Cisco DNA Center Fast Start Use Case: Software-Defined Access
Contents

Overview of Cisco DNA Center................................................................. 4
What is a fast start use case?................................................................. 4
Introduction......................................................................................... 4

Prerequisites ..................................................................................... 5
Cisco DNA Center installed and set up.................................................. 5
Device discovery, inventory, and topology............................................ 7
Cisco DNA Center-to-ISE integration.................................................... 7
Manual underlay setup........................................................................ 7
ISE configuration............................................................................... 8

Use Case 1. SD-Access workflow: Build network parameters .............. 8
Cisco DNA Center design: Build a site hierarchy................................. 8
Cisco DNA Center network settings...................................................... 9
Device credentials............................................................................. 10
IP pools and reservations.................................................................... 11
  Define a global IP pool for the network.......................................... 11
  Create reservations for campus, guest, multicast, and border handoff 11
Configure wireless SSIDs..................................................................... 14
  Build a WPA2 enterprise SSID for the campus............................... 14
  Build the guest wireless SSID (optional)........................................ 16

Use Case 2. SD-Access workflow: Policy............................................ 17
Define a scalable group tag for user groups......................................... 18
Create the VN and choose scalable groups.......................................... 20
  Campus virtual network.................................................................... 20
  Guest virtual network (optional)...................................................... 21
Microsegmentation within a VN and policy between scalable groups... 21
  Create and apply a “deny all” rule between scalable groups........... 22
  Create a custom contract (optional)................................................. 24
  Create a policy to block guest-to-guest access (optional).............. 26

Use Case 3. SD-Access workflow: Fabric provisioning......................... 27
Provision devices from Cisco DNA Center........................................... 27
  Provision wired switches................................................................... 27
  Provision wireless LAN controllers................................................. 30
  Verify TACACS operation................................................................. 31
Create the SJC fabric domain and a transit site.................................. 32
Add devices to the fabric and define their roles................................... 35
Configure the fusion router manually.................................................. 40
Onboard hosts.................................................................................... 41
  Define the default authentication policy for fabric.......................... 41
  Bind IP pools to the Campus VN.................................................... 41
  Bind the guest IP pool to the Guest VN (optional)............................ 42
  Bind the access point IP pool to the INFRA_VN.............................. 42
  Assign a static port for access points............................................. 43
Onboard wireless clients for Campus and Guest.................................. 44
  Bind IP pools to the Campus SSID.................................................. 44
  Bind IP pools to the Guest SSID..................................................... 45
Provision access points....................................................................... 45
Multicast............................................................................................ 46
Layer 2 flooding................................................................................ 48
## Use case validation

- Client group tag classification
- Test intra-VN connectivity
- Verify guest wireless access (optional)

## Appendix

- Underlay template
- Configure dynamic authentication with ISE
- Create user identity groups for the Campus scenario
- Create an identity for each Campus user
- Create SD-Access device credentials
- Define an 802.1X authorization profile and policies for Campus users
- ISE policies for wireless guest access
- Fusion configuration
  - Create Layer 3 connectivity between the border and the fusion router
  - Extend virtual networks from the border to the fusion router
  - Use VRF leaking to share routes on the fusion router and distribute them to the border
  - Share virtual networks between border nodes for traffic resiliency
Overview of Cisco DNA Center

Cisco DNA Center is the foundational controller and analytics platform at the heart of Cisco’s intent-based network. It offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center UI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience.

What is a fast start use case?

A fast start use case demonstrates real value for customers who move to Cisco DNA Center. Cisco validates the use case, including step-by-step guidance for deployment. Cisco partners and SEs can deploy the use case in the field with back-end support from the business teams. The use case requires a specific combination of equipment, OS version, and configuration.

Introduction

This guide demonstrates the value of the Cisco® Software-Defined Access (SD-Access) solution using a specific combination of equipment, OS version, and configuration. To obtain the best outcome, follow this guide exactly. The procedures and configurations described have been tested and validated. If you must deviate from this guide, we recommend that you stage the setup out of band and conduct extensive testing before you deploy Cisco DNA Center and SD-Access in production.

To deploy the SD-Access solution in your network, a Cisco DNA Advantage license is required.

Table 1. Prerequisites, workflows, and outcomes

<table>
<thead>
<tr>
<th>Prerequisites</th>
<th>Workflows</th>
<th>Outcomes</th>
</tr>
</thead>
<tbody>
<tr>
<td>● Install and set up single-node Cisco DNA Center</td>
<td>Design</td>
<td>• Easily enable network connectivity</td>
</tr>
<tr>
<td>● Complete network discovery</td>
<td>● Set up network parameters: shared services, IP pools, wireless</td>
<td>• Understand and manage segmentation</td>
</tr>
<tr>
<td>● Complete inventory collection</td>
<td>Policy</td>
<td>• Create and deploy microsegmentation</td>
</tr>
<tr>
<td>● Configure the network topology</td>
<td>● Create the virtual network</td>
<td>● Create the group-based policy</td>
</tr>
<tr>
<td>● Install Cisco Identity Services Engine (ISE)</td>
<td>Provision fabric</td>
<td>● Create a single fabric site</td>
</tr>
<tr>
<td>● Add ISE to Cisco DNA Center</td>
<td>● Onboard endpoints to the fabric</td>
<td></td>
</tr>
<tr>
<td>● Create the manual underlay</td>
<td></td>
<td></td>
</tr>
<tr>
<td>● Configure the border and fusion router</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 2. Recommended platforms and supported OS versions for Cisco DNA Center 1.2.6

<table>
<thead>
<tr>
<th>Device type</th>
<th>Platform</th>
<th>OS version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco DNA Center</td>
<td>DN1-HW-APL</td>
<td>1.2.6</td>
</tr>
<tr>
<td>Fabric edge</td>
<td>Cisco Catalyst® 9300 or 9400 Series Switches</td>
<td>Cisco IOS® XE 16.9.2</td>
</tr>
<tr>
<td>Fusion router</td>
<td>Cisco 4000 Series Integrated Services Routers (ISRs)</td>
<td>Cisco IOS XE 16.9.2</td>
</tr>
<tr>
<td>Fabric border/control plane</td>
<td>Cisco Catalyst 9300 or 9500 Series Switches, 4000 Series ISR</td>
<td>Cisco IOS XE 16.9.2</td>
</tr>
<tr>
<td>Wireless LAN controller</td>
<td>Cisco 3504 or 5520 Wireless Controllers</td>
<td>AireOS 8.5 MR4 (8.5.140.0)</td>
</tr>
<tr>
<td>Access point</td>
<td>802.11ac Wave 2 (Cisco Aironet® 1800, 2800 or 3800 Series)</td>
<td>Table 3. Recommended platforms and supported OS versions for Cisco DNA Center 1.2.8</td>
</tr>
<tr>
<td>Identity Services Engine</td>
<td>VM or appliance</td>
<td>2.3 patch 5 or 2.4 patch 5</td>
</tr>
</tbody>
</table>
Table 3. Tested scale guidelines

<table>
<thead>
<tr>
<th>Switches or routers</th>
<th>Endpoints</th>
<th>Fabric or sites</th>
<th>Fabric edge nodes</th>
<th>Virtual networks</th>
<th>IP pools</th>
<th>Scalable groups</th>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>200 Access points: 500 Hosts: 5000</td>
<td>Fabric domain: 1 Fabric site: 1</td>
<td>200</td>
<td>5</td>
<td>20</td>
<td>20</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

Table 4. Recommended platforms and supported OS versions for Cisco DNA Center 1.2.8

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Platform</th>
<th>OS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Center</td>
<td>DN1-HW-APL</td>
<td>1.2.8</td>
</tr>
<tr>
<td>Fabric Edge</td>
<td>Catalyst 9300, Catalyst 9400</td>
<td>IOS-XE 16.9.2s</td>
</tr>
<tr>
<td>Fusion Router</td>
<td>ISR 4000</td>
<td>IOS-XE 16.9.2s</td>
</tr>
<tr>
<td>Fabric Border/Control Plane</td>
<td>Catalyst 9300, Catalyst 9500, ISR 4000</td>
<td>IOS-XE 16.9.2s</td>
</tr>
<tr>
<td>Wireless LAN Controller</td>
<td>WLC3504, WLC5520</td>
<td>AireOS 8.5MR4</td>
</tr>
<tr>
<td>Access Point</td>
<td>11ac wave2 (1800, 2800, 3800)</td>
<td>AireOS 8.5MR4</td>
</tr>
<tr>
<td>Identity Services Engine</td>
<td>VM/appliance</td>
<td>2.4 Patch 5</td>
</tr>
</tbody>
</table>

Prerequisites

This document assumes that the tasks explained in the following sections have been performed.

Cisco DNA Center installed and set up

If you haven’t done so already, install Cisco DNA Center according to the [Cisco DNA Center Appliance Installation Guide](#).

After you install Cisco DNA Center, be sure to use the Cloud Update to get the latest version, Cisco DNA Center 1.2.6 or 1.2.8. A single-node Cisco DNA Center running version 1.2.6 or 1.2.8 must be installed.

In the Cisco DNA Center UI, go to Settings > About Cisco DNA Center > Show Packages to check the version running on the appliance.
### Hide Packages

<table>
<thead>
<tr>
<th>Package</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Policy</td>
<td>2.1.23.170130</td>
</tr>
<tr>
<td>Assurance - Base</td>
<td>1.2.6.63</td>
</tr>
<tr>
<td>Assurance - Sensor</td>
<td>1.2.6.76</td>
</tr>
<tr>
<td>Automation - Base</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Automation - Intelligent Capture</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Automation - Sensor</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Command Runner</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Device Onboarding</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Device Onboarding UI</td>
<td>2.1.23.60287</td>
</tr>
<tr>
<td>Cisco DNA Center Platform</td>
<td>1.0.4.14</td>
</tr>
<tr>
<td>Cisco DNA UI</td>
<td>1.2.0.55</td>
</tr>
<tr>
<td>Image Management</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>NCP - Base</td>
<td>2.1.23.60287</td>
</tr>
<tr>
<td>NCP - Services</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Network Controller Platform</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>Network Data Platform - Base Analytics</td>
<td>1.1.7.590</td>
</tr>
<tr>
<td>Network Data Platform - Core</td>
<td>1.1.7.765</td>
</tr>
<tr>
<td>Network Data Platform - Manager</td>
<td>1.1.7.645</td>
</tr>
<tr>
<td>Path Trace</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>SD Access</td>
<td>2.1.24.60052</td>
</tr>
<tr>
<td>System</td>
<td>1.1.0.659</td>
</tr>
</tbody>
</table>

### Release Notes

© 2018 Cisco Systems Inc. All Rights Reserved.

[OK]
Device discovery, inventory, and topology

Devices must be discovered from Cisco DNA Center. They appear as “reachable” and “managed.”

Cisco DNA Center-to-ISE integration

Verify that ISE 2.3 patch 5 or ISE 2.4 patch 5 is installed and integrated with Cisco DNA Center. After successful integration, default scalable groups are imported from ISE to Cisco DNA Center.

Manual underlay setup

This guide references the following topology and IP addressing scheme, which will be different in your network. Screen shots used throughout this guide are based on the following setup to guide you through the workflow and expected results. The appendix contains a recommended underlay template.
This guide uses the following IP addressing scheme for the fabric overlay provisioning.

<table>
<thead>
<tr>
<th>Fabric site: SJC Fabric</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scalable groups</strong></td>
</tr>
<tr>
<td>Guest</td>
</tr>
<tr>
<td>HR, ACCT, Employees</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

**Shared services**
- Cisco DNA Center Vlan65: 100.65.0.101/24
- ISE Vlan64: 100.64.0.100/24
- WLC Vlan127: 100.127.100.10/24
- DNS/DHCP Vlan128: 100.128.0.1/24

**ISE configuration**
Refer to the appendix for ISE configuration and authorization rules.

**Note:** The SD-Access use case requires that you complete the following sections in order. Do not deviate from the workflow.

**Use Case 1. SD-Access workflow: Build network parameters**
After completing this workflow, you will be able to easily enable network services across the site.

This workflow covers the following areas:
- Create a network hierarchy.
- Configure network settings to define shared services, device credentials, IP pools, and wireless Service Set Identifiers (SSIDs).

Cisco DNA Center provides a robust design application to allow customers of every size and scale to easily define their physical sites and common resources required for automation in device provisioning and fabric configuration.

**Cisco DNA Center design: Build a site hierarchy**
To allow Cisco DNA Center to group devices based on location, begin by laying out a hierarchy of areas, buildings, and floors. A site hierarchy lets you enable unique network settings and IP spaces for different groups of devices.

The behavior of Cisco DNA Center is to inherit settings from the global level into subsequent levels in the hierarchy. This enables consistency across large domains, while also giving administrators the flexibility to adapt and change for a local building or a floor.

**Note:** When creating a building in the Cisco DNA Center design hierarchy, it is critical that you use a real physical street address, such as the local Cisco office or the customer's current location. Cisco DNA Center uses the street address to select the country codes for the wireless implementation.

The WLC pulls its country code from Cisco DNA Center based on the street address of the building it is provisioned within. For successful registration and advertisement of SSIDs, the APs must match the country code set on the WLC.
This guide assumes that you are familiar with creating a site hierarchy in Cisco DNA Center. Refer to the Base Automation Starter Kit for details on creating a site hierarchy. When complete, the hierarchy should look like the following.

**Cisco DNA Center network settings**
Cisco DNA Center lets you save common resources and settings with the Network Settings application. Information pertaining to the enterprise can be stored and reused across the network.

In the Cisco DNA Center UI, navigate to **Design > Network Settings**. This is where you configure all device-related network settings.

This guide assumes that you are familiar with creating shared services for the network across sites in Cisco DNA Center. Refer to the Base Automation Starter Kit for details. At this point, the required network information has been set at a global level for all fabric devices, as shown below.
Device credentials

Next, you define device credentials to allow Cisco DNA Center to manage network devices. Refer to the Base Automation Starter Kit for details.

The following screen shot shows an example username, netadmin.
IP pools and reservations

Define a global IP pool for the network

This guide assumes that you are familiar with the creation, management, and reservation of IP pools for fabric, virtual networks (VNs), and endpoints in Cisco DNA Center.

In the following example, we create a large global IP pool and reserve a subset for a building, SJC-13. Refer to the Base Automation Starter Kit for details. Navigate to Design > Network Settings > IP Address Pools to add an IP pool.

**Note:** Use an IP addressing scheme that meets your network specifications.

Skip DHCP and DNS assignment for now. (You will assign them later.)

Create reservations for campus, guest, multicast, and border handoff

In the hierarchy on the left, choose the SJC-13 building to create a reservation for it. Reservations are made at the building level when building an SD-Access fabric.
When you navigate to the building level, the following message appears. It explains the functioning of the hierarchy within Cisco DNA Center. To prevent its reappearance, check Don't show again. Click OK to continue.

At the SJC-13 level, click Reserve IP Pool to make a reservation specific to this building.
Enter the following information and click Reserve. The reservation will be used by the campus virtual network.

Similarly, build new IP pool reservations from the defined global IP pool for APs, border handoff, guest network (optional), and multicast (optional) under SJC-13. After all IP pools are created, you will see the following screen. Note that the subnet scheme might be different in your network.
Configure wireless SSIDs

Build a WPA2 enterprise SSID for the campus

Navigate to Design > Network Settings > Wireless.

Next to Enterprise Wireless, click Add.
On the next screen, enter sda-campus as the network name. Check the Fast Lane check box. Leave the remaining fields with their default values. Click Next.

Enter the following information to create a wireless profile.

Click Finish. The new SSID appears in the Enterprise Wireless area.
Build the guest wireless SSID (optional)
On the same screen, click **Add** next to Guest Wireless. For the SSID name, enter **sda-guest**. Click **Web Auth** to authenticate against ISE.

Click **Next**. In the Wireless Profiles area, check the **Campus-SSIDs** check box. Scroll down and click **Save**.
Click **Next**. In the Portal Customization area, click **Add** to bring up the Portal Builder. Enter the name **sda-guest-portal** in the top left of the window. Leave the defaults for the remaining values.

*Note:* You have the option to customize the portal or its behavior.

Scroll down to the bottom of the window and click **Save**. Click **Finish** to complete the guest wireless network.

**Use Case 2. SD-Access workflow: Policy**

After completing this workflow, you will be able to define and deploy a consistent policy across the site for wired and wireless users.

This workflow covers the following areas:

- Create a virtual network (macrosegmentation).
- Create and deploy a microsegmentation policy with custom contracts.
Security and policy are an integral part of SD-Access. Cisco ISE is a critical pillar that automates the security policy by integrating with Cisco DNA Center. Segmentation within SD-Access is enabled through VNs—which are equivalent to virtual routing and forwarding instances (VRFs)—and Cisco scalable group tags (SGTs). VNs provide macro-level segmentation with complete isolation of devices, whereas SGTs allow microsegmentation within the VN by providing logical segmentation based on group membership. ISE maintains all the scalable group information, which Cisco DNA Center uses for policies and the corresponding contracts. These policies and contracts are communicated back to ISE via REST APIs. ISE then pushes those policies and the scalable group access control list (SGACL) contracts to the network infrastructure.

Define a scalable group tag for user groups

A user group can be associated with a scalable group tag (SGT). SGTs are carried throughout the network and are the basis for access policy enforcement. This section explains how to define SGTs for the HR and ACCT groups.

Note: In the Cisco DNA Center UI, navigate to Policy > Dashboard and make sure that you see Scalable Groups, which confirms that the Cisco DNA Center and ISE pxGrid connection is up and the SGTs are synchronizing as expected. By default, ISE is predefined with 16 scalable groups.

From the Policy page, click Group-Based Access Control. Click Security Groups to view the default SGTs pushed from ISE. Click Add Groups. This launches a new browser tab that connects to ISE. You will notice in ISE these Scalable Groups are Referred to as Security Groups- these are all the same (SGT). Click the Add button above the table header.
For the SGT name, enter hr. Choose an icon, and add a description of your choice. Click Submit at the bottom of the page to save the new group. Do the same for a new SGT account. The following is merely an example; you can create SGTs with different names.
Return to Cisco DNA Center and refresh the Scalable Groups table. Go to the second page and verify that Cisco DNA Center learned the newly created SGTs.

Create the VN and choose scalable groups
This section explains how to create the campus and guest VNs and assign the desired scalable groups to the new VNs.

Campus virtual network
Click Virtual Network. Click the blue plus icon at the top left and add a new VN named Campus. Drag and drop the following scalable groups to the new VN on the right side. Click Save.

**Note:** The preceding screen shot is merely an example; you can customize the VN name and assign different scalable groups to it.
Once saved, the VN looks like the following example, with the new Campus VN selected on the left and four groups assigned to it on the right.

**Note:** By assigning scalable groups to a specific VN, you ensure that only users who authenticate with ISE and possess the specified tags have access to the VN. This means that a user can be in only one group, and that group determines what subnet or IP pool is available at the time of authentication. This process provides centralized, automated access control and segmentation based on a tested technology, Cisco TrustSec®.

By default, any network device or user within the VN is permitted to communicate with other users and devices in the same VN. For communication to occur between VNs, traffic must leave the fabric border and then return, typically traversing a firewall or fusion router.

**Guest virtual network (optional)**

Navigate to **Policy > Virtual Network**. Click the blue plus icon to add a new VN named Guest. Drag and drop only the **Guests** scalable group to the right side. Check the **Guest Virtual Network** check box. Click **Save**.

**Microsegmentation within a VN and policy between scalable groups**

Segmentation using SGTs provides an additional layer of granularity within a VN. The group membership in ISE is defined based on business roles and requirements. ISE can push an SGT and the corresponding dynamic VLAN to an endpoint through an authorization profile based on user credentials, device type, and profiling or posture state.
The rules that are built in this section using the Cisco DNA Center Policy application are implemented as downloadable SGACLs in ISE. The ACLs are then provided to the edge switches to be applied at the time of client authentication. These SGACLs are applied at the destination edge port for a consistent segmentation policy to be implemented at scale, in a practical way.

Create and apply a “deny all” rule between scalable groups
This section explains how to create a simple scalable group-based rule (SGACL). This rule blocks all network traffic between two scalable groups, ACCT and HR.

Note: After the user has been assigned a scalable group (either statically or through an ISE authorization rule), SGACLs are downloaded to the edge device. These rules are created, deleted, or updated dynamically via ISE; there is no need to roll out the updates device by device.

In the Cisco DNA Center UI, click Policy to begin building rules.

Navigate to Policy > Group-Based Access Control > Group-Based Access Control Policies.
Next to **Add Policy**, click the blue plus icon to bring up the **Create Policy** window.

Enter the following information to create a new policy with **acct** as the source scalable group, **hr** as the destination scalable group, and **deny** as the contract. Click **Save**.

At the warning message, click **Yes**.
By default, access control policies are unidirectional. Check the **Enable Bi-directional** check box to create a policy for bidirectional traffic. The newly created policy is listed on the Group-Based Access Control Policies page, as follows.

Create a custom contract (optional)
This section explains how to create a more discrete group-based access control policy that permits certain traffic types. The policy is created using the custom application tool, which allows for port and protocol when writing rules. The following example shows a rule to permit only HTTP and FTP traffic.

Navigate to **Policy > Group-Based Access Control > Access Contract**.

Click the blue plus icon next to Add Contract. In the Name field, enter `web_my_ftp_only`. Under Implicit Action, choose **Deny**.

Add a permit statement for http (TCP 80) and click **Add**.
Add a second permit statement that uses a custom port/protocol by clicking the blue **Add Port/Protocol** link.

<table>
<thead>
<tr>
<th>Action</th>
<th>Port/Protocol</th>
<th>Add</th>
<th>Edit</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permit</td>
<td>http (TCP 80)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Permit</td>
<td><strong>Select Port/Protocol</strong></td>
<td>Add</td>
<td>Edit</td>
<td>Delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In the Add Port/Protocol window, enter the following information, then click **Save**.

Choose the newly created port/protocol and click **Add** so it resembles the following screen shot. Click **Save**.
Under **Access Contract**, the new contract should match the following screen shot.

![Access Contract Screen Shot](image)

The following screen shot shows how to create a policy with a custom contract between the ACCT source scalable group and the HR destination scalable group. Do not click Save, because this example shows a custom contract.

![Policy Creation Screen Sshot](image)

Create a policy to block guest-to-guest access (optional)

This section explains how to create and apply a microsegmentation rule that blocks users in the Guest VN with the Guest tag from communicating on any port or protocol with other users in the same VN.

Navigate to Policy > Group-Based Access Control > Group-Based Access Control Policies.
Click **Add Policy**. Choose **Guests** as the source and destination scalable groups, binding them with a **deny** contract. Click **Save**.

**Use Case 3. SD-Access workflow: Fabric provisioning**

After learning this workflow, you will be able to easily enable end-to-end network connectivity.

This workflow covers the following area:

- Provision a single-site fabric with segmentation policy for wired and wireless.

**Provision devices from Cisco DNA Center**

**Provision wired switches**

In the Cisco DNA Center UI, navigate to **Provision > Device Inventory**.

Select all the devices that will become the fabric border, control plane, and fabric edges. Do not select the fusion router or the intermediate nodes. Use the Selected Devices pull-down to provision a device.
Enter the name of the site where your devices are deployed. You can select the same site for all devices by checking the **Apply to All** check box and clicking **Assign**.

**Note:** You can simultaneously provision only devices of the same device type. For example, do not provision a wireless LAN controller and a Cisco Catalyst 9500 Series switch together.

From the **Choose a site** drop-down list, choose **Global/SJC/SJC-13/SJC-13-2-MDF** for both cp-borders, and choose **Global/SJC/SJC-13/SJC-13-1** for edge-1.

At the bottom of the Provision Devices wizard, click **Next** three times to reach the Summary screen.
Click **Deploy**. In the pop-up window, click **Now** and then click **Apply**.

**Note:** Cisco DNA Center lets you deploy devices immediately or schedule deployment for later, such as during a change window.

After the provisioning process begins, a message in the lower right corner shows the status.

When a device is provisioned, Cisco DNA Center updates its internal database to include authentication, authorization, and accounting (AAA), 802.1X, and Cisco TrustSec, and then configures the devices to enable a secure communication channel with the device.

**Note:** Before proceeding, make sure that all devices are provisioned to a site and are in the Managed state.
Provision wireless LAN controllers
Navigate to Provision > Device Inventory.

Check the wlc1 check box. From the Actions drop-down list, choose Provision.

Choose Global/SJC/SJC-13/SJC-13-2-mdf as the site and click Next.

Choose Global/SJC/SJC-13 as the managed AP location and click Next.
Click **Next** again to reach the Summary screen, and then click **Deploy**.

The Provision Status of the WLC changes to **Success**.

After the provision process completes, make sure that the new sda-campus and sda-guest SSIDs are present on the WLC. On the WLC GUI, navigate to WLANs to see the SSIDs.

**Verify TACACS operation**

This section explains how to test and verify the TACACS configuration added during provisioning.

- See the section “Create SD-Access Device Credentials” to create network user credentials (netadmin) on ISE.
- Telnet/SSH into the provisioned device using the defined network credentials.
- Access the device vty console.
- Refer to the ISE TACACS Live Logs and confirm that authentication succeeded.
Create the SJC fabric domain and a transit site

After Cisco DNA Center provisions devices to sites, a fabric can be created. This section explains how to create a fabric domain and add devices to the new SD-Access fabric with unique fabric roles.

In the Cisco DNA Center UI, navigate to Provision > Fabric, where you create and manage your different fabric domains.

Next to Add Fabric Domain or Transit, click the blue plus icon and choose Add Fabric.
In the Add Fabric Domain window, enter sjc fabric as the fabric name. Choose SJC-13 as the location. Click Add.

The newly created fabric appears under Fabric Domains, as shown below.
Next, create an IP transit for the fabric site. Doing so enables external connectivity to and from the fabric site.

Navigate to **Provision > Fabric.** Next to **Add Fabric Domain or Transit,** click the blue plus icon and choose **Add Transit.**

In the Add Transit window, choose **IP-Based** as the transit type. Choose **BGP** (Border Gateway Protocol) as the routing protocol. Enter an Autonomous System (AS) number, which is defined on the fusion router, to form the BGP neighbor relationship with the border node. Click **Save.**
Add devices to the fabric and define their roles
This section explains how to add devices to the newly created fabric domain.

Navigate to Provision > Fabric and click the newly created sjc fabric to go to the fabric-specific management page, as shown below.

Under Fabric-Enabled Site, click Global/SJC/SJC-13. Doing so automatically shows devices associated with the site under the newly created fabric domain.

In the resulting topology, click a node and assign it a role. To add a device to the fabric, the device must be assigned one of these roles: Border, Control Plane (CP), or Edge. Control Plane and Border functionality can coexist on a single device. The wireless LAN controller will also be integrated into the fabric.
Choose `cp-border-1` and add it as **CP+Border**, as follows.

Next, enter additional information for the border node.

- In the pop-up window, under **Border to**, choose **Outside World (External)** to have it serve as the entry to and exit out of this fabric site.
- Enter the local BGP AS number. The following example uses **65534** as the local AS number on the border node.
- Choose the previously defined IP pool for external handoff.
- Check the **Connected to the Internet** check box.
- Under **Transits**, select and add the **sjc transit** that you created previously.
Choose **sjc transit** and click **Add Interface**, as shown below.

On the next screen, choose the border interface that connects to the fusion router.

Next, select all the VNs in the drop-down. This interface will be used to extend VN routes to the fusion router for external reachability.
A blue outline appears around cp-border-1, indicating that it will be added to the fabric when changes are applied.

Repeat these steps for the other fabric node acting as the CP+Border.

The following screen shot shows cp-border-2 added to the fabric, so it also has a blue border.
Next, click an edge node and click **Add to Fabric**. Verify that all switches have a blue border. Click **Save** and apply the changes.

A small green message appears in the lower right, indicating that fabric provisioning succeeded. All devices turn solid blue, indicating that they have been added to the SJC fabric.

**Note:** Hold down the Shift key and the left mouse button to highlight the access switches that are to be provisioned as edge nodes and click **Add to Fabric**.

Similarly, click the wireless LAN controller and click **Add to Fabric**. Save the changes. After provisioning succeeds, the devices turn solid blue, as shown below.
Configure the fusion router manually

To allow a host in a VN to communicate with a server and endpoint in the global routing table (GRT):

1. Create the Layer 3 connectivity between the border and the fusion router.
2. Use BGP to extend the VRFs from the border to the fusion router (ISR).
3. Use VRF leaking to share the routes between the VRF and GRT on the fusion router.
4. Share the VNs between two border nodes by forming BGP neighbors.

Once completed, the end host will route through the SD-Access fabric to the border, then leave the fabric to traverse the fusion router. The fusion router will leak the traffic to the GRT and vice versa, and then send it back to the border, where it will be reencapsulated into the SD-Access fabric and routed to the destination end host.

Note: We are using a VRF “underlay” to be able to easily leak routes between the shared services subnet and VNs created for the fabric overlay.

Refer to the appendix for a detailed configuration of the fusion router for VRF route leaking.
Onboard hosts
After the overlay is provisioned, IP address pools must be added to enable hosts to communicate within the fabric. When an IP pool is configured in SD-Access, Cisco DNA Center immediately connects to each edge node to create the appropriate switch virtual interface (SVI) to allow the hosts to communicate. In addition, an anycast gateway is configured for each IP pool on all edge nodes. This is an essential element of SD-Access, because it allows hosts to easily roam to any edge node with no additional provisioning.

This section explains how to configure the authentication policies for the SJC fabric.

Define the default authentication policy for fabric
In the Cisco DNA Center UI, navigate to **Provision > Fabric > sjc fabric > SJC-13** and click the **Host Onboarding** tab.

In the **Select Authentication Template** area, click **Closed Authentication**. Click **Save** and then **Apply**.

![Select Authentication Template](image)

This change enforces closed authentication on all edge ports within the fabric.

Bind IP pools to the Campus VN
In the Cisco DNA Center UI, navigate to **Provision > Fabric > sjc fabric > Host Onboarding**. The following screen shot is an example that shows Virtual Networks. Click **Campus**.

![Virtual Network](image)

In the Edit Virtual Network window, check the **SJC-13-campus** check box. Choose **Data** as the traffic type. Leave Layer-2 Extension with its default, which is **On**. Click **Update**, and then click **Apply**.

![Edit Virtual Network: Campus](image)

At this point, the VN has an IP address space to support clients. Now the VRF and LISP configurations for this VN are configured on the switches.
Bind the guest IP pool to the Guest VN (optional)
Under Virtual Networks, click Guest.

Check the sjc13-guest check box and choose Data as the traffic type. Make sure that Layer-2 Extension is set to On. Click Update and then Apply.

Bind the access point IP pool to the INFRA_VN
Click INFRA_VN and in the pop-up window, and choose the sjc13-APs pool. Make sure that Pool Type is set to AP, then click Update. Click Apply.

When you select the address pool for AP onboarding, Cisco DNA Center pushes a macro on the AP-connected fabric edge switch port. The AP is detected using Cisco Discovery Protocol and automatically assigned a VLAN corresponding to that subnet.

**Note:** If the AP was already plugged in, perform a shut/no shut on that port for the macro to populate.

Assign a static port for access points
For APs, we recommend that you change the ports to No Authentication, which is different from the global authentication template configured earlier.

Scroll to the bottom of the Host Onboarding page. In the **Select Port Assignment** area, choose a fabric edge and choose the AP-connected ports. Click **Assign**.
In the side window that opens, from the **Connected Device Type** drop-down list, choose **Access Point (AP)**. From the **Auth Template** drop-down list, choose **No Authentication**. Click **Update**.

Repeat the preceding steps to onboard additional APs in your network.

**Note:** Assuming that DHCP option 43 pointing to the WLC IP address is already configured on the DHCP server, the fabric edge-connected APs will register with the fabric WLC at this point.

Onboard wireless clients for Campus and Guest

**Bind IP pools to the Campus SSID**

Navigate to **Provision > Fabric > SJC-13 > Host Onboarding**. Scroll down to the **Wireless SSIDs** section.
Click the drop-down for the **sda-campus** address pool. From the **Address Pool** drop-down list, choose the IP pool **Campus: 100.100.0.0**, as shown below. Click **Save** and then **Apply**.

![Image of Wireless SSIDs](image)

At this point, Cisco DNA Center activates the WLAN.

**Bind IP pools to the Guest SSID**

Under **Provision > Fabric > SJC-13 > Host Onboarding**, go to the **Wireless SSIDs** section. Similarly, select the IP pool for **Guest** (created earlier).

![Image of Wireless SSIDs](image)

Click **Save** and then **Apply**.

**Note:** WLANs are not enabled (SSIDs broadcast) until an IP pool is assigned to the object in Cisco DNA Center.

**Provision access points**

Return to **Provision > Device Inventory**. Check the check box next to the AP, and then from the **Actions** menu, choose **Provision**.

![Image of Device Inventory](image)
Assign the AP to **Global/SJC/SJC-13/SJC-13-1**, then click **Next**.

![Provision Devices](image1)

On the Configuration screen, from the **RF Profile** drop-down list, choose **Low**. The following screen shot is merely an example; choose a profile that matches the RF environment at the location where the AP resides.

![Provision Devices](image2)

Click **Next**. On the Summary screen, click **Deploy** and then **OK**. The Provision Status of the AP changes to **Success**.

![Provision Devices](image3)

**Multicast**

Multicast traffic forwarding is used by many applications in enterprise networks to simultaneously distribute copies of data to multiple different network destinations. Within an SD-Access fabric deployment, multicast traffic flows can be handled in one of two ways—overlay or underlay—depending on whether the underlay network supports multicast replication.

The SD-Access use case focuses on multicast replication in the overlay. In this case, the first SD-Access fabric node that receives the multicast traffic (also known as the head end) must replicate multiple unicast copies of the original multicast traffic to each of the remote fabric edge nodes where the multicast receivers are located. This approach is known as head-end multicast replication. This approach provides an efficient multicast distribution model for networks that do not support multicast in the underlay. Dual rendezvous points (RPs) are supported on border nodes in a fabric site. When a redundant RP is added to the network, a Multicast Source Discovery Protocol (MSDP) session is enabled between the RP nodes for redundancy, automated by Cisco DNA Center. MSDP allows RPs to share information about active sources.
This section explains how to enable multicast in the fabric for the Campus VN.

1. Configure and reserve an IP pool for multicast. This will be used to configure RP and MSDP peering between the border nodes for redundancy (configured in Use Case 1).

2. Navigate to **Provision > Fabric > sjc fabric > SJC-13**. Right-click the border node and choose **Enable Rendezvous Point**.

3. In the **Associate Multicast Pools to VNs** window, expand the Campus VN and choose the **SJC_Multicast pool**.
4. Click Next and then Enable.
5. Repeat the preceding steps to enable a second RP on the second border node.
6. Click Save to save the multicast RP configurations.
7. Click the Host Onboarding tab. You should see an M icon on the Campus VN, indicating that multicast is enabled.

Layer 2 flooding

By default, traffic is not flooded in the fabric. However, traffic flooding is relevant in certain environments involving building management systems and Internet of Things (IoT) systems where endpoints rely purely on broadcast or link local multicast to enable communication. Similarly, Address Resolution Protocol (ARP) flooding is essential to wake up silent hosts for them to respond to network traffic.

With the Layer 2 flooding option in SD-Access, we are using multicast to enable the transport infrastructure to flood multidestination traffic types—ARP, broadcast, and link local multicast—on a per-IP pool basis. This requires multicast to be enabled on the underlay infrastructure.

1. Manually configure multicast on all underlay devices. This includes ip multicast-routing globally and ip pim sparse-mode on all routed uplinks. See the appendix for an underlay template that covers the multicast configuration.
2. Navigate to Provision > Fabric > sjc fabric > SJC-13 and click Host Onboarding. Choose the Campus VN. In the pop-up window, choose the sjc13-campus IP pool and set Layer-2 Flooding to On, as shown below.

3. Click Update. The configuration is pushed automatically on all fabric nodes to facilitate flooding of traffic in the IP pool.
Use case validation

Client group tag classification

- Connect two test workstations (wired or wireless) to the Campus VN. Connect one with ACCT and the other with HR credentials.
- Go to ISE and click Operations > Radius Live Logs. Click the detailed log for each client. Check for the SGT under Authorization. You should see an SGT of 16 for the HR user and 17 for the ACCT user.
- Both wired and wireless clients in the Campus VN should receive an IP address within the same 100.100.0.0/16 subnet.

All users in the campus have a consistent experience, both wired and wireless.

Test intra-VN connectivity

From the two clients, start an Internet Control Message Protocol (ICMP) ping test to the default gateway and to each other. The pings to the default gateway succeed, while the restrict-acct-to-hr policy prevents the HR user from communicating with the ACCT user despite sharing the same subnet.

Return to the Group-Based Access Control Policies window in Cisco DNA Center. Delete the restrict-acct-to-hr policy while the ping tests are still running on the clients. Connectivity between the HR client and the ACCT client is restored shortly after the removal of the rule from Cisco DNA Center.

Verify guest wireless access (optional)

Use a wireless-capable test client to connect to the sda-guest SSID being broadcast by the AP.

Once connected, open a browser window and try to access a web page. You should automatically be redirected to a captive portal window. Log in to the network with a new account by using the registration link at the bottom. After you are logged in to the guest wireless network, test access to the web.

Appendix

Underlay template

The recommended manual underlay should consist of /32 routing for all the loopbacks and point-to-point interfaces present on all devices. These loopbacks are used for the fabric overlay connectivity. There should not be any subnet routes for our underlay subnet in use on the fabric devices. The only subnets in the underlay are external IP routes such as the Cisco DNA Center, ISE, WLC, and DHCP/DNS subnets.

Use the following template to configure devices for the underlay.

```plaintext
service timestamps debug datetime msec
!
service timestamps log datetime msec
!
service password-encryption
!
service sequence-numbers
!
```
! Setup NTP Server
! Setup Timezone & Daylight Savings

ntp server ${ntpServerIp}
!
</#if>
ntp update-calendar
!
! Enable external SSHv2 access
!
crypto key generate rsa label dnac-sda modulus 1024
ip ssh version 2
!
ip scp server enable
!
line vty 0 15
login local
transport input ssh
! maybe redundant
transport preferred none

! Set VTP mode to transparent (no auto VLAN propagation)
! Set STP mode to Rapid PVST+ (prefer for non-Fabric compatibility)
! Enable extended STP system ID
! Set Fabric Node to be STP Root for all local VLANs
! Enable STP Root Guard to prevent non-Fabric nodes from becoming Root
! Confirm whether vtp mode transparent below is needed

vtp mode transparent
!
spanning-tree mode rapid-pvst
!
spanning-tree extend system-id
no udld enable
!
errdisable recovery cause all
!
errdisable recovery interval 300
!
ip routing

! ip multicast-routing !

! ip pim ssm default !

! Enable SNMP and RW access based on ACL !
snmp-server community ${snmpRO} RO !
snmp-server community ${snmpRW} RW !

</#list>
</#if>

hostname ${hostname} !

! Config below applies only on underlay orchestration

! ! Setup a Loopback & IP for Underlay reachability (ID) ! Add Loopback to Underlay Routing (ISIS) !

interface loopback 0
description Fabric Node Router ID
ip address ${xtrIp} 255.255.255.255
ip router isis
ip pim sparse-mode
clns mtu 1400
! Set MTU to be Jumbo (9100, some do not support 9216)!
${systemMtu}
!
!
ip multicast-routing !

! FABRIC UNDERLAY ROUTING CONFIG:

! ! Enable ISIS for Underlay Routing ! Specify the ISIS Network ID (e.g. encoded Loop IP)
! Specific the ISIS domain password
! Enable ISPF & FRR Load-Sharing
! Enable BFD on all (Underlay) links
!
router isis
net ${isisNetAddress}
domain-password ${isisPassword}
ispf level 1-2
metric-style wide
nsf ietf
log-adjacency-changes
bfd all-interfaces
! passive-interface loopback 0
!
! FABRIC UNDERLAY INTERFACE CONFIG:
! Enable ISIS for Underlay Routing on all uplink interfaces
!
interface TenGigabitEthernetx/x/x
description Fabric Physical Link
no switchport
dampening
ip address x.x.x.x 255.255.255.252
ip router isis
logging event link-status
load-interval 30
bfd interval 500 min_rx 50 multiplier 3
no bfd echo
isis network point-to-point
ip pim sparse-mode

Configure dynamic authentication with ISE
The ISE authorization policy is defined by configuring rules based on identity groups or other conditions. In this
guide, the authorization policy is used to authenticate users to SD-Access and authorize them to use network
resources. In this guide local users are used. Majority of customers will integrate ISE with AD and use AD users in
their authentication and authorization policies. Please refer to the AD ISE Integration guide for establishing this
integration and using the AD groups in authorization policies.
Create user identity groups for the Campus scenario

1. In ISE, from the main menu, choose Administration > Identity Management > Groups.

2. On the left side, click User Identity Groups. Click Add above the table to create a group for the ACCT client.

3. Enter a name for the user identity group. (The description is optional.) Click Submit.

A new ACCT user group is created, as shown below.
4. Create another group for HR and Employee.

Create an identity for each Campus user
1. In ISE, from the lower menu bar, choose Administration > Identity Management > Identities.

2. Click Add to add a user to ISE.
3. Create a user with a password and assign that user to the groups HR and Employee. Click Submit.
4. Repeat the preceding steps to create additional users under user groups.

Create SD-Access device credentials
After Cisco DNA Center provisions a networking device, its configuration is modified to leverage RADIUS and an AAA server, which is ISE. Therefore, any device users who perform administration of the network devices must be added to ISE.

Create an admin user as described in the preceding section. This use cases uses the netadmin user from the netadmin user group.
Define an 802.1X authorization profile and policies for Campus users
The authorization policy checks the user identity groups to see if a user authenticating to the network is a member of a known group (Employee, ACCT, HR). The policy verifies that the user authenticates via an 802.1X connection. If the user's password is correct, authentication succeeds and the user is assigned the correct SGT and VLAN.

This section explains how to create a rule for each user identity group: Employee, ACCT, and HR.

1. In ISE, from the lower menu bar, choose **Identities > Policy > Policy Sets.**

2. Use the arrow on the far right to expand the default policy set.

3. Click the arrow on the last row to expand **Authorization Policy.**
4. Locate the top-most rule, click the arrow to the far right, and choose **Insert New Row from Above**. Note: Administrators can also copy and edit an existing rule, if preferred. Doing so is helpful when adding multiple similar rules.

![Image showing policy set with rules]

5. Name the rule **802.1xACCT**. Under Conditions, click the plus icon, which opens the Conditions Studio.

6. In the right panel, click the **Click to add an attribute** window. Click the identity group icon. Choose **IdentityGroup Name**. To the right of the **Equals** drop-down list, choose **User Identity Groups: ACCT**, as follows.

![Image showing Conditions Studio with IdentityGroup Name selected]

7. When complete, the authentication policy appears as a new entry in the default policy.

![Image showing policy set with new entry]

8. After the conditions are defined, you must select the results of a match. In the first window, click the plus symbol and choose **Create a New Authorization Profile**. The authorization profile is where VLAN association can be created for later use by the 802.1X authorization policy. The VLAN used must be the one that Cisco DNA Center generates automatically when provisioning the IP pools.

![Image showing Create a New Authorization Profile option]
9. Name the authorization profile CAMPUS_USER_AUTHZ. From the Access Type drop-down list, choose ACCESS_ACCEPT. Enter an optional description. In the Common Tasks area, choose VLAN and 100_100_0_0-Campus, which is mapped to IP pool 100.100.0.0/16. Click Save.

![Authorization Profile](image)

**Note:** Cisco DNA Center generates well-formatted VLAN names when deploying an IP pool to a VN. The format is [<IP_Pool_Subnet>_<Virtual_Network_Name>], where the subnet octets are separated by underscores, not decimals.

10. Click Save. You are returned to the policy set screen. Choose the newly created CAMPUS_USER_AUTHZ authorization profile.

![Policy Set](image)

11. In the second window, choose the security group ACCT. Click Save.

![Security Group](image)
12. Repeat the preceding steps to create rules for the HR group.

ISE policies for wireless guest access
This section describes Cisco DNA Center’s automatically configured policies in ISE to support the Guest VN’s wireless captive portal.


2. Under Standard Authorization Profiles, choose sda-guest-portal_Profile. Cisco DNA Center created this profile automatically to support the Guest VN wireless network as part of the workflow completed earlier.
3. Scroll down to **Common Tasks** and check the **Static IP/Host name/FQDN** check box. In the text box, enter the ISE IP address as the static IP address.

![Common Tasks](image)

4. Scroll down to the bottom of the page and click **Save**.

**Note:** In a production environment, this change is not required. This change is required in a lab network when no DNS reverse lookup entry for ISE is available. For reachability, clients must be offered the IP address of the ISE as opposed to its FQDN.

**Fusion configuration**

To allow a host in a VN to communicate with a server and endpoint in the GRT:

1. Create the Layer 3 connectivity between the border and the fusion router.
2. Use BGP to extend the VRFs from the border to the fusion router (ISR).
3. Use VRF leaking to share the routes between the VRF and GRT on the fusion router.
4. Share the VNs between two border nodes by forming BGP neighbors.

Once completed, the end host will route through the SD-Access fabric to the border, then leave the fabric to traverse the fusion router. The fusion router will leak the traffic to the GRT and vice versa, and then send it back to the border, where it will be reencapsulated into the SD-Access fabric and routed to the destination end host.
Create Layer 3 connectivity between the border and the fusion router

1. The first task is to allow IP connectivity from each border node to each fusion router for every VN that requires external connectivity.

In this example, shared services (DHCP, DNS, ISE, WLC, and Cisco DNA Center) are part of the vrf underlay on the fusion router.

Cisco DNA Center automatically configures the border for external BGP (eBGP) handoff (toward the fusion router). View that configuration and then configure the fusion router with the IP addresses in the point-to-point subnet. Use the Layer 3 subinterface on the fusion router that matches the VLAN on the border node.
Enter the following command-line interface (CLI) commands to verify the external handoff configuration pushed by Cisco DNA Center on the fabric border nodes:

- `show running-config | section vrf definition`
- `show running-config | section interface Vlan`
- `show running-config | section router bgp`

See the following logical representation.

For Cisco Catalyst 3000 and 6000 Series Switches and the Cisco Catalyst 9000 family, a trunk is configured on the border to the fusion router, along with an SVI for each VRF that is handed off. If the border is an ASR or ISR, Cisco DNA Center configures subinterfaces for the handoff.

2. View the configuration that Cisco DNA Center applies on the border’s uplink to the fusion router during the IP transit handoff:
   - `Border# show run int <interface>`
   
   where `<interface>` is the external link that was selected under IP transit during fabric border provisioning.

3. Create the Layer 3 subinterfaces on the fusion router. Define the VRFs first, and then configure the Layer 3 subinterfaces.

   Copy the Campus VRF from the border to the fusion router. Copying is required, because the Route Distinguisher (RD) and Route Target (RT) must match exactly, and they are automatically generated numbers from Cisco DNA Center.

   Copy the auto-provisioned vrf definition from the border configuration.

   **EXAMPLE:**
   ```
   Border# show running-config | section vrf definition
   Building configuration...

   Current configuration : 25943 bytes
   <..snip..>
   boot-end-marker
   !
   !
   vrf definition Campus
   rd 1:4099
   !
   ```
Address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
exit-address-family

Paste the auto-provisioned vrf definition from the border configuration into the fusion router.

vrf definition Campus
  rd 1:4099
  !
  address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
exit-address-family
  !

On the fusion router, make sure the Layer 3 interface that is connected to the border is not configured with an IP address. Create Layer 3 subinterfaces on the link connecting the border node so the VNIs can be carried to the fusion router.

Repeat the steps for every VN on the fabric border.

4. Configure the fusion router for subinterfaces. Make sure the VRFs and VLAN numbers align with the border.

  !
  interface GigabitEthernet0/0/2.3001
    description INFRA_VN interface to CP-BORDER-1
    encapsulation dot1Q 3001
    vrf forwarding underlay
    ip address 172.30.100.2 255.255.255.252
    no ip redirects
  !
  interface GigabitEthernet0/0/2.3002
    description vrf interface to CP-BORDER-1
    encapsulation dot1Q 3002
    vrf forwarding Campus
    ip address 172.30.100.6 255.255.255.252
    no ip redirects
  !
  interface GigabitEthernet0/0/2.3003
    description vrf interface to CP-BORDER-2
    encapsulation dot1Q 3003
    vrf forwarding Campus
    ip address 172.30.100.10 255.255.255.252
    no ip redirects
1. On the fusion router, create a BGP router instance using the AS number defined earlier (65535). Define the address family VRF for each VN that was automated on the border.

```
router bgp 65535
  bgp router-id 100.127.0.2
  bgp log-neighbor-changes

address-family ipv4 vrf underlay
  network 100.64.0.0 mask 255.255.255.0
  network 100.65.0.0 mask 255.255.255.0
  network 100.127.0.0 mask 255.255.255.0
  network 100.128.0.0 mask 255.255.255.0
  network 172.30.100.0 mask 255.255.255.252
  network 172.30.100.12 mask 255.255.255.252
  neighbor 172.30.100.1 remote-as 65534
  neighbor 172.30.100.1 update-source GigabitEthernet0/0/2.3001
  neighbor 172.30.100.1 activate
  neighbor 172.30.100.13 remote-as 65534
  neighbor 172.30.100.13 update-source GigabitEthernet0/0/2.3004
  neighbor 172.30.100.13 activate
```

5. Verify IP connectivity between the fusion router and the border for each VRF.

Extend virtual networks from the border to the fusion router

Cisco DNA Center has fully automated the border BGP handoff configuration. Configure the fusion router to extend the fabric VNs.
maximum-paths 2
exit-address-family
!
address-family ipv4 vrf Campus
  network 172.30.100.4 mask 255.255.255.252
  network 172.30.100.8 mask 255.255.255.252
  neighbor 172.30.100.5 remote-as 65534
  neighbor 172.30.100.5 update-source GigabitEthernet0/0/2.3002
  neighbor 172.30.100.5 activate
  neighbor 172.30.100.9 remote-as 65534
  neighbor 172.30.100.9 update-source GigabitEthernet0/0/2.3003
  neighbor 172.30.100.9 activate
  maximum-paths 2
  exit-address-family
!

2. Verify that BGP neighborship is established between the border and fusion router for all defined VNs.
   sh ip bgp vpnv4 all summary

3. The fusion router now knows about each VN route learned via an eBGP session. Verify the IP routes on the
   fusion router for each VRF.
   Show ip route vrf <VN_name>

Use VRF leaking to share routes on the fusion router and distribute them to the border
Route maps are used to select the routes to leak to VNs. Import and export of these route maps enables the VRF
route leaking required on the fusion router.

! vrf definition Campus
  rd 1:4099
  !
  address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
  route-target import 65535:102
exit-address-family
!
vrf definition underlay
  rd 65535:102
  route-target export 65535:102
  route-target import 65535:102
  route-target import 1:4099
!
  address-family ipv4
exit-address-family

Share virtual networks between border nodes for traffic resiliency
Deploy a resilient direct link between border nodes to enable automatic traffic redirection against connectivity failures between a border and fusion device. Create an internal BGP (iBGP) neighbor relationship between the border nodes for every configured VN.

Border 1
!
vlan 41
no shut
!
int vlan 41
  vrf forward Campus
  ip address 172.30.100.101 255.255.255.252
desc L3 Border 2 Border iBGP link in Campus VN
no shut
!
int < interface >
  description "Connection to Border-2"
  switchport
  switchport mode trunk
no shut
!
router bgp <AS number>
!
address-family ipv4 vrf Campus
    neighbor 172.30.100.102 remote-as 65534
    neighbor 172.30.100.102 activate
!
exit-address-family

Border 2
!
vlan 41
no shut
!
int vlan 41
    vrf forward Campus
    ip address 172.30.100.102 255.255.255.252
    desc L3 Border 2 Border iBGP link in Campus VN
    no shut
!
int gig < >
    desc “Connection to Border-2”
    switchport
    switchport mode trunk
    no shut
!
router bgp 65534
!
address-family ipv4 vrf Campus
    neighbor 172.30.100.101 remote-as 65534
    neighbor 172.30.100.101 activate
!
exit-address-family