with Cisco IoT Solutions - BRKIOT-1126

Emanuel Tjellum, IoT Wizardry, Cisco Systems, Inc.

Schedule Wednesday, Feb 7 | 3:45 PM - 4:45 PM CET

Creative and unusual use case ideas for industrial networking devices. - BRKIOT-2808

Marvin Sreter, Technical Solutions Architect, Cisco Systems, Inc.

Schedule Thursday, Feb 8 | 5:00 PM - 6:00 PM CET

Cybersecurity Awareness for Our Critical Infrastructure Water Customers - BRKIOT-2368

Thomas Archuleta, Technical Solutions Architect, Cisco Systems, Inc.

Schedule Thursday, Feb 8 | 2:30 PM - 4:00 PM CET

Implementing Segmentation in Industrial Networks - BRKIOT-2882

Andrew McPhee, Industrial Security Solution Manager, Cisco Systems, Inc.

Schedule Wednesday, Feb 7 | 8:30 AM - 10:00 AM CET

The New Digital Substation - more efficient, more secure and ready for demanding modern Grid applications - BRKIOT-2015

Markus Smith, Utilities & Renewable Energy Solution Manager, Cisco Systems, Inc. - **Distinguished Speaker**
Edward Aguilera, Systems Engineering Leader, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 3:15 PM - 4:15 PM CET

Industrial PoE: The Ultimate Guide for Beginners - BRKIOT-1128

Albert Mitchell, Technical Marketing Engineer, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 1:30 PM - 2:30 PM CET

Let's get Physical with IoT Wireless - BRKIOT-2265

Igor Mislove, Technical Solutions Architect, Cisco Systems, Inc. - **Distinguished Speaker**

Schedule Thursday, Feb 8 | 12:00 PM - 1:30 PM CET

Mission-Critical OT Network Best Practices Using Private 5G Wireless Services - BRKSPM-3581

Flavia Steinhilber, Systems Architect, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 4:45 PM - 6:15 PM CET

Modernizing Critical Infrastructure Utility and Railway WAN Transport with SR and EVPN - BRKSP-2776

Angela Bane, Technical Marketing Engineer, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 8:00 AM - 9:00 AM CET

Securing Industrial IoT Networks - A look at ISA/IEC-62443 and How Cisco Can Help Secure the IoT Network - BRKIOT-1527

Nancy Cam-Winget, Cisco Fellow, Cisco Systems, Inc. - **Distinguished Speaker**
Andrew McPhee, Industrial Security Solution Manager, Cisco Systems, Inc.

Schedule Tuesday, Feb 6 | 8:00 AM - 9:00 AM CET

Securing Industrial Networks: Where to start - using Cyber Vision for OT Asset Visibility - BRKIOT-2910

Nicolas Deville, IOT Security Product Manager, Cisco Systems, Inc.
Steve Matthews, Technical Solutions Architect, Cisco Systems, Inc.

Schedule Thursday, Feb 8 | 8:45 AM - 10:15 AM CET

Stronger Together: Uniting IT and OT Security with Cyber Vision - LTRSEC-2381

Peet Durrant, Technical Product Systems Engineer, Cisco Systems, Inc. - **Distinguished Speaker**
Michal Maciejczak, Solution Delivery Architect, Cisco Systems, Inc. - **Distinguished Speaker**
Zach Alford, Security Solution Architect, Cisco Systems, Inc.

Schedule Thursday, Feb 8 | 2:00 PM - 6:00 PM CET

IOT Learning Map

Internet of Things

Transform your IoT Infrastructure

In this new IoT world, the network is the nervous system that allows everything to work together. And while it's creating limitless possibilities, it also introduced more complexity. Today everything is a connected device, from a robot to a power transformer, from a vehicle to crane.

CISCO *Live!*
Amsterdam | February 5-9, 2024

START

Monday, February 5 | 8:30 a.m.
TECIOT-1000

IoT Fundamentals Bootcamp

Monday, February 5 | 8:45 a.m.
TECIOT-2584

Designing IoT Wireless Networks

Monday, February 5 | 2:00 p.m.
TECIOT-2201

Dive into the depths of Industrial Resiliency Protocols

Tuesday, February 6 | 11:30 a.m.
BRKIOT-2601

8 Tips for Deploying Indoor Wireless Mobility with Cisco Industrial Wireless

Tuesday, February 6 | 3:30 p.m.
IBOIOT-1083

Sensors, sensors everywhere! Using LoRaWAN and Cisco Industrial Asset Vision

Tuesday, February 6 | 4:45 p.m.
BRKIOT-2104

-40C Industrial Networking: Where Enterprise Products Fear to Go

FINISH

Wednesday, February 7 | 3:45 p.m.
BRKIOT-1126

Connecting moving assets with Cisco IoT Solutions

Thursday, February 8 | 11:45 a.m.
IBOIOT-2471

5 ways to improve outcomes with digital transformation for roadways

Thursday, February 8 | 12:00 p.m.
BRKIOT-2265

Let's get Physical with IoT Wireless

Thursday, February 8 | 5:00 p.m.
BRKIOT-2808

Creative and unusual use case ideas for industrial networking devices.

Thursday, February 8 | 5:00 p.m.
IBOIOT-2501

Cisco Catalyst WAN Manager for OT/Industrial Networks: Fabric or non-fabric, which is right for me?

Friday, February 9 | 9:15 a.m.
BRKIOT-2299

Assessing Software-Defined Access (SDA) for Industrial Automation: Best Practices for a Successful Deployment

If you are unable to attend a live session, you can watch it in the On-Demand Library after the event.



The bridge to possible

Thank you

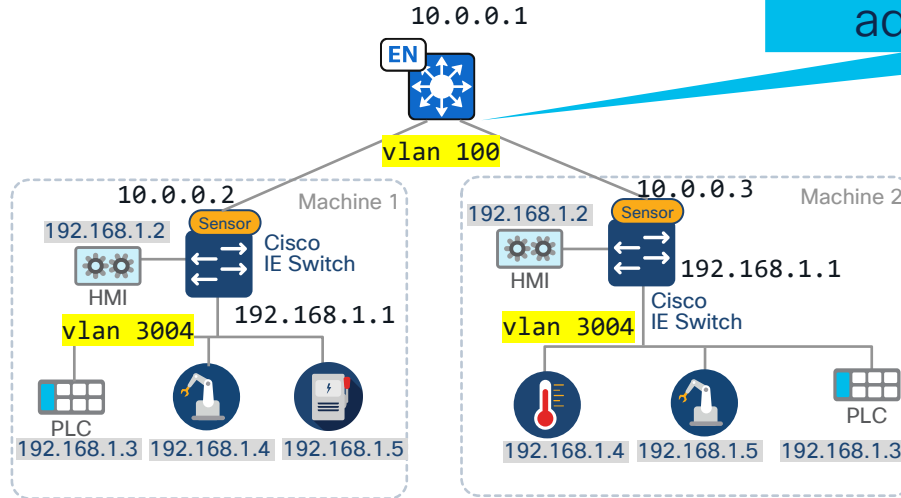
CISCO *Live!*

Backup slides

this slide starts the backup slides for L2NAT
and special segmentation cases.
Slides after this are not intended for formal
presentation.
Remain in ppt as a technical resource

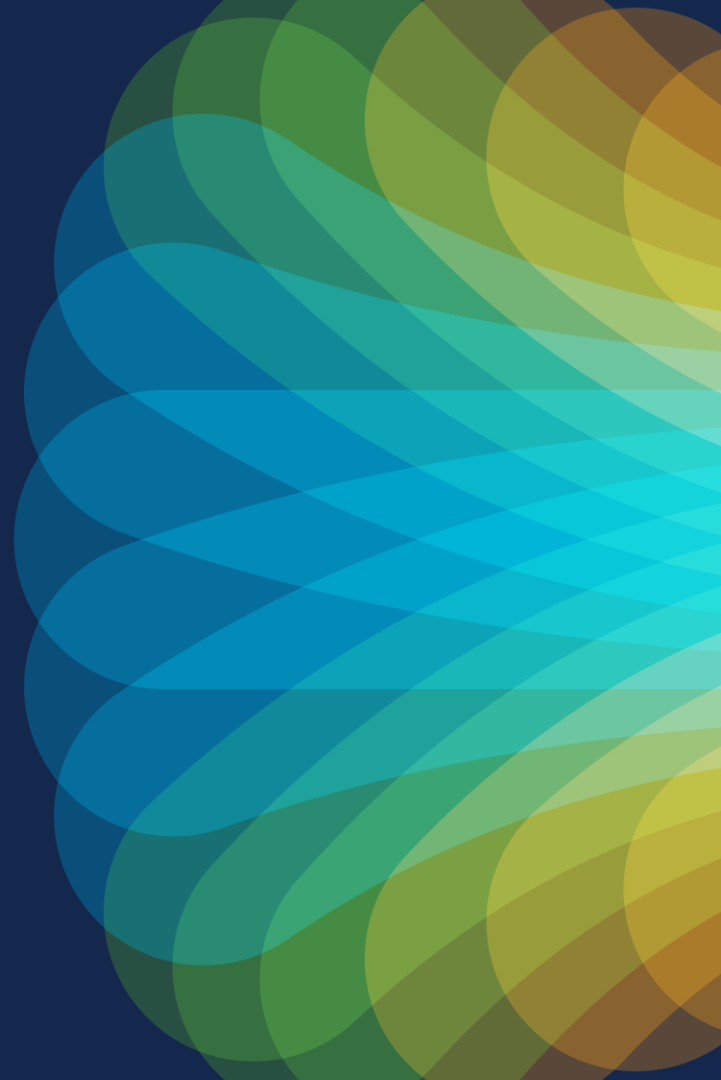
L2NAT Example

Sees multiple IPs to single MAC address as switch is "routing"



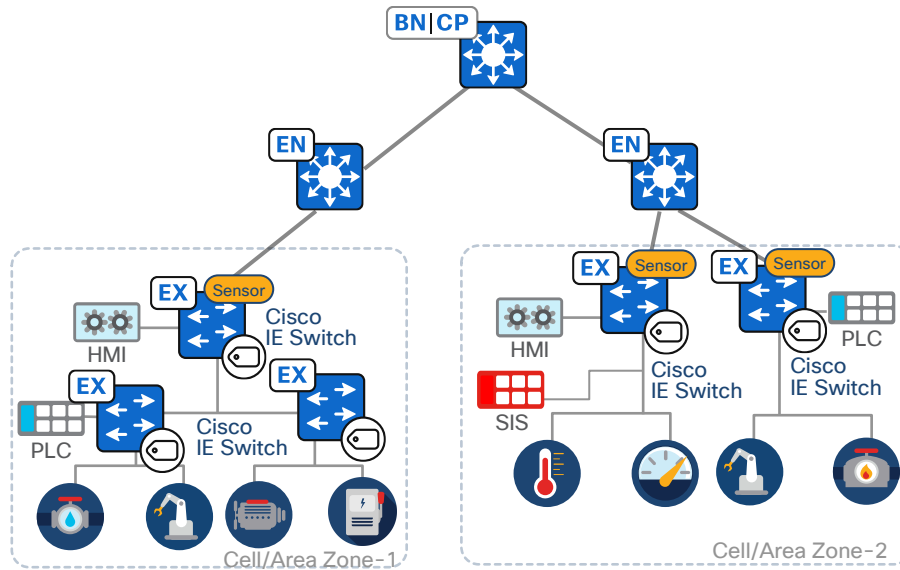
Eliminate machine to machine Broadcast:
different vlan 'private' from 'public'
Vlan 3004 inside machine
Vlan 100 outside machine
IE switch 'routes' between vlans.
IE switch is L3 GW for 192.168.1.x

Special Segmentation Cases



Case 1: What if I have only IE3400/IE9300?

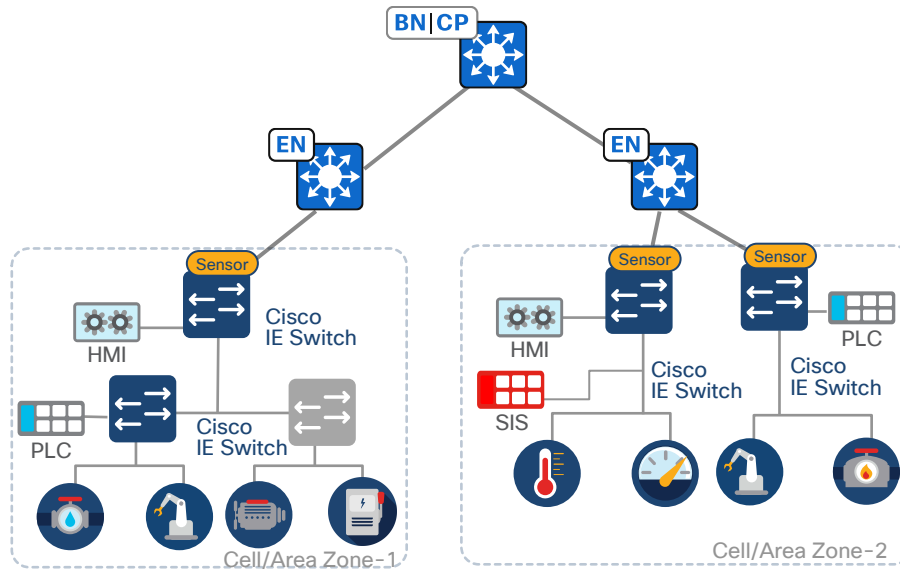
Could I enforce at the access?



- If all switches support enforcement, it is possible to enforce at the access.
- There is no need to use SXP
- Nodes could be PEN or non-Fabric
- Make sure policy does not get in the way of critical connectivity
- Not compatible with PTP

Case 2: Could I Use Vlan to SGT only?

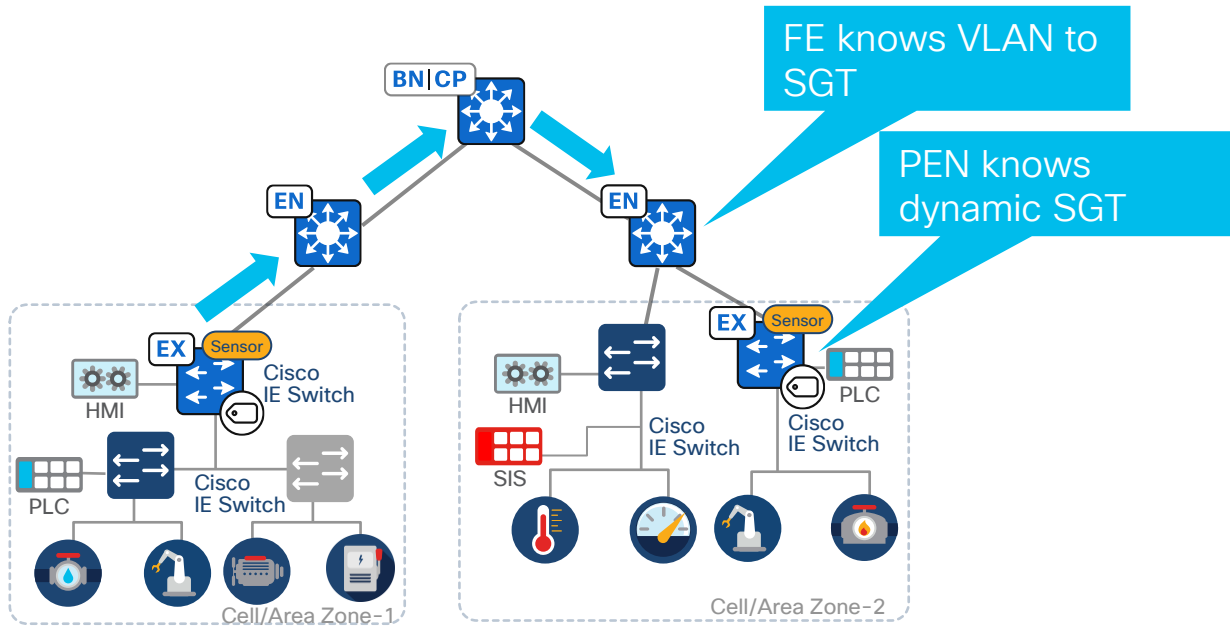
No SXP propagation



- Vlan to SGT only provides “zone to zone” segmentation only.
- Make sure different zones use different Vlans
- It cannot be mixed with dynamic authentication unless propagation of dynamic tags is configured

Case 3: Avoid Incorrect Enforcement

Enforcing early based on Vlan to SGT could lead to undesirable results

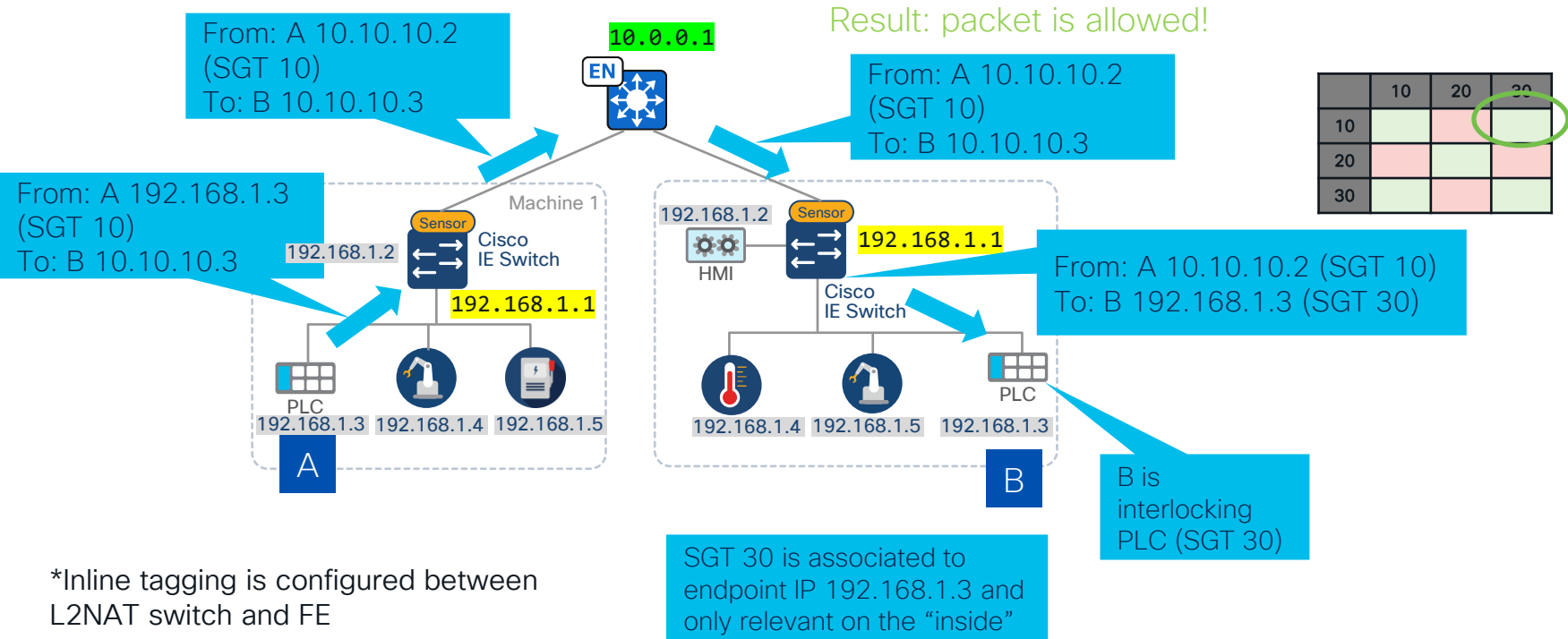


FE + PEN topology could lead to enforcement based on Vlan instead dynamic tag, either:

- Use EN instead PEN
- Disable enforcement on the FE downlink

Case 4: L2NAT Case

Enforce on L2NAT switch when dynamic tags are applied



*Inline tagging is configured between L2NAT switch and FE

The background of the slide is a vibrant, abstract graphic. It features a large, stylized cloud shape on the left side, composed of overlapping, semi-transparent layers of orange, red, and yellow. To the right of the cloud, a bright, multi-colored sunburst or starburst pattern radiates outwards, transitioning through a spectrum of colors including yellow, green, blue, and purple. The overall effect is energetic and colorful.

cisco *Live!*

Let's go