



Validated Profile: Manufacturing Vertical

Solution Overview 2

Hardware and Software Specifications 3

Solution Use Case Scenarios 4

Topology 6

Scale 7

Solution Key Notes 8

References 21

Solution Overview

This guide provides guidance on a typical operational technology (OT) network deployment profile that uses Cisco DNA Center and Cisco SD-Access. You can use this guide as a validation reference.

OT networks have followed the Purdue model (which was released in 1990) for the last couple of decades. Since its release, significant changes have occurred in the networking industry and these innovations are leveraged in the OT industry today.

The following sections describe the key considerations for a large evolving Manufacturing IT/OT network that needs to meet today's automation requirements.

Resiliency, Redundancy, and High Availability

As OT networks have become critical to an organization's functionality (as in many cases, an OT network is the core of a company's standing), it's critical to provide strict network- and service-level resiliency. Network-level resiliency is achieved with a robust fabric network design that includes dual-fabric borders nodes, dual-fabric control plane nodes, dual-anchor borders and control plane nodes, dual wireless controllers, fabric switches with either hardware stacking or StackWise Virtual, a REP ring of IE extended nodes, and dual-fabric transit control plane nodes (where applicable). Service-level resiliency is achieved by deploying the following:

- A Cisco DNA Center three-node cluster.
- A distributed Cisco Identity Services Engine (ISE) cluster with multiple Policy Administration Nodes (PAN), Monitoring Nodes (MNT), as well as active and standby Platform Exchange Grid (pxGrid) and local Policy Service Nodes (PSN).

Security and Network Segmentation

Today's OT network sometimes provides limited segmentation capabilities. Mostly these networks are VLAN based. When deeper segmentation is needed, many organizations create physically separate OT networks. To solve this issue, network administrators use logical segmentation, which has the strength of physical separation and the simplicity of a single network. This segmentation can also help address cybersecurity issues. If segmentation is instantiated by IP Access Control Lists (ACLs), it can become difficult to scale, troubleshoot, and maintain over time in most simple deployments.

Within the Cisco SD-Access architecture, Cisco DNA Center and Cisco ISE work together to provide automation for planning, configuration, segmentation, identity, and policy services. Note that Cisco ISE is responsible for device profiling, identity services, policy services, and dynamically exchanging information with Cisco DNA Center.

The Cisco SD-Access solution addresses the need for complete data and control plane isolation between IT devices and manufacturing floor devices by using *macrosegmentation*. By creating and putting different devices into different overlay virtual networks (VNs), the manufacturing OT network achieves complete data isolation and provides security among different IT departments.

Cisco SD-Access also addresses the need for granular data plane isolation between endpoints within the same VN by using *microsegmentation* with scalable group tags (SGT) for Group-Based Policy (GBP). Cisco DNA Center IT administrators create groups, place employees in those groups by their roles, and define the policies that control how these groups can interact with each other.

Silent Hosts Handling

In the OT network, one of the biggest issues is the *silent hosts* on the manufacturing floor. Some endpoints on this floor are silent hosts. These silent endpoints do not broadcast their presence in the network. Cisco DNA Center offers a solution to silent hosts through the Layer 2 flooding capability. Layer 2 flooding enables the flooding of broadcast, link-local multicast, and ARP traffic for a given overlay subnet. This capability maps the overlay subnet to a dedicated multicast group in the underlay, encapsulates the

targeted traffic in a fabric Virtual Extensible LAN (VXLAN), and then sends the data to the destination underlay multicast group. This solution makes use of PIM Any-Source Multicast (PIM-ASM) in the underlay, which can be configured automatically (using the Cisco DNA Center LAN Automation workflow) or manually (in the later phase of deployment). This solution offers flexibility to OT networks by accommodating various OT devices with different embedded capabilities.

Layer 2-Only VN (Gateway Outside the Fabric)

OT networks have naturally a high number of Layer 2 networks in their factory floors for various use cases and business purposes. To gain a high level of security, you need to have the Layer 2 traffic inspected by a firewall outside of the fabric network. This requirement means that the first hop for all the traffic needs to be outside the fabric. This implementation uses a combination of Layer 2-only VN and underlay multicast features.

Network Assurance and Analytics

Network administrators can efficiently manage and monitor their networks to quickly respond to the OT system's dynamic needs. The deployment proactively predicts network-related and security-related risks by using telemetry to improve the performance of the network, devices, and applications. Cisco DNA Assurance, with the use of Cisco AI Network Analytics, collects telemetry data, monitors the performance of network devices, flags any issues that it detects, and offers remediation steps.

With Cisco DNA Assurance and Cisco AI Network Analytics, network administrators can monitor not only the overall health of the network devices and connected endpoints (both wired and wireless) but can determine the individual health of the devices, endpoints, and their applications. With this 360-degree analytics, administrators can identify the individual issues that network elements are facing, such as wireless laptop connectivity or an OT device's connection to a wireless SSID.

Cisco AI Endpoint Analytics

Modern security threats seek to exploit a single vulnerable point of entry in an Enterprise network for Enterprise information. When an entry point is breached, a lateral spread of threats across devices can spread in mere seconds. Granular network segmentation, like the Cisco SD-Access solution, is the preferred method to prevent this kind of lateral spread of threats. The OT network traditionally contains thousands of similar devices, such as automated guided vehicles (AGVs), programmable logic controllers (PLCs), and various manufacturing equipment and monitoring devices. Finding and identifying all the devices on a network is time-consuming and tedious. Cisco AI Endpoint Analytics addresses this issue by identifying the devices by type, manufacturer, communication protocols, and ports through passive network telemetry monitoring and deep packet inspection of the network.

Cisco DNA Center also shares the endpoint classification attributes with Cisco ISE. When new devices onboard through identity-based authentication, they can be automatically identified by the manufacturer and type and then are added to the appropriate group. It's easier to define and enforce security policies when these policies are applied to groups rather than individual endpoints. Group-based policies can be easily edited to adapt to new circumstances, such as security breakage by endpoints, and applied globally to an entire network.

Hardware and Software Specifications

The solution is validated with the hardware and software listed in the following table. For the complete list of hardware supported, see the [Cisco Software-Defined Access Compatibility Matrix](#).

Role	Model Name	Hardware Platform	Software Version	Software Version
Cisco DNA Center Controller	DN2-HW-APL-XL	Cisco DNA Center Appliance 3-Node Cluster	2.3.3.7	2.3.5.5

Role	Model Name	Hardware Platform	Software Version	Software Version
Identity Management, RADIUS Server	ISE-VM-K9	Cisco Identity Services Engine Virtual Appliance	3.1 Patch 2	3.2 Patch 2
	SNS-3695-K9	Secure Network Server for Cisco ISE Applications (large)		
Cisco SD-Access Fabric Control Plane Node	ASR1001-X	Cisco 1000 Series Aggregation Services Routers	17.6.6a	17.6.6a, 17.9.4a
	C9500-24Y4C	Cisco Catalyst 9300/9500 Series Switches	17.6.6a	17.6.6a, 17.9.4a
	C9500-24Q			
	C9300-48P			
C9300-24P				
Cisco SD-Access Fabric Border	C9500-24Y4C	Cisco Catalyst 9300/9500 Series Switches	17.6.6a	17.6.6a, 17.9.4a
	C9500-40X			
	C9500-12Q			
	C9500-24Q			
	C9300-48P			
	C9300-24P			
Cisco SD-Access Fabric Edge	C9300-48P	Cisco Catalyst 9300 Series Switches	17.6.6a	17.6.6a, 17.9.4a
	C9300-24P			
Cisco SD-Access Wireless Controller	C9800-80-K9	Cisco Catalyst 9800-80 Wireless Controller	17.6.6a	17.6.6a, 17.9.4a
Cisco SD-Access Extended Node	IE-3400H-16T	Cisco Catalyst IE3400 Rugged Series	17.6.6a	17.6.6a, 17.9.4a
	IE-3300-8P2S	Cisco Catalyst IE3300 Rugged Series	17.6.6a	17.6.6a, 17.9.4a

Solution Use Case Scenarios

The following use cases were validated on the Manufacturing Vertical profile using the topology shown in Figure 1.

- Service and network resiliency
 - High Availability can be achieved throughout the network with dual Cisco SD-Access borders and dual control plane nodes, a border StackWise Virtual link and border/edge stack, and dual-transit control planes in the transit network. If failover and recovery of the network failure occurs, there should be no or minimal interruption to the traffic flow.

- Administrators can configure Cisco DNA Center in the three-node High Availability mode. If services or node failure occur in the Cisco DNA Center cluster, the system should recover without user intervention.
 - The Cisco ISE distributed deployment model should be recovered with the PAN, PSN, and pxGrid service failover.
 - Administrators can implement a critical VLAN for fabric edges if Cisco ISE is unreachable.
 - Cisco DNA Center can back up the configuration and data on demand or by schedule. The backup file can be restored onto Cisco DNA Center to roll back to previous configurations.
- Implement multitiered security to protect sensitive OT network data
 - Administrators can segment users, guests, and Internet of Things (IoT) and OT devices into their logical network to limit the movement of network threats.
 - Administrators can enable Closed Authentication Onboarding (the dot1x authentication) or MAC Authentication Bypass (MAB) for wired and wireless endpoints to prevent unauthorized access.
 - Administrators can create groups, place users and endpoints into those groups by their identities, and define group-based policies that control the traffic between groups.
 - Administrators can implement a high scale of access control policies for factory floors and Security Group ACLs (SGACL) that are properly installed on edge devices when clients are onboarding.
 - Administrators can monitor Cisco DNA Center activities with the audit logs that record system events (which includes what occurred, when and where it occurred, and which users initiated the event).
 - Administrators can create granular role-based users with different privileges to access Cisco DNA Center.
- Simplified management
 - Cisco DNA Center provides the central management of device inventory and allows user to view device information, including the IP address, provision status, software releases, and inventory insights.
 - In Cisco DNA Center, administrators can use the Software Image Management (SWIM) function to upgrade the Golden image on switches, routers, extended nodes, and wireless controllers.
 - In Cisco DNA Center, the Fabric Border and Control Plane RMA workflow makes device replacement seamless.
 - The Site Border Layer 3 Handoff VLAN consumption optimization provides administrators VLAN assignment flexibility in a scaled multisite environment.
 - LAN Automation with the overlapping pool option provides significant IP address optimization by allowing the underlay network to reuse the same address across different fabric sites.
- Network services
 - Administrators can implement the Layer 2-Only VN feature, which is intended to support Cisco SD-Access fabric endpoints. For security reasons, this has a strict entry point to the network (for example, through a firewall), which resides outside the fabric.
 - Administrator can enable redundancy with a recovery time of less than 50 ms for network failures with extended nodes and can configure a Resilient Ethernet Protocol (REP) ring for the fabric site.
 - Administrators can enable Layer 2 flooding to handle silent OT devices as well as broadcast, unknown unicast, and multicast (BUM) traffic within fabric sites.
- Monitor a network and its clients using Cisco DNA Assurance and Cisco AI Endpoint Analytics

- Administrators can use Cisco DNA Assurance to monitor network health and identify network issues. Cisco DNA Assurance can report issues triggered by various network failures, including link down, AP down, and switch stack member down.
- Administrators can use Cisco DNA Assurance to monitor wired and wireless client health and identify client onboarding issues.
- Administrators can enable Telemetry Data Logger (TDL)-based assurance for better scale and performance in reporting client health.
- Administrators can monitor a large number of concurrent endpoints, with Assurance charts showing information for 100,000 concurrent endpoints and 250,000 transient endpoints.
- Administrators can use Cisco AI Endpoint Analytics to identify and profile endpoints and IoT devices.
- Administrators can monitor wireless network performance with wireless sensors.
- Administrators can enable Application telemetry and use Cisco DNA Assurance to monitor application health for latency, jitter, and packets drops.
- Administrators can visualize communications between existing endpoints to assess the need and impact of introducing new access controls.
- Administrator can use group-based policy analytics capabilities to create and implement microsegmentation policies.

Topology

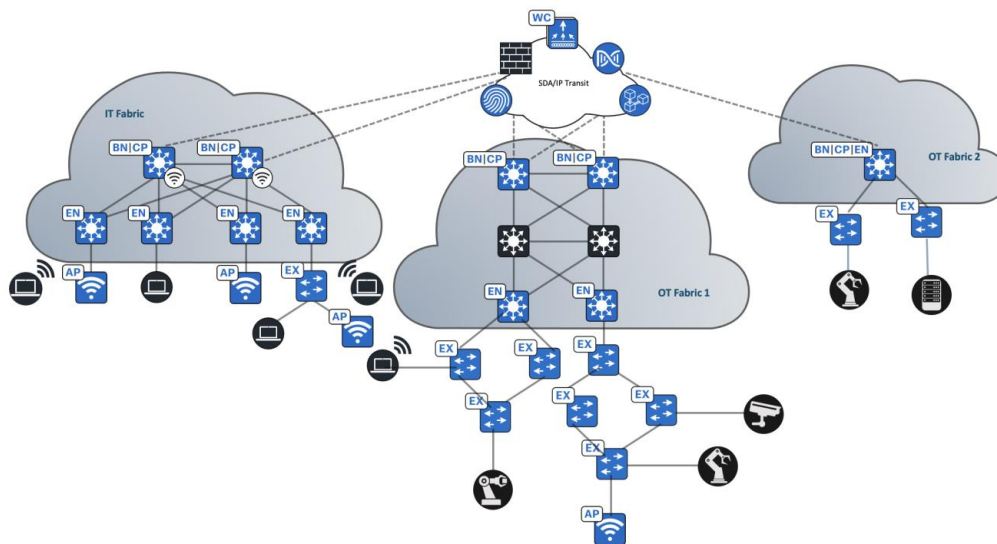
The test topology for the Manufacturing Vertical profile includes a three-node Cisco DNA Center cluster to manage one IT network site, one medium-scale OT site, and one small OT network. The Cisco SD-Access transit is deployed to connect these networks. The following figure illustrates the logical topology of the Manufacturing Vertical solution test bed.

The test bed setup has the following components:

- IT Fabric has dual co-located border and control plane nodes, a wireless controller, fabric edges, and extended nodes.
- OT Fabric 1 has dual borders, dual-dedicated control plane nodes, dual wireless controllers, 10 fabric edges, and 20 extended nodes.
- OT Fabric 2 is a small site that has Fabric-in-a-box (FiaB) on hardware stacking with an embedded wireless controller and extended nodes.
- The Cisco SD-Access transit is implemented with dual-transit control plane nodes. IT network borders are configured to provide internet access to other OT sites via the Cisco SD-Access transit.

The following figure illustrates the logical topology of the solution test bed.

Figure 1: Solution Test Logical Topology



Scale

Solution test verified the scale numbers listed in the following table. For the hardware capacity, see the [Cisco DNA Center Data Sheet](#).

Category	Value
Device inventory	5000
Devices per fabric site	1000
Buildings and floors	2000
VNs per fabric site	64
IP pools per fabric site	500
Wireless controllers per fabric site	2
Fabric sites	500
APs in inventory	12,000
Endpoints	100,000 (80,000 wired, 20,000 wireless)
SSIDs	10
SGTs	4000
IE devices in a REP ring	18

Solution Key Notes

This section describes technical notes that are useful for deploying the solution.

Uncarpeted Space Extension

In the manufacturing world, devices in OT networks are likely to be placed in uncarpeted or rugged locations. In this case, you can use Cisco Industrial Ethernet (IE) switches as extended nodes (ENs). Cisco SD-Access ENs enable mobility by offering a Layer 2 port extension and increasing the port density to existing fabric edge nodes. Meanwhile, these ENs also provide segmentation and group-based policies to the endpoints connected to these switches. Note that Cisco DNA Center provides a zero-touch plug-and-play automated workflow to discover, provision, and add ENs to the fabric.

Cisco DNA Center has two different support options for ENs: classic ENs and policy extended nodes (PENs). In addition to the operation and management provided by classic ENs, PENs directly support SGT policy enforcement with SGACLs. This local support of SGACLs provides direct east-west traffic enforcement on PENs.

ENs are connected to a single fabric edge switch through an 802.1Q trunk port. This port can be deployed as an EtherChannel if two or more links are aggregated at the upstream fabric edge. Cisco DNA Center automates the trunk and the EtherChannel creation. After the ENs are onboarded through the workflow, the endpoints (including fabric-mode APs and other Power over Ethernet (PoE) devices) can connect directly to the EN, expanding the wired and wireless services to uncarpeted spaces as needed. For Cisco SD-Access EN deployment details, see the [Cisco Extended Enterprise Non-Fabric and SD-Access Fabric Design Guide](#).

REP Ring

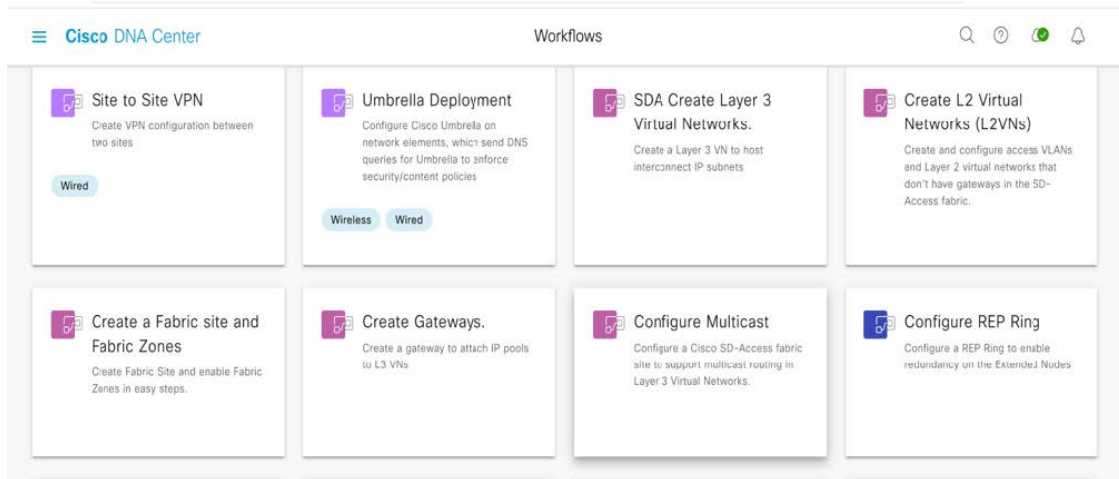
OT networks tend to have network devices far more geographically distributed compared to IT networks. There can be several miles between neighboring switches. Due to these geographically dispersed installations, it can be impractical or too expensive to use a star topology because they're not able to physically connect via cable every access switch back to the distribution layer. While OT networks often contain networks with star topologies, we also see other topologies, such as the linear daisy chain and rings topologies.

Generally, for manufacturing, zero-loss and sync are required for motion applications, and these are less stringent applications. For example, the input and output operations on motion applications can withstand up to 100 ms of Layer 2 convergence times. In most manufacturing industries, this level of resilience and precision is not mandated. At Cisco, OT networks are commonly deployed as REP rings with variants of the spanning Tree Protocol (STP) still providing resiliency.

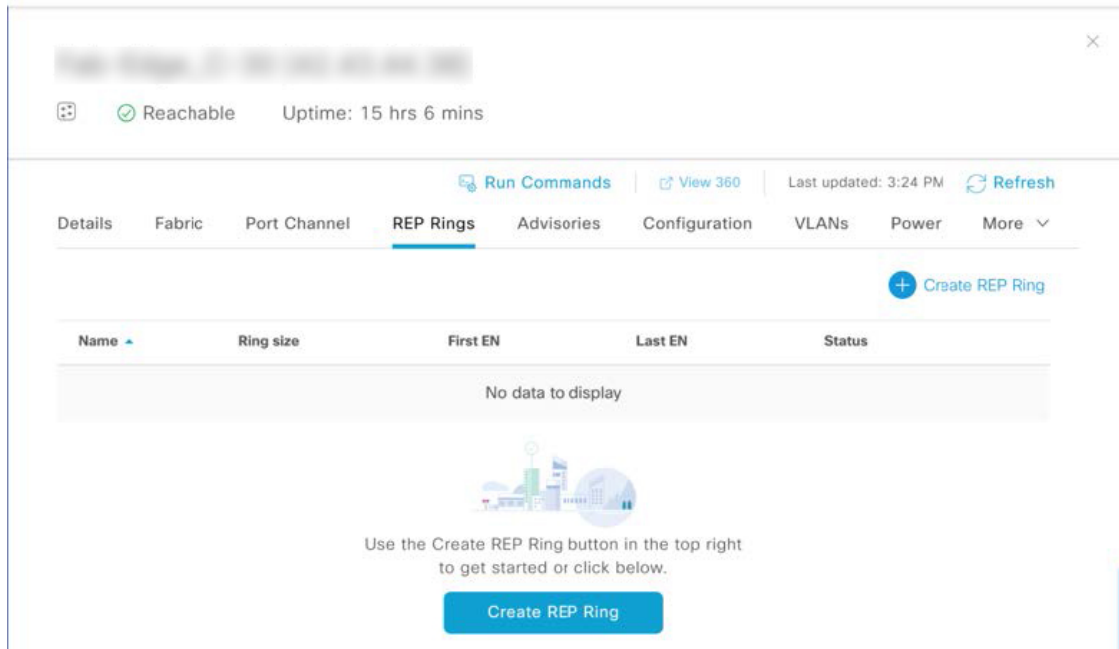
Cisco DNA Center provides the workflow to create and deploy a REP ring on the Cisco SD-Access fabric site, where IE switches are connected to fabric edges and onboarded as two daisy chain of ENs. With Cisco DNA Center, you can complete this REP ring automation by following this procedure.

Procedure

Step 1 From the top-left corner, click the menu icon and choose **Workflows > Configure REP Ring**.



Alternatively, you can navigate to the Fabric Site topology view and choose the fabric edge node or the FiaB node where you want to create the REP ring. Then in the **REP Rings** tab, click **Create REP Ring**.



Step 2 On the **Select a fabric site** page, from the **Select Fabric Site** drop-down list, choose a fabric site.

Select a fabric site

Select a fabric site that contains fabric edges and extended nodes to proceed.

 This action might interrupt network traffic for a brief period. ✕

Select Fabric Site* ^

- BGL-17
- BGL-18

Step 3 On the **Select a fabric edge node** page, choose a fabric edge node.

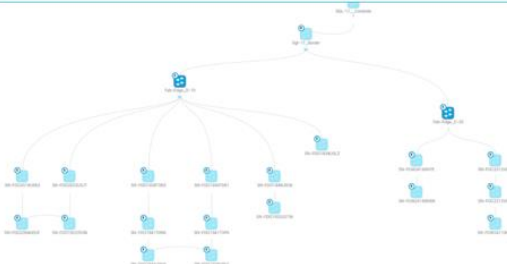
Cisco DNA Center Configure REP Ring

Select a fabric edge node

EQ, Find Hierarchy EQ, Find by device IP, type, role, family & MAC

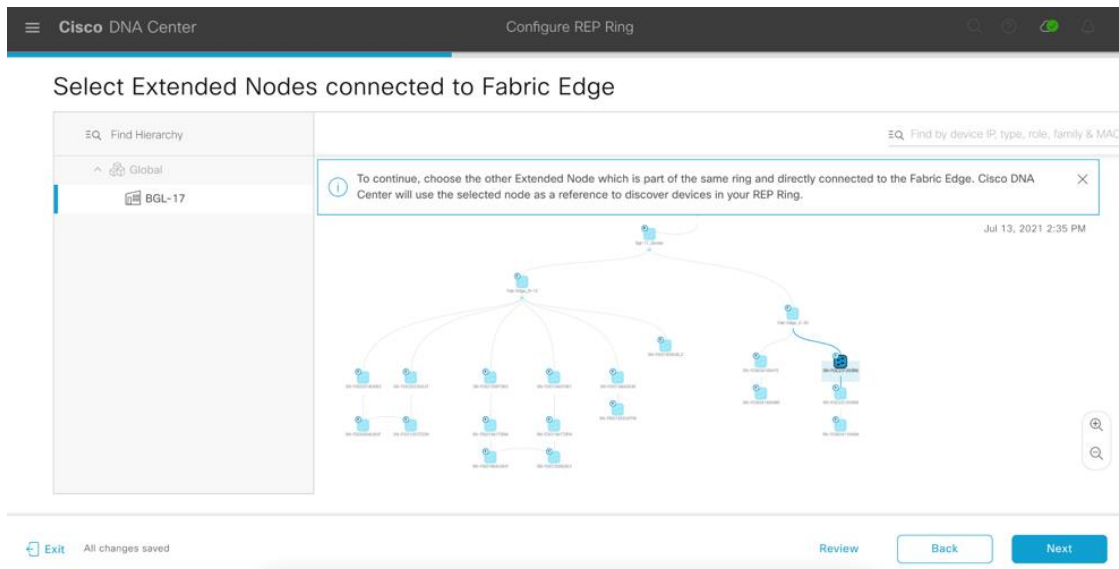
1 Select a fabric edge node to proceed. Cisco DNA Center will use the selected node as a reference to discover devices in your REP Ring. ✕

Jul 13, 2021 3:48 PM

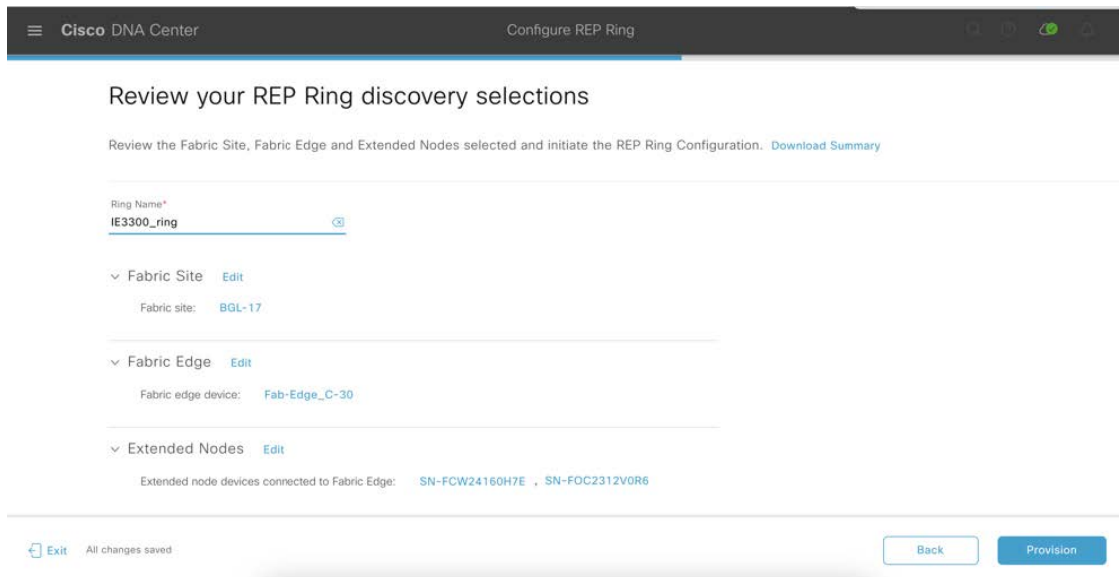


Exit All changes saved Review Back Next

Step 4 On the **Select Extended Nodes connected to Fabric Edge** page, choose the ENs to connect to the fabric edge nodes. You can choose two ENs to connect to the fabric edge node.



Step 5 On the **Review your REP Ring discovery selections** page, review and edit (if needed) your fabric site, edge node, and EN configurations.



Step 6 When you're ready, click **Provision**.

Step 7 On the **REP Ring Summary** page, click **Next**.

This page displays the details of the REP ring that is created along with the discovered devices.

Cisco DNA Center Configure REP Ring

REP Ring Summary

Summary of the discovered REP Ring Nodes and REP Ring Configuration status

IE3300_ring

RING DETAILS

Fabric Site	BGL-17	Discovery Status	Success
Fabric Edge	Fab-Edge_C-30	Number of devices discovered	6
Extended node devices connected to Fabric Edge	SN-FCW24160H7E, SN-FOC2312V0R6		

DISCOVERED DEVICES

Ring order	Devices	First port	Second port
1	Fab-Edge_C-30	Port-channel2	Port-channel1
2	SN-FCW24160H7E	Port-channel1	Port-channel2
3	SN-FCW24160H6N	Port-channel1	Port-channel2

[Exit](#) All changes saved

When the REP ring is created, a success message is displayed.

Cisco DNA Center Configure REP Ring

REP Ring Configuration is Successful


IE3300_ring is configured at fabric site BGL-17 ✔

What's Next?

[Configure another ring](#)

[Fabric Site Home](#)

[Workflows Home](#)



Step 8 (Optional) To verify the creation of the REP ring, go to the fabric site window and click the fabric edge node. On the slide-in pane, under the **REP Ring** tab, you can see the list of all the existing REP rings on the edge node.

Ring order	Devices	First port	Second port
1	Fab-Edge_C-30	Port-channel2	Port-channel1
2	SN-FCW24160H7E	Port-channel1	Port-channel2
3	SN-FCW24160H6N	Port-channel1	Port-channel2
4	SN-FCW24110H0A	Port-channel2	Port-channel1
5	SN-FOC2312V0R8	Port-channel2	Port-channel1
6	SN-FOC2312V0R6	Port-channel2	Port-channel1

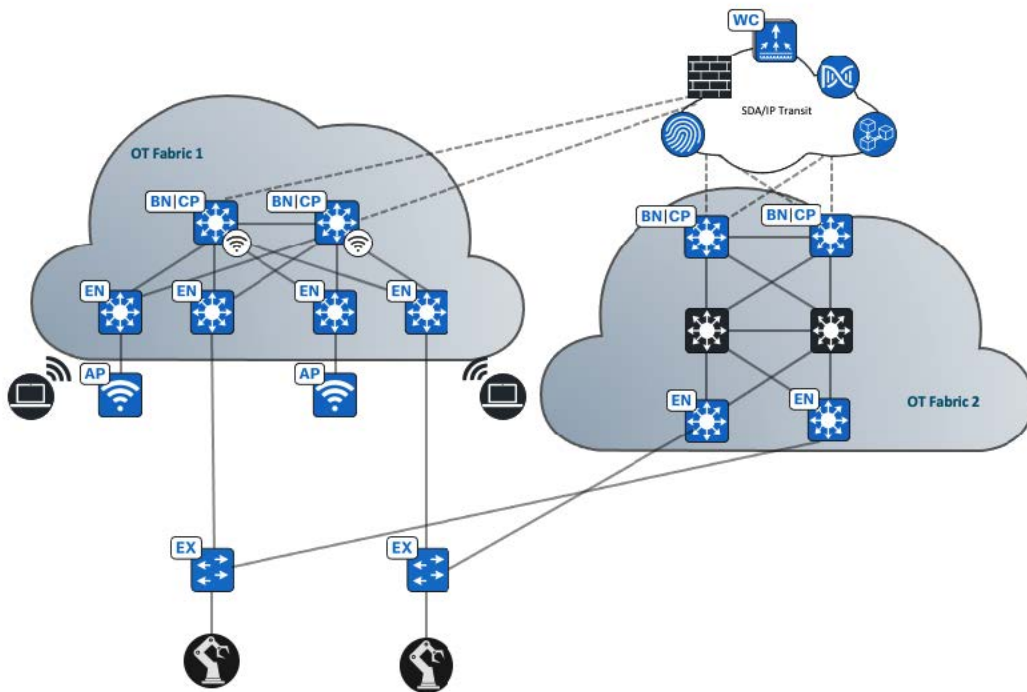
Zero-Loss Redundancy: Dual Fabric with PRP

As OT networks have become critical to an organization's functionality (as in many cases, an OT network is the core of a company's standing), it's critical to provide resiliency options for these networks. These schemes for redundancy can take between a few milliseconds to a few seconds for the network to recover and for traffic to flow again. If the quality management system, like SAP, for a manufacturing floor is down—regardless of its Tier-1, Tier-2, or Tier-3 manufacturing—then the manufacturing line is down. Thus, if the network is impacted, it's likely the plant will be down, costing millions of dollars per second.

To recover from network failures, redundancy can be provided by network elements that are connected in mesh or ring topologies where a network failure causes a reconfiguration in the network to reopen traffic flow. Typically, this is accomplished by opening a blocked port. (Note that these topologies use protocols like RSTP, REP, or MRP.) However, zero packet loss is required for the manufacturing industry.

The Parallel Redundancy Protocol (PRP) is defined in the international standard, International Electrotechnical Commission (IEC) 62439-3. PRP is designed to provide hitless redundancy (that is, zero recovery time after failures) in Ethernet networks. PRP uses a different scheme, where the end nodes implement redundancy (instead of network elements) by connecting two network interfaces to two independent, disjointed parallel networks (LAN-A and LAN-B). Each of these Dually Attached Nodes (DANs) have redundant paths to all other DANs in the network.

The solution is to leverage PRP in the Cisco SD-Access network to achieve zero packet loss by creating a redundant Cisco SD-Access fabric and connecting the ENs to both the main and redundant sites. The following topology contains two Cisco SD-Access fabric sites.



Cisco DNA Center implements this solution by using the EN onboarding and CLI templates to push the PRP-specific configuration onto the ENs. You can implement this configuration with the following steps.

Procedure

- Step 1** Connect the extended node via the regular Port Aggregation Protocol (PAgP) port channel to Fabric 1 where it's onboarded by the LAN Automation process as a PEN.

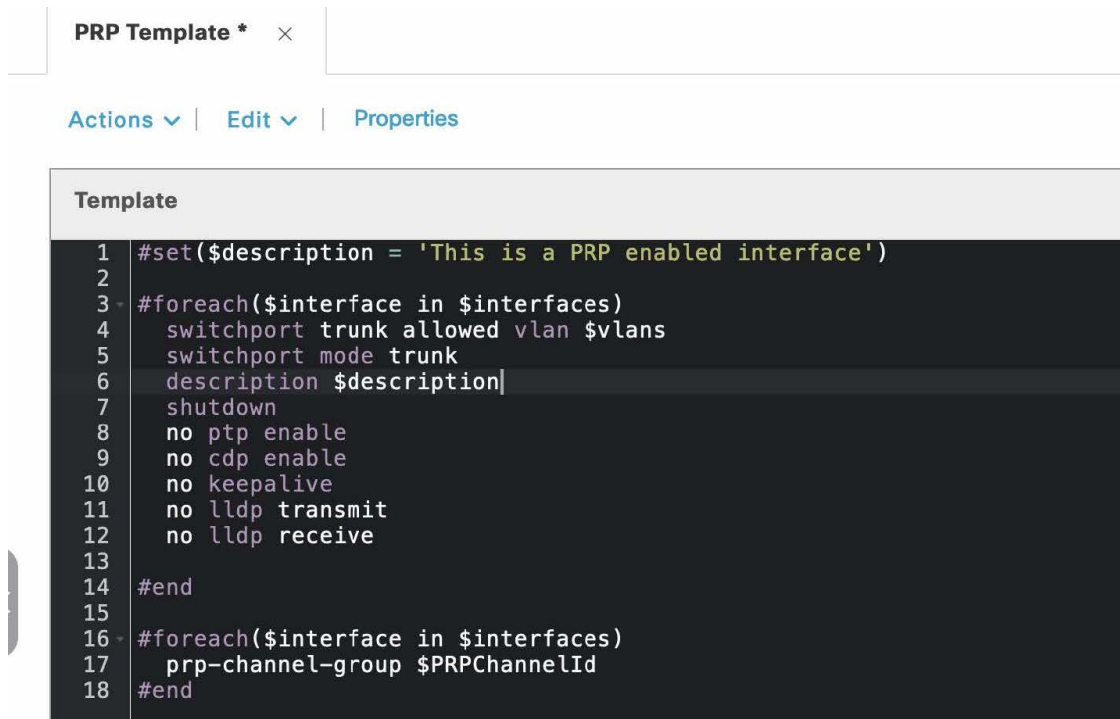
```
interface Port-channel1
description Extended2
switchport mode trunk
!
interface GigabitEthernet1/0/11
switchport mode trunk
cts manual
policy static sgt 8000 trusted
channel-group 1 mode desirable
```

- Step 2** When the IE switch onboards successfully, the downlink port on the Fabric 2 edge node is configured as PAgP trunk port from the Cisco DNA Center GUI.

```
interface Port-channel1
switchport mode trunk
device-tracking attach-policy IPDT_POLICY
!
interface GigabitEthernet1/0/13
switchport mode trunk
channel-group 1 mode desirable
```

Step 3 When the edges from both fabric sites are connected to the IE switch and provisioned, the PRP configuration can be applied to the uplink ports on the IE switch using a Cisco DNA Center provisioning template.

See the following sample of a Velocity template for the PRP configuration.



The screenshot shows a web interface for a Velocity template. At the top, there is a tab labeled "PRP Template *". Below the tab are three menu items: "Actions", "Edit", and "Properties". The main content area is titled "Template" and contains a code editor with the following configuration:

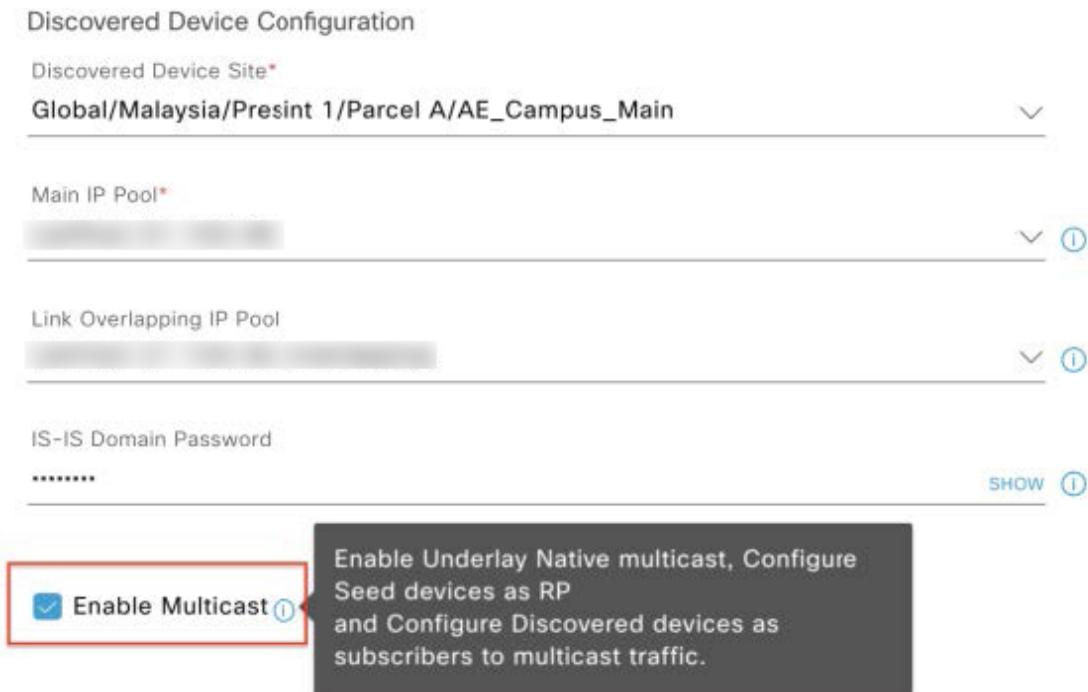
```
1 #set($description = 'This is a PRP enabled interface')
2
3 #foreach($interface in $interfaces)
4     switchport trunk allowed vlan $vlans
5     switchport mode trunk
6     description $description|
7     shutdown
8     no ptp enable
9     no cdp enable
10    no keepalive
11    no lldp transmit
12    no lldp receive
13
14 #end
15
16 #foreach($interface in $interfaces)
17     prp-channel-group $PRPChannelId
18 #end
```

Layer 2-Only VN (Gateway Outside of the Fabric)

OT networks have naturally a high number of Layer 2 networks in their factory floors for various use cases and business purposes. To achieve a high level of security, the Layer 2-level traffic needs to be inspected by a firewall outside the fabric network. This requirement means that the first hop for all the traffic needs to be outside the fabric. This implementation is achieved by using a combination of Layer 2-only VN and underlay multicast features.

For the underlay multicast feature, enabling multicast in the physical underlay network is essential to the future fabric multicast service deployment. We highly recommended enabling underlay multicast during the LAN Automation workflow. During the LAN Automation workflow, Cisco DNA Center provides an option to also automate the underlay PIM-ASM configuration for new devices. This workflow will create a Loopback60000 on the seed device and use this address as default rendezvous point for the underlay multicast network. Figure 2 shows how to enable underlay multicast with the LAN Automation workflow.

Figure 2: Enable Underlay Multicast with the LAN Automation Workflow

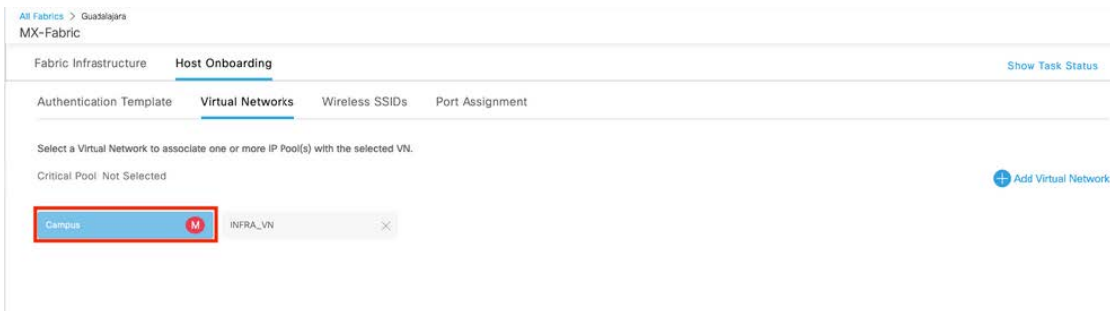


The following procedure shows you how to enable multicast in the physical Layer 2-only service on Cisco DNA Center with the Layer 2-only VN workflow and deployment.

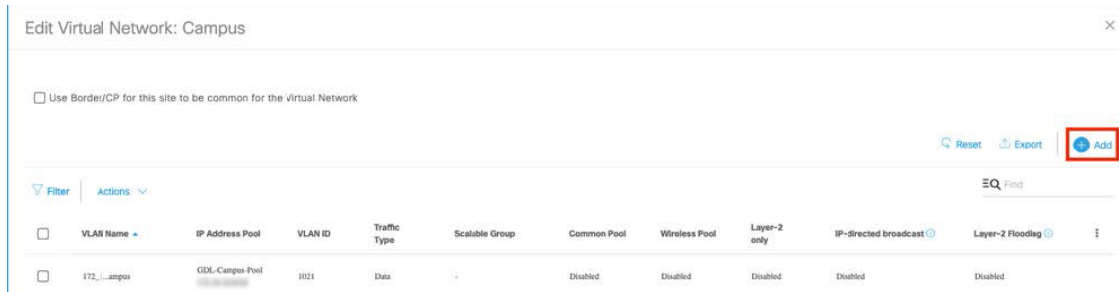
Procedure

Step 1 Choose a fabric site and then on the fabric site's window, choose **Hosting Onboarding > Virtual Networks**.

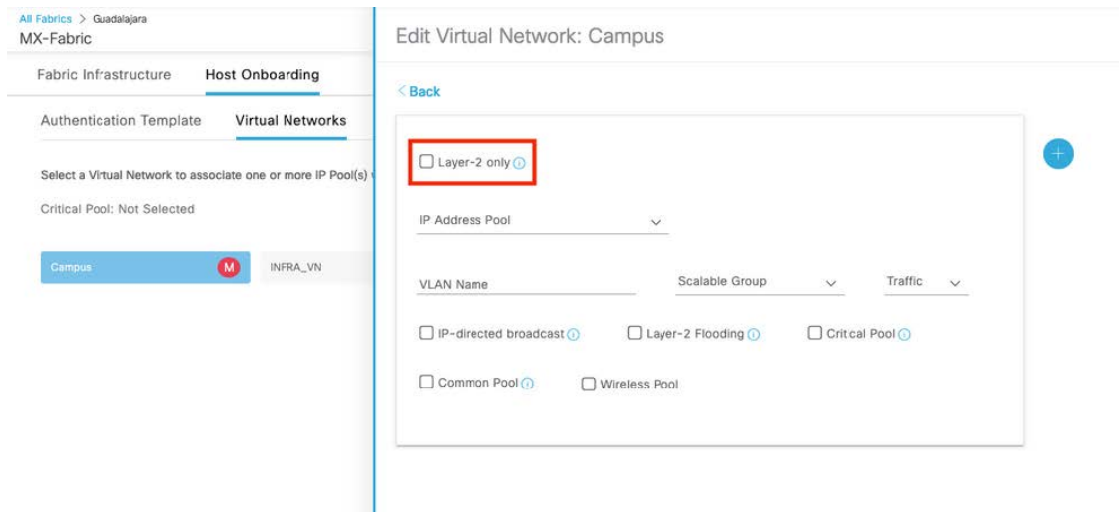
Step 2 Choose the VN where you want to add the Layer 2-only service.



Step 3 On the **Edit Virtual Network: Campus** slide-in pane, click **Add** as if you were adding a new IP pool.

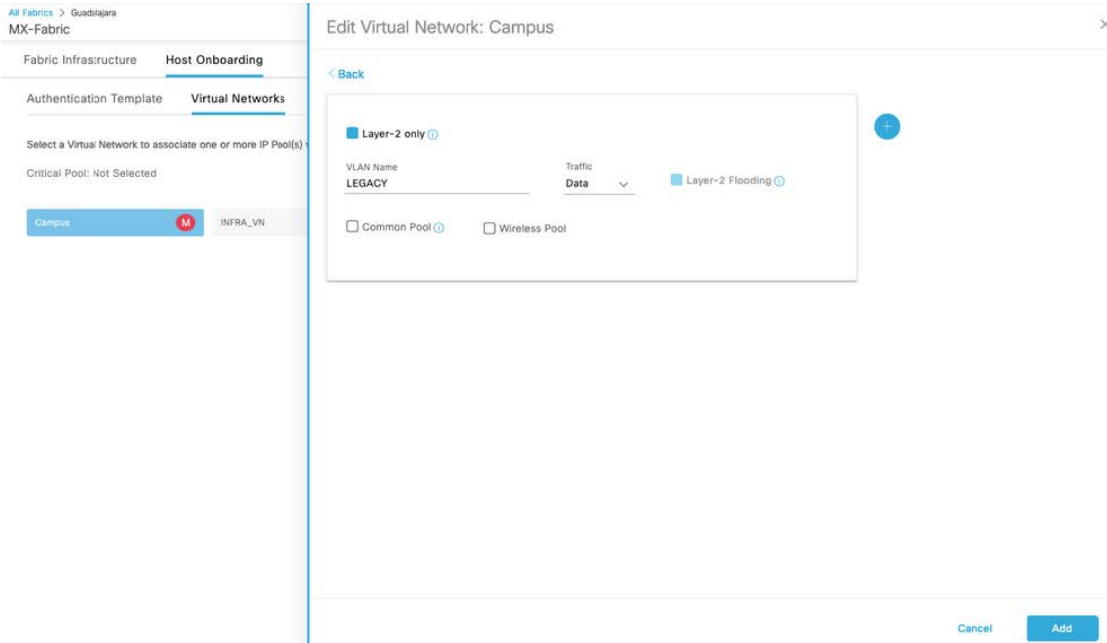


On the **Edit Virtual Network: Campus** slide-in pane, the **Layer-2 only** check box displays. This is where you can specify that this segment is a Layer 2-only service.

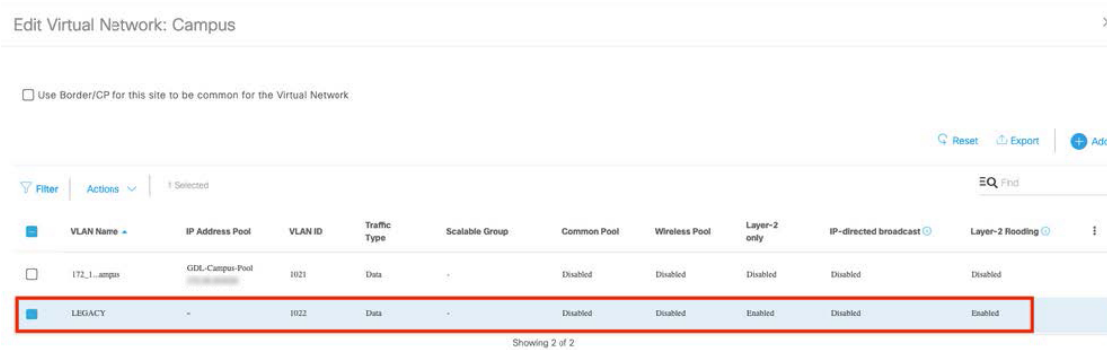


Step 4 Check the **Layer-2 only** check box, complete the required information, and then click **Add**.

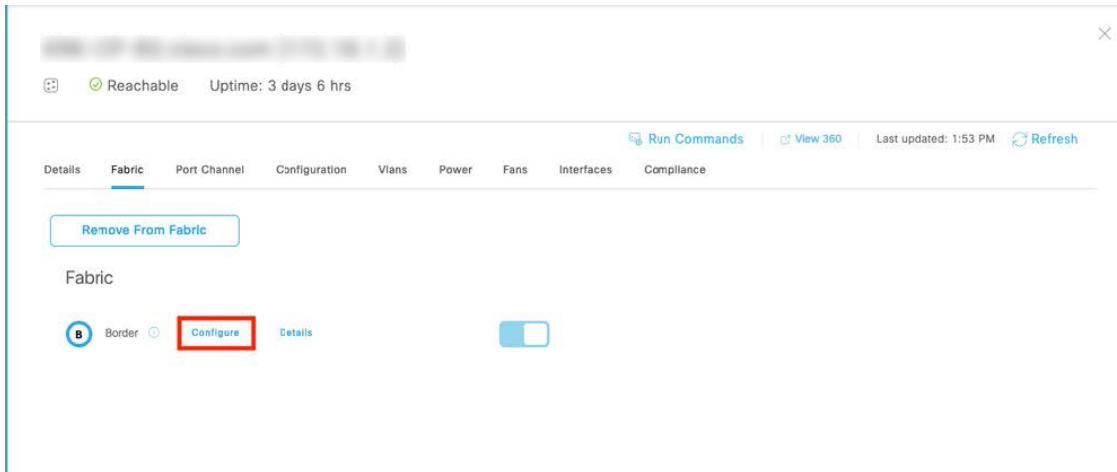
Note Cisco DNA Center uses the entered name to identify and map the external VLAN to the fabric VLAN.



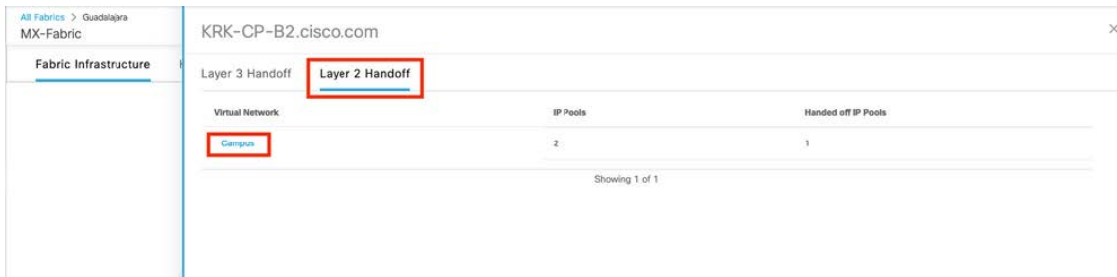
The **Edit Virtual Network: Campus** slide-in pane now displays the Layer 2-only segment, listed as if it's another IP pool.



Step 5 Return to Fabric Infrastructure and click on the device that you want to add as a Layer 2 border. Either select the **Border** radio button or select the **Configure** radio button if you're modifying an existing border.

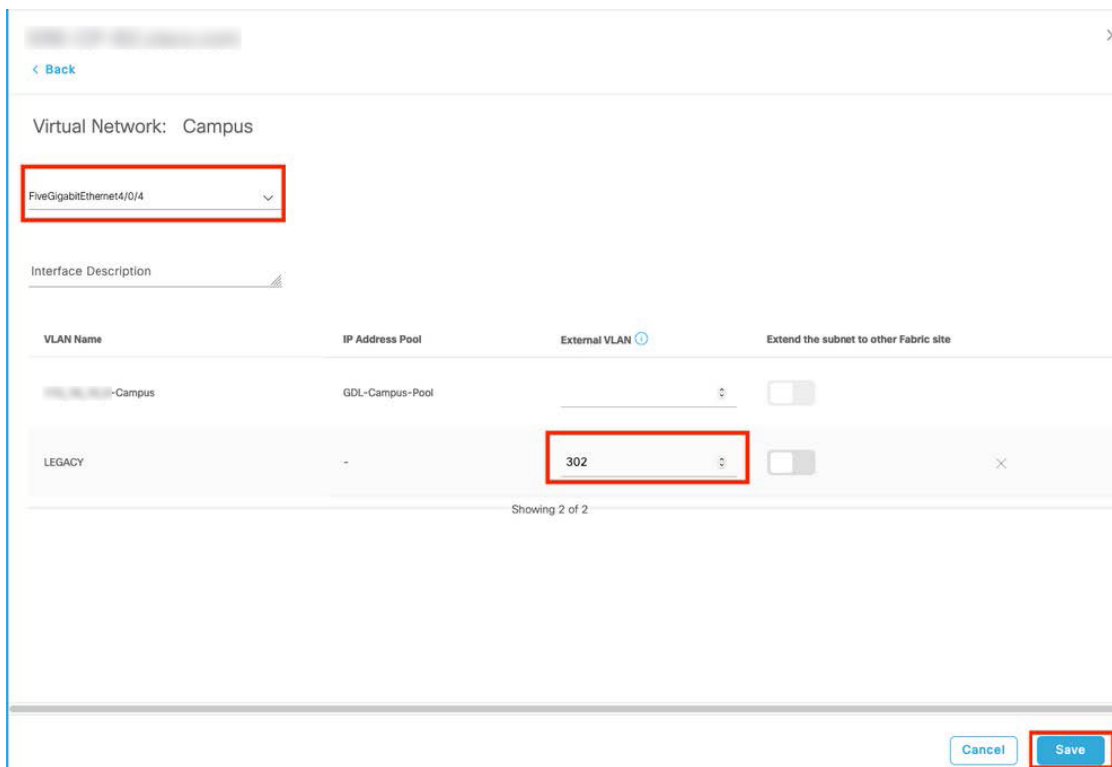


Step 6 On the slide-in pane, click the **Layer 2 Handoff** tab to view a list of available VNs and then click the desired VN.



Step 7 Choose the interface that connects to the Fusion device, specify the External VLAN ID, and then click **Save**.

Note The External VLAN ID is the VLAN that the outside gateway belongs to.



When Cisco DNA Center completes the fabric devices configurations, the feature is ready for testing.

Cisco AI Endpoint Analytics

In the OT network, you need to manage a variety of devices from contractors and vendors. Along with scale, comes the issue of security. Modern security threats look for vulnerable points of entry to exploit an Enterprise network's valuable information. Identifying and tracking all the devices in a network is time-consuming and tedious. The Cisco AI Endpoint Analytics feature addresses this issue by identifying devices by type, manufacturer, model, OS type, communication protocols, and ports through passive network telemetry monitoring and deep packet inspection. This feature allows an administrator to create profiling rules to classify devices based on those attributes. Coupled with machine learning, Cisco DNA Center can detect spoofed endpoints and help administrators determine the appropriate action.

Cisco AI Endpoint Analytics is an additional application that runs with Cisco DNA Center. You can download and install the application from the catalog server. Then, you can enable it in Cisco DNA Center's system settings. Cisco DNA Center needs to connect to the cloud to download the latest endpoint analytics model. After you successfully install Cisco AI Endpoint Analytics, click the menu icon and choose **Policy** to access it.

Cisco AI Endpoint Analytics uses multiple methods to detect malicious endpoints. It uses Change in Profile labels, Network Address Translation (NAT) mode detection, a concurrent MAC address, posture, an authentication method, and machine learning features to identify and flag spurious endpoints. An overall trust score is generated for every endpoint. The trust score is a weighted average of multiple risk scores. A lower trust score indicates a higher risk for an endpoint.

Furthermore, Cisco DNA Center shares the endpoint classification attributes with Cisco ISE. When new devices onboard through identity-based authentication, they can be automatically identified by the manufacturer and type and then are added to the appropriate group. Defining and enforcing security policies is easier when these policies are applied to groups rather than to individual endpoints.

Group-based policy can easily be updated to adapt to new circumstances, such as security breaches by endpoints, and applied globally to the entire network.

The following figure shows details, specifically highlighting the IOT Asset attributes, for an endpoint as displayed in Cisco AI Endpoint Analytics.

The screenshot displays the Cisco AI Endpoint Analytics interface. At the top, there is a search bar with a close button (X). Below it, the 'Hostname' field is empty. A notification box indicates 'Two (2) unassigned profiles. Expand to show.' with a close button (X). The main content area has three tabs: 'Details', 'Trust Score', and 'Attributes', with 'Attributes' being the active tab. Under 'Attributes', there are expandable sections for 'RADIUS' and 'SNMP'. The 'IOTAsset' section is expanded, showing a list of attributes and their values:

assetDeviceType	IO Module
assetHwRevision	-
assetId	[REDACTED]
assetIpAddress	[REDACTED]
assetMacAddress	[REDACTED]
assetName	[REDACTED]
assetProductId	-
assetProtocol	ARP,ARP, CIP-IO, EthernetIP
assetSerialNumber	-
assetSwRevision	-
assetVendor	Rockwell Automation

References

- [Cisco SD-Access Solution Design Guide \(Cisco Validated Design\)](#)
- [Cisco Software-Defined Access for Distributed Campus Prescriptive Deployment Guide](#)
- [Cisco Software-Defined Access Compatibility Matrix](#)

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2023 Cisco Systems, Inc. All rights reserved.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.