



Implementing Cisco SD-Access with DNA Center

DNA Center & SD-Access Overview



What is SD-Access?

- + Software Defined Access (SD-Access) is Cisco's solution for central configuration automation and management of Catalyst Switches
 - + Central controller is called Digital Network Architecture Center (**DNA Center** / DNAC)
 - + DNAC was recently renamed to **Cisco Catalyst Center**
- + SD-Access uses VXLAN instead of traditional VLANs to segment traffic
 - + First build infrastructure connectivity for the underlay network
 - + E.g. IPv4 routing connectivity between switches in the global VRF table
 - + Next, build an overlay network for "customer" traffic
 - + e.g. VRF "Customer1" for end-host application traffic
 - + End-host traffic is tunneled between switches using VXLAN
 - + Original IP over Ethernet packet goes inside new IP/UDP/VXLAN header

How Does SD-Access Work? – Network Discovery & Automation

- + DNA Center centrally controls/automates the SD-Access deployment as follows:
 - + Run “**Discovery**” to find new devices for “**LAN Automation**”
 - + E.g. assign DHCP addresses to new switches for Auto-Install / Plug-and-Play / ZTP
 - + Once discovered, automatically configure switch-to-switch links with **IS-IS**
 - + We now have IP reachability between switches in the global VRF (underlay)
 - + Run Locator/ID Separation Protocol (**LISP**) from **Edge Switches** to **Border Switch(es)**
 - + Allows Border to learn which Edge Switches have which endpoints attached

How Does SD-Access Work? - Forwarding

- + Edge Switches uses LISP for forwarding decisions as follows:
 - + We tell DNAC to assign VLAN “Users” to Edge-Switch1 Gi0/1 & Edge-Switch2 Gi0/1
 - + Each VLAN maps to a unique VXLAN Virtual Network Identifier (VNI) “V”
 - + Mappings happen automagically, we don’t care about them
 - + Edge-Switch1 learns MAC/IP “A”, and registers it to Border via LISP
 - + “A” is reachable via Edge-Switch1 Loopback “X”
 - + Edge-Switch2 learns MAC/IP “B”, and registers it to Border via LISP
 - + “B” is reachable via Edge-Switch2 Loopback “Y”
 - + “A” sends a packet to “B”
 - + Edge-Switch1 asks Border with LISP, “where is B located?”
 - + Border says “B” is via “Y” with LISP
 - + “A” to “B” traffic is now VXLAN tunneled from Loopback “X” to Loopback “Y”
 - + VXLAN header includes VNI “V” so we know which segment it is for





Implementing Cisco SD-Access with DNA Center

SD-Access Implementation Overview



In This Section

- + SD-Access implementation steps overview
- + DNA Center UI overview

SD-Access Implementation Overview

- + What are we trying to accomplish?
 - + Establish basic IP connectivity between end-hosts attached to SD-Access network

- + What steps are involved?
 - + Establish management connectivity between DNA Center & SD-Access Devices
 - + E.g. discover devices with SSH / SNMP / NETCONF
 - + Program the underlay network from DNA Center
 - + E.g. enable IS-IS between the switches, define LISP nodes & roles
 - + Program the overlay network from DNA Center
 - + E.g. define the VLANs & IP subnets for the end-host applications

High Level Steps for Implementing SD-Access with DNA-C - Part 1/4

- + Define the Sites' Area/Building/Floor under Network Hierarchy
 - + E.g. Chicago > 1000 W Addison St. > Main Floor
- + Define pools of IP addresses for automation
 - + Underlay pool for LAN Automation
 - + Infra pool for WLC/AP connectivity
 - + L3 Handoff pool for Border routing
 - + End host pools (e.g. Employees, Guest, etc.)
- + Define credentials for DNAC to login to devices
 - + SSH username/password, enable password, SNMPv2/3, NETCONF
- + Perform Network Discovery to add devices to inventory
 - + Assumes at least one switch (e.g. Border Switch) has IP address and SSH/SNMP/NETCONF credentials pre-configured via CLI
 - + I.e. enable **netconf-yang** in global config on Border Switch CLI

High Level Steps for Implementing SD-Access with DNA-C - Part 2/4

- + Prepare for LAN Automation
 - + New switches should be blank and at initial config dialogue
 - + More info at [LAN Automation Deployment Guide – PNP Agent Initial State](#)
- + Enable LAN Automation
 - + Choose port(s) on “Seed Device” (e.g. the Border Switch) where the other switches are attached downstream
- + Create a “Fabric Site” and “Provision” the devices to the Fabric Site
 - + Different than “assigning” them to a site; this is a required step
- + Define the “Virtual Networks” (VNs) for the site
 - + VN numbers will map to VLANs on the backend automatically
 - + You can specify the VLAN manually or let it auto-generate the number
 - + VNs will map to previously created IP address pool

High Level Steps for Implementing SD-Access with DNA-C - Part 3/4

- + Enable at least one (LISP) Control Plane Node
 - + This is typically also a function of the Border Switch
 - + Defines if you are running LISP/BGP or LISP Pub/Sub
 - + LISP Pub/Sub requires newer code on Border & Edges
- + Define which switches are Edge Nodes
 - + I.e. the switches attached to end-hosts
- + Enable at least one Border Node
 - + Used to advertise routes out of the SD-Access fabric towards the WAN
 - + Advertisement is with BGP + VRF-Lite
 - + Could be the same as the Control Plane Node(s), but doesn't have to be
- + Configure a "Fusion Router" to peer BGP with the Border Node
 - + Fusion Router leaks routes from Border Node into global routing table
 - + Just a regular router, not part of the LISP / VXLAN network

High Level Steps for Implementing SD-Access with DNA-C - Part 4/4

- + “Onboard” the end-hosts
 - + Choose which VLAN/VNs are assigned to the Edge Switch(es) access ports
 - + Can also use ISE integration to assign the Security Group Tag (SGT)
 - + Allows for filtering / Network Admission Control (NAC) based on tag

- + Verify that end-hosts are registered to LISP control-plane
 - + **Edge# show mac address-table**
 - + **Edge# show ip route vrf [customer_vrf]**
 - + **Edge# show lisp vrf**
 - + **Edge# show lisp instance-id [id] dynamic-eid [detail]**
 - + **Border# show ip lisp map-cache instance-id [id]**





Implementing Cisco SD-Access with DNA Center

DNA Center Network Hierarchy



What is DNA Center Network Hierarchy?

- + Cisco DNA Center uses Network Hierarchy by defining **Areas**, **Buildings**, and **Floors** to mirror the physical network deployment
- + **Devices** are assigned to **Buildings** & can form hierarchy in the Inventory Tool
- + **Access Points (APs)** are assigned to **Floors**
 - + Floor definitions are required if you are running WLAN
- + **Buildings** will later represent our “**Fabric Sites**” for automatic provisioning

Defining the Network Hierarchy

- + DNAC > Design > Network Hierarchy
 - + Define an Area
 - + E.g. “Chicago”
 - + Define a Building
 - + E.g. “1000 W Addison St.”
 - + Define a Floor
 - + E.g. “Main Concourse”





Implementing Cisco SD-Access with DNA Center

DNA Center Network Settings



What are DNA Center Network Settings?

- + Network Settings are definitions for common network resources such as...
 - + DHCP, DNS, NTP, AAA, & Syslog Servers' IP addresses
 - + Device Login & Password credentials for SSH, SNMP, HTTP(s), NETCONF
 - + Pools of IP Addresses used for automating...
 - + Underlay connectivity between the Switches
 - + Infrastructure connectivity for Wireless Access Points
 - + “Layer 3 Handoff” pools for External BGP routing towards the WAN
 - + End-host pools for users, guests, applications, etc.

Defining the Network Settings

- + DNAC > Design > Network Settings > Network
 - + DHCP, DNS, NTP, & AAA Servers' IPs

- + DNAC > Design > Network Settings > IP Address Pools
 - + Pools can be defined at the Global, Area, Building, Floor, etc. level
 - + “Global” level pools should be large ranges, e.g. 10.1.0.0/16
 - + “Site” level pools are sub-ranges of this, e.g. 10.1.2.0/24
 - + Pools must be pre-defined first, so we can map them to VNs later
 - + Pools must be at the correct level of hierarchy
 - + E.g. if wrong, they won't show up for VN assignment later

Defining the Device Credentials

- + DNAC > Design > Network Settings > Credentials
 - + SSH (port 22 default) & NETCONF (port 830 default)
 - + SNMP v2 / v3
 - + HTTP / HTTPS
- + Credentials must be configured on the other side for discovery to work:

```
Border#
```

```
ip domain-name INE.local
```

```
username dnac secret PASS123
```

```
enable secret PASS456
```

```
!
```

```
line vty 0 4
```

```
login local
```

```
transport input ssh
```

```
!
```

```
crypto key generate rsa general-usage modulus 4096
```

```
!
```

```
netconf-yang
```





Implementing Cisco SD-Access with DNA Center

DNA Center Device Discovery



What is DNA Center Device Discovery?

- + DNAC can automatically discover & manage SD-Access underlay devices
 - + Devices are discovered and then assigned to previously defined Sites
- + Assumes IP reachability between the DNAC & managed devices
 - + At least one device must start with basic IP & routing towards DNAC via CLI
 - + e.g. a static default route
- + Assumes devices have pre-defined credentials & remote mgmt is enabled
 - + Usernames & passwords, enable SSH & NETCONF, SNMPv2/3, etc. via CLI
- + DNAC runs a “Discovery Job” by defining an IP address range to search
 - + CDP can then be used to further discover the first device’s neighbors

Performing Network Discovery

- + DNAC > Tools > Discovery > Add Discovery
 - + Define the IP address(es) of Devices to discover
 - + Reference the previously created Device Credentials
 - + Assign Discovered Devices to your Site
- + At least one “**Seed**” device needs to have a basic config
 - + E.g. on Border CLI, define IP & default route, enable SSH, NETCONF, & SNMPv2/3
- + All devices ultimately need IP transport to DNA-C itself
 - + I.e. DNA-C can't program them if it can't reach them
- + Note that Discovery can be a slow process...





Implementing Cisco SD-Access with DNA Center

DNA Center LAN Automation



What is DNA Center LAN Automation?

- + DNAC can automate the provisioning of new network devices
 - + Onsite hands rack & stack, cable, and power up the switches with blank config
 - + DNAC uses a combo of PnP (Plug and Play) & Zero Touch Provisioning (ZTP)
 - + E.g. Auto-Install is used for DNAC to push a config to the device
 - + DNAC automates IP addressing & IS-IS routing
 - + Every switch advertises Lo0 into IS-IS for its VXLAN Tunnel Endpoint (VTEP)
 - + DNAC can also automate software updates, and apply predefined templates
- + More info at [DNA Center SD-Access LAN Automation Deployment Guide](#)

Performing LAN Automation

- + DNAC > Provision > LAN Automation
 - + Choose the Site
 - + Choose the Seed Device
 - + Choose target port(s) where the other switches are attached, add them, & click Next
 - + Choose the IP Address Pool for automated Underlay addressing
 - + Define Discovered Devices Hostname Prefix
 - + E.g. "CHI1-Edge-"

LAN Automation Behind the Scenes

- + What is DNAC actually doing during LAN Automation?
 - + On Seed, enables IP on VLAN 1 SVI running IS-IS
 - + On Seed, creates DHCP pool for VLAN 1, & sets the target ports to access vlan 1
 - + “New Switch” boots up blank and performs Auto-Install
 - + Make sure you don’t send any keys to the console, even [CR]
 - + Enables IP on VLAN 1 SVI on “New Switch” w/ IS-IS; routing fabric is now established
 - + Rinse and repeat...





Implementing Cisco SD-Access with DNA Center

SD-Access Fabric Sites

What are DNA Center Fabric Sites?

- + In SD-Access, a **“Fabric Site”** means an independent network containing:
 - + One or more LISP Control Plane Nodes
 - + One or more LISP Edge Node
 - + Typically, at least one Fabric Border Node to exit the LISP network
 - + E.g. route towards the WAN
 - + Typically, an Identity Services Engine (ISE) Policy Service Node (PSN)
 - + Typically, one or more Wireless LAN Controllers (WLC) in Fabric-Mode

- + A **“Fabric Site”** maps back to the Network Hierarchy defined in DNAC
 - + E.g. you could have a large campus with multiple Buildings, each being a separate Fabric Site
 - + LISP/VXLAN could be used to inter-connect Fabric Sites, or just IPv4

Creating the Fabric Site

- + DNAC > Provision > SD-Access > Fabric Sites > Create Fabric Sites
 - + Choose Site
 - + Define Authentication Template
 - + I.e. none, open dot1x, or closed dot1x
 - + Deploy





Implementing Cisco SD-Access with DNA Center

SD-Access Device Provisioning



What is DNA Center Device Provisioning?

- + Once a **Fabric Site** is defined, devices in **Inventory** are **Provisioned** to the **Fabric Site**
- + Provisioning takes the Devices, applies any defined segmentation **Policy**, and deploys them to the **Fabric Site**
- + Once devices are provisioned to a site, their Fabric Roles can be defined
 - + E.g. Control Plane, Border, and/or Edge
 - + DNAC automatically creates the necessary infrastructure config for the fabric overlay

Provisioning the Devices to the Site

- + DNAC > Provision > Inventory
 - + Check the Device > Actions > Provision > Provision Device
 - + Repeat for all Devices for the Site
- + Verify that the devices were successfully provisioned to the Site
 - + DNAC > Provision > SD-Access > Fabric Sites
 - + Choose site, click a device name to open pop-out
 - + In pop-out window, click Fabric tab (should be default)
 - + It should allow you to configure the device
- + If “*Device not Provisioned*”, check the DNAC logs
 - + DNAC > Activities > Tasks





Implementing Cisco SD-Access with DNA Center

SD-Access Virtual Networks



What are DNA Center Virtual Networks?

- + Virtual Networks (VNs) are VRFs behind the scenes
 - + VRFs are logical layer 3 routing tables, similar to how VLANs separate layer 2
 - + Devices within the same VN can talk by default
 - + Devices in different VNs cannot talk by default
 - + No route leaking between VRFs unless you manually configure it
- + One or more IP Address Pools map to the VN
 - + E.g. you can have more than one VLAN in the VRF
- + Edge Switches learn IP/MAC addresses on their access ports, then advertise them into LISP with the VN information
 - + Implies that VNs could have overlapping addresses
 - + E.g. both “Employees” and “Guests” could use 192.168.0.0/24
- + VN information is encoded in the VXLAN Data Plane between Edge Switches
 - + Edge switches know which VRFs the packets belong to due to the tag

Creating & Assigning the Virtual Networks

- + DNAC > Provision > SD-Access > Virtual Networks > Create Virtual Network
 - + Define VN Name
 - + E.g. “Employees” & “Guests”
- + DNAC > Provision > Fabric Site > Host Onboarding > Virtual Networks
 - + Define the IP Pool for Overlay addressing
 - + VLAN info can be manually defined or auto-generated
 - + Can define Security Group for NAC w/ISE integration
 - + Define Traffic Type
 - + Data or Voice
 - + Wireless Pool checkbox
 - + Needed if VN used for WLAN later
 - + Add, Rinse & Repeat for additional VLANs or VNs, then Deploy





Implementing Cisco SD-Access with DNA Center

SD-Access LISP Device Roles



What are the SD-Access LISP Device Roles?

- + DNAC has control over three LISP device roles in the fabric
 - + Edge Nodes
 - + Control Plane Nodes
 - + Border Nodes

- + Edge Nodes
 - + Receives IPv4/IPv6 traffic from end hosts
 - + Does a LISP lookup on the destination to find the RLOC/VTEP
 - + I.e. the destination Switch's Loopback0
 - + If destination unknown, ask the Control Plane Node
 - + Sends & receives Overlay VXLAN packets with other Edge Nodes, using the Underlay for transport

What are the SD-Access LISP Device Roles?

- + Control Plane Nodes are like BGP RRs, but for LISP
 - + Learn all the LISP routes (IPs & MACs) from the Edge Nodes
 - + Reply to Edge Nodes when they need to do a LISP lookup
 - + Control Plane nodes don't have to be in the Data Plane
 - + E.g. a node could be Control but not Border, or both

- + Border Nodes
 - + Exit from the LISP network to the IP network
 - + I.e. the path out of the fabric to the WAN
 - + DNAC automates BGP configuration on Border Nodes to Fusion Routers
 - + VLAN sub-interfaces are created, one per-VN
 - + "L3 Transit" Pool is used to automate IP addressing
 - + EBGP peerings are established, one per-VN

Configuring the SD-Access Edge Switches' Role

- + DNAC > Provision > Fabric Site
 - + Select the Edge Switch
 - + Go to Fabric tab
 - + Enable "Edge Node"
 - + Add & Deploy

Configuring the SD-Access LISP Control Plane Node

- + DNAC > Goto Provision > Fabric Site
 - + Click Topology View in upper right to see visualization
 - + Click List View in upper right to list all Devices

- + Select the Border Switch and go to Fabric tab
 - + Enable "Control Plane Node"
 - + Choose LISP/BGP (backwards compatible) or LISP Pub/Sub (requires newer code)

Configuring the SD-Access L3 Transit Network

- + The “L3 Transit” network will be used for external routing between the Border Node and the Fusion Router
 - + On the Border Node, each peering will be in a separate VRF
 - + On the Fusion Router, each peering will be in the global (default) VRF
 - + Fusion router is outside the scope of SD-Access
 - + Could be any router running BGP to Border Node(s)
- + DNAC > Provision > SD-Access > Transits > Create Transit
 - + Define Name
 - + Define Transit Type
 - + e.g. IP-Based
 - + Define BGP Remote-AS of Fusion Router

Configuring the SD-Access Border Node

- + DNAC > Provision > Fabric Site
 - + Select the Border Switch and go to Fabric tab
 - + Enable "Border Node" & click configure
 - + Check "Enable Layer-3 Handoff", set the BGP Local ASN
 - + Under "Add Transit Site", choose the previously created Transit
 - + Select IP Pool for L3-Handoff from Border to Fusion
 - + Click Add External Interface
 - + I.e. the Layer 2 Trunk between Border & Fusion
 - + Enable the Virtual Networks (VNs) you want to advertise into BGP
 - + Choose a unique VLAN ID (e.g. 3000-3099) for each VN
 - + Click Save > Add > Add > Deploy > Apply Now

Verifying the Border Node to Fusion Router Connection

- + Verifying the Border Node configuration
 - + Port on Border should be configured as a Layer 2 Trunk
 - + E.g. `show interface trunk`
 - + Border should have SVIs from Layer-3 Handoff IP Pool
 - + One SVI per-VN being advertised
 - + I.e. VRF-Lite
 - + Each SVI has a separate subnet from the Pool
 - + E.g. `show ip route vrf *`
 - + BGP on Border should have one peer per VRF/VN
 - + E.g. `show bgp ipv4 unicast vrf all summary`

Fusion Router Considerations

- + Fusion Router is outside the scope of SD-Access
 - + I.e. its config is not automated by DNA-C
- + Fusion Router should be configured as follows:
 - + One sub-interface per-VN, following the VLAN tags and subnets defined on Border
 - + One EBGP peering to Border per-VN, but all in the global (default) VRF
 - + Dynamic neighbors could be used to reduce the admin overhead
 - + E.g. listen for BGP from the entire Layer-3 Handoff IP Pool
 - + BGP filtering should be applied to not leak routes between VNs back towards Border
 - + Default desired behavior is for VNs to be isolated
 - + Fusion Router could leak routes between VNs on purpose if desired





Implementing Cisco SD-Access with DNA Center

SD-Access Host Onboarding



What is DNA Center SD-Access Host Onboarding?

- + Host onboarding combines all previous steps to finally build the Overlay
- + Host onboarding includes...
 - + Defining the target switch(es) and switch port(s)
 - + Binding the VN / VLAN / IP Pool to the port
 - + Choosing the host authentication template
 - + I.e. for 802.1x authentication
 - + Additional wireless options like SSID if using WLAN

Onboarding the SD-Access End Hosts

- + DNAC > Provision > Fabric Site > Host Onboarding > Port Assignment
 - + Choose Edge Switch on left
 - + Check interface(s) to configure on right
 - + Click Assign at top
 - + Choose Connected Device Type
 - + e.g. User Devices vs. AP
 - + Choose VN/VLAN previously created
 - + Optionally choose Security Group
 - + If doing ISE integration
 - + Optionally customize the Authentication Template
 - + Optionally add Description
 - + Click Update & Deploy





Implementing Cisco SD-Access with DNA Center

Verifying the SD-Access Fabric



How to we Verify the SD-Access Fabric?

- + For SD-Access we need to verify four main components
 - + Underlay routing between the Edge Switches
 - + I.e. IS-IS routing between the switches
 - + Control Plane registration from the Edge Switches to Control Plane Node(s)
 - + I.e. the LISP map-cache
 - + VXLAN Data Plane between Edge Switches
 - + E.g. PING between end hosts in the fabric
 - + External routing out of the fabric
 - + E.g. PING from end host in the fabric to the external WAN

Verifying the SD-Access Underlay

- + DNA Center programs IS-IS routing between switches to build the underlay
 - + **Border-1# show isis neighbors**
 - + **Edge-1# show isis neighbors**
 - + **Edge-1# show ip route isis**
 - + **Edge-1# show ip route [Edge-2 Loopback0]**
 - + **Edge-1# ping [Edge-2 Loopback0] source Loopback0**
 - + **Edge-1# traceroute [Edge-2 Loopback0] source Loopback0**

Verifying the SD-Access Overlay

- + DNAC should create a VLAN to VN/LISP Instance mapping
 - + **Edge# show run interface gi0/1**
 - + **Edge# show lisp vrf**
- + The LISP Instance number is global to the Fabric
 - + Edge should see the MAC/IP being learned on the access port
 - + **Edge# show mac address-table**
 - + **Edge# show ip route vrf [vrf]**
 - + **Edge# show lisp instance-id 1234 dynamic-eid detail**
 - + Control Node (also Border in our case) should see all endpoints for each instance
 - + **Border#show ip lisp map-cache instance-id 1234**
- + LISP supports both Layer 2 & Layer 3 Tunnelling over VXLAN
 - + Edge should see one LISP instance for Ethernet, and a separate instance for IP



Recommended Resources

- + [Cisco DevNet Sandbox](#)
- + [Cisco SD-Access Solution Design Guide \(CVD\)](#)
- + [Software-Defined Access for Distributed Campus Deployment Guide](#)
- + [Cisco Press - Cisco Software-Defined Access](#)

