

CCNA Day 62

Software-Defined Networking

6.0 Automation and Programmability

10%



6.1 Explain how automation impacts network management

6.2 Compare traditional networks with controller-based networking

6.3 Describe controller-based and software defined architectures (overlay, underlay, and fabric)

- 6.3.a Separation of control plane and data plane

- 6.3.b North-bound and south-bound APIs

6.4 Compare traditional campus device management with Cisco DNA Center enabled device management

6.5 Describe characteristics of REST-based APIs (CRUD, HTTP verbs, and data encoding)

6.6 Recognize the capabilities of configuration management mechanisms Puppet, Chef, and Ansible

6.7 Interpret JSON encoded data

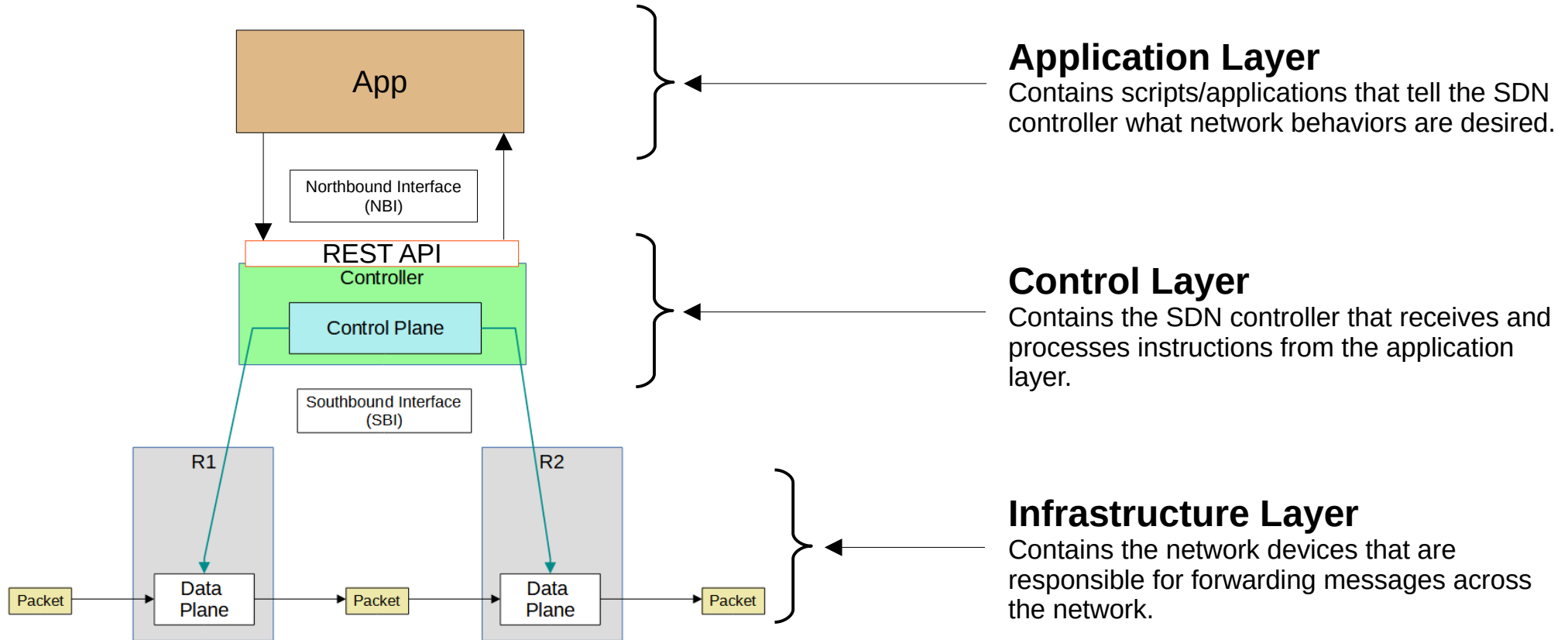


Things we'll cover

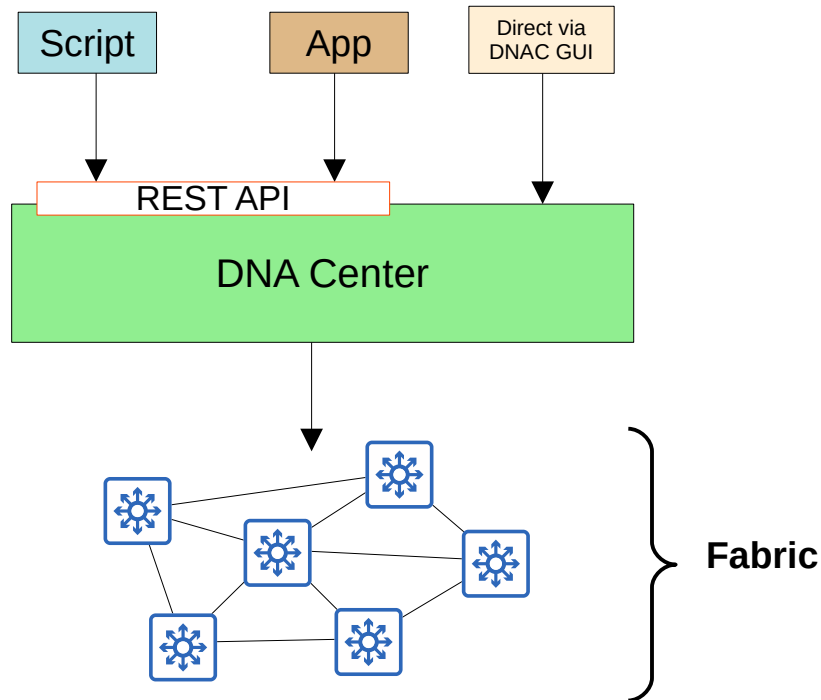
- SDN Review
- Cisco SD-Access
- Cisco DNA Center
- DNA Center network management vs traditional

- **Software-Defined Networking (SDN)** is an approach to networking that centralizes the control plane into an application called a *controller*.
- Traditional control planes use a distributed architecture.
- An SDN controller centralizes control plane functions like calculating routes.
- The controller can interact programmatically with the network devices using APIs.
- The **SBI** is used for communications between the controller and the network devices it controls.
- The **NBI** is what allows us to interact with the controller with our scripts and applications.

SDN Architecture

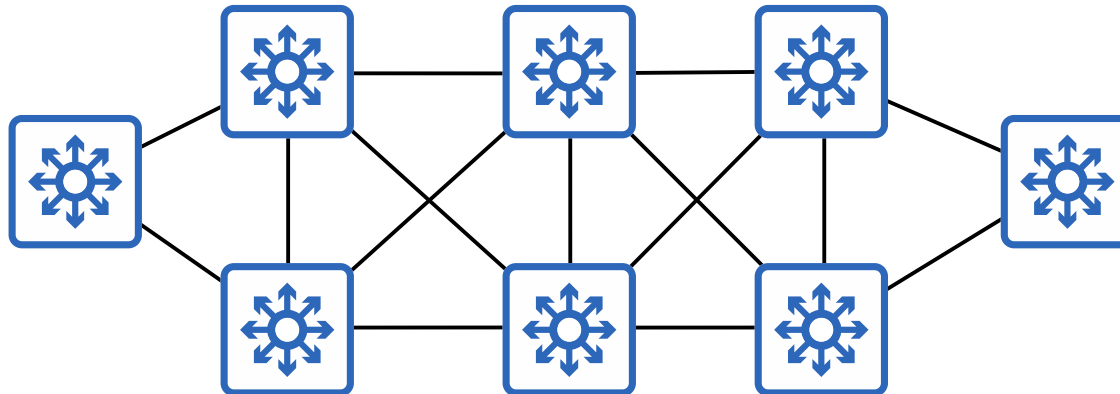


- Cisco **SD-Access** is Cisco's SDN solution for automating campus LANs.
 - ACI (Application Centric Infrastructure) is their SDN solution for automating data center networks.
 - SD-WAN is their SDN solution for automating WANs.
- Cisco **DNA (Digital Network Architecture) Center** is the controller at the center of SD-Access.



- The **underlay** is the underlying physical network of devices and connections (including wired and wireless) which provide IP connectivity (ie. using IS-IS).
→ Multilayer switches and their connections.
- The **overlay** is the virtual network built on top of the physical underlay network.
→ SD-Access uses VXLAN (Virtual Extensible LAN) to build tunnels.
- The **fabric** is the combination of the overlay and underlay; the physical and virtual network as a whole.

Underlay

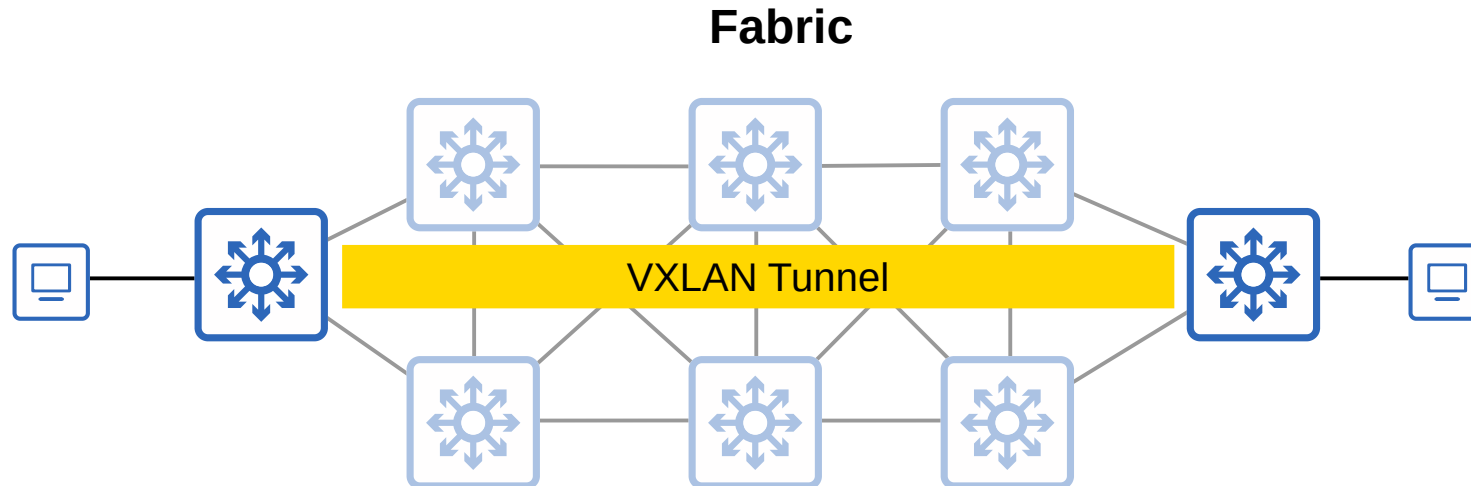


- The **underlay** is the underlying physical network of devices and connections (including wired and wireless) which provide IP connectivity (ie. using IS-IS).
→ Multilayer switches and their connections.
- The **overlay** is the virtual network built on top of the physical underlay network.
→ SD-Access uses VXLAN (Virtual Extensible LAN) to build tunnels.
- The **fabric** is the combination of the overlay and underlay; the physical and virtual network as a whole.

Overlay



- The **underlay** is the underlying physical network of devices and connections (including wired and wireless) which provide IP connectivity (ie. using IS-IS).
→ Multilayer switches and their connections.
- The **overlay** is the virtual network built on top of the physical underlay network.
→ SD-Access uses VXLAN (Virtual Extensible LAN) to build tunnels.
- The **fabric** is the combination of the overlay and underlay; the physical and virtual network as a whole.

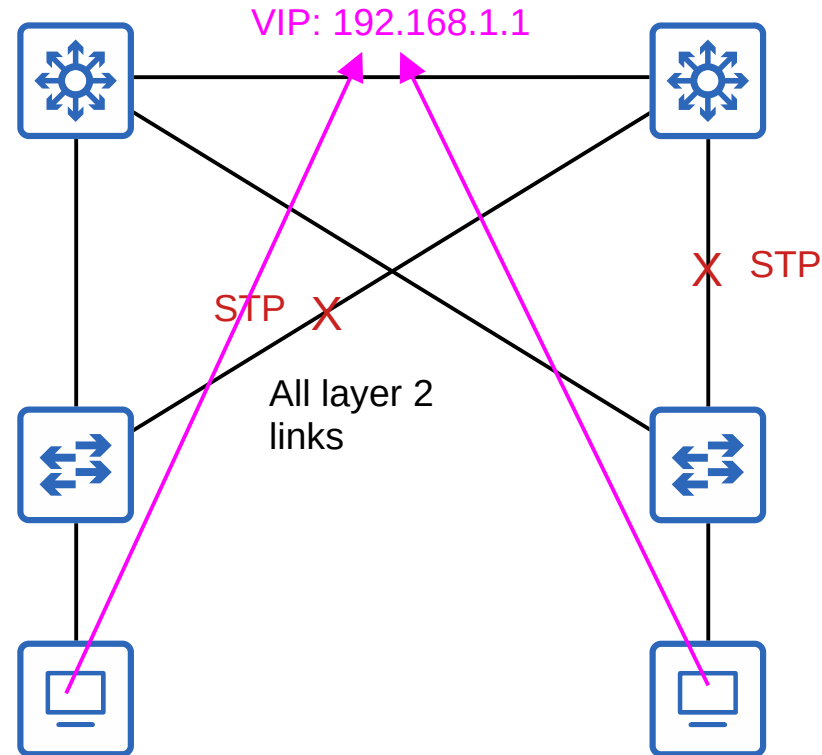


SD-Access Underlay

- The underlay's purpose is to support the VXLAN tunnels of the overlay.
- There are three different roles for switches in SD-Access:
 - **Edge nodes**: Connect to end hosts
 - **Border nodes**: Connect to devices outside of the SD-Access domain, ie. WAN routers.
 - **Control nodes**: Use LISP (Locator ID Separation Protocol) to perform various control plane functions.
- You can add SD-Access on top of an existing network (*brownfield deployment*) if your network hardware and software supports it.
 - Google 'Cisco SD-Access compatibility matrix' if you're curious.
 - In this case DNA Center won't configure the underlay.
- A new deployment (*greenfield deployment*) will be configured by DNA Center to use the optimal SD-Access underlay:
 - All switches are Layer 3 and use IS-IS as their routing protocol.
 - All links between switches are routed ports. This means STP is not needed.
 - Edge nodes (access switches) act as the default gateway of end hosts (*routed access layer*).

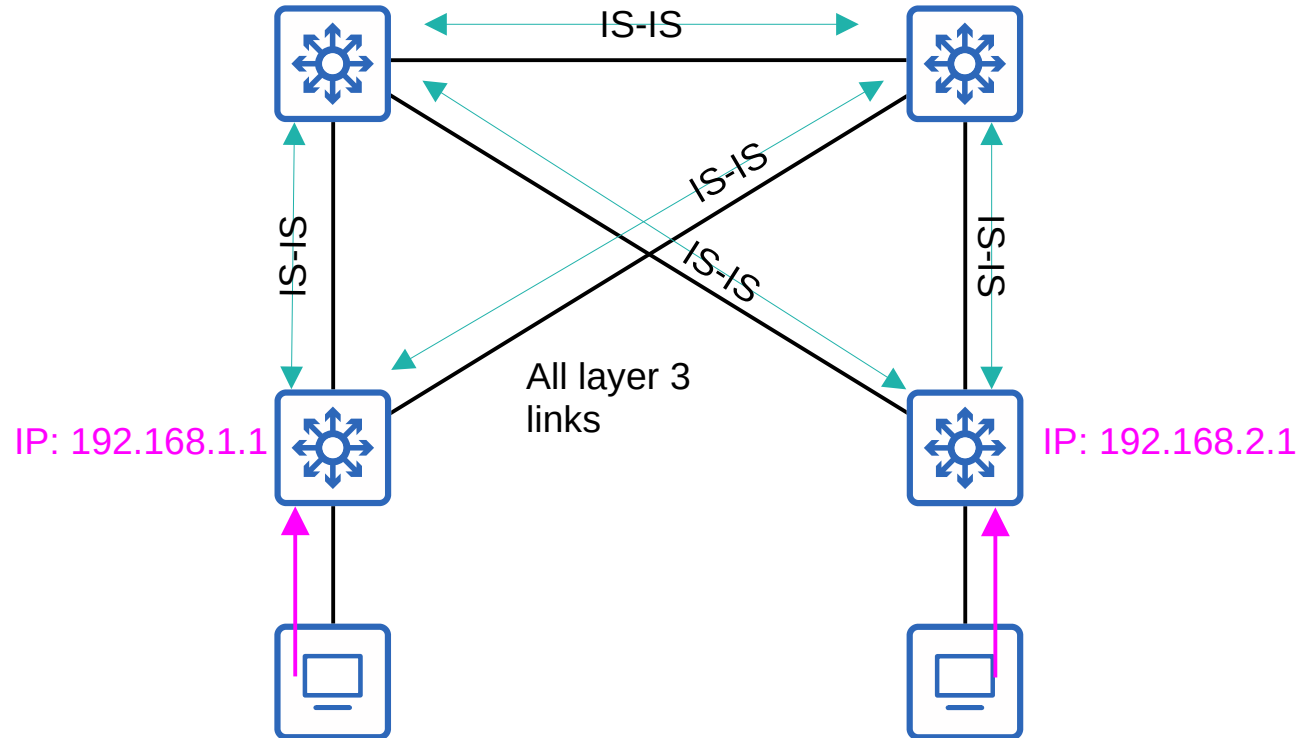
SD-Access Underlay

Traditional LAN



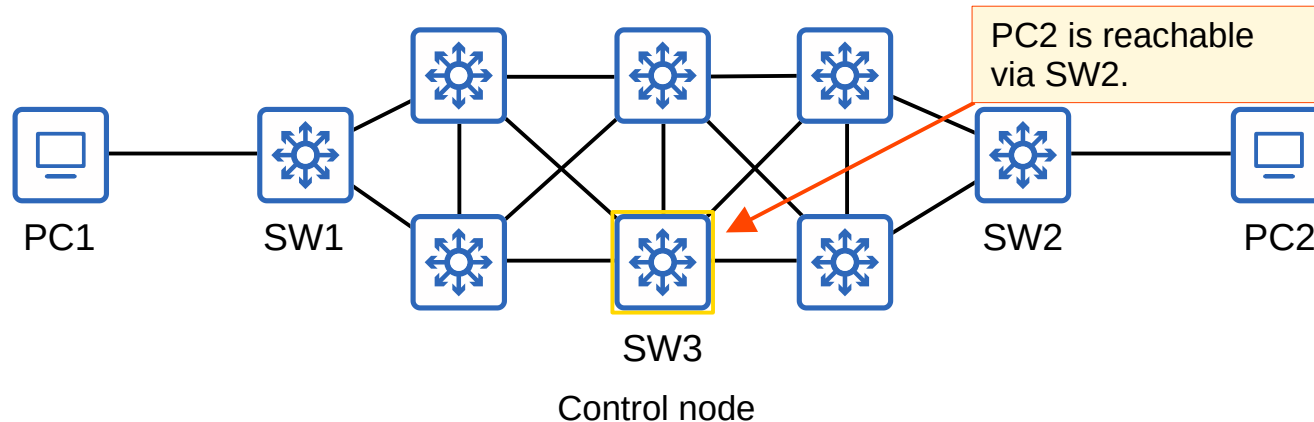
SD-Access Underlay

SD-Access Underlay



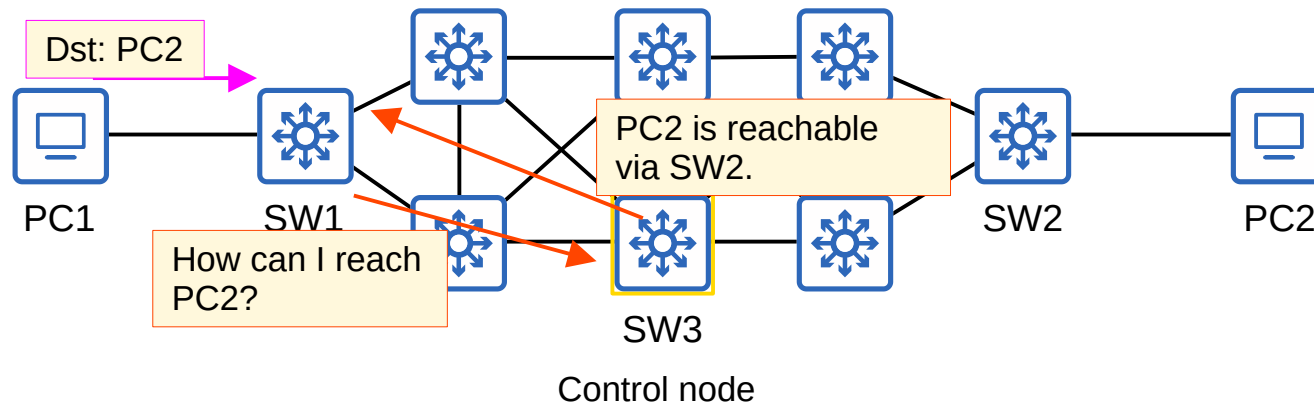
SD-Access Overlay

- LISP provides the control plane of SD-Access.
 - A list of mappings of EIDs (endpoint identifiers) to RLOCs (routing locators) is kept.
 - EIDs identify end hosts connected to edge switches, and RLOCs identify the edge switch which can be used to reach the end host.
 - There is a LOT more detail to cover about LISP, but I think you can see how it differs from the traditional control plane.
- Cisco TrustSec (CTS) provides policy control (QoS, security policy, etc).
- VXLAN provides the data plane of SD-Access.



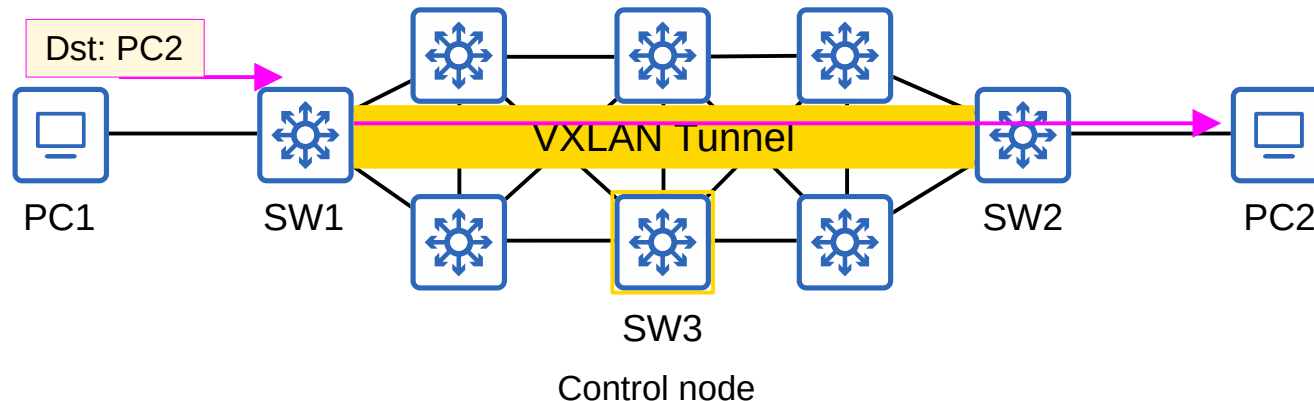
SD-Access Overlay

- LISP provides the control plane of SD-Access.
 - A list of mappings of EIDs (endpoint identifiers) to RLOCs (routing locators) is kept.
 - EIDs identify end hosts connected to edge switches, and RLOCs identify the edge switch which can be used to reach the end host.
 - There is a LOT more detail to cover about LISP, but I think you can see how it differs from the traditional control plane.
- Cisco TrustSec (CTS) provides policy control (QoS, security policy, etc).
- VXLAN provides the data plane of SD-Access.



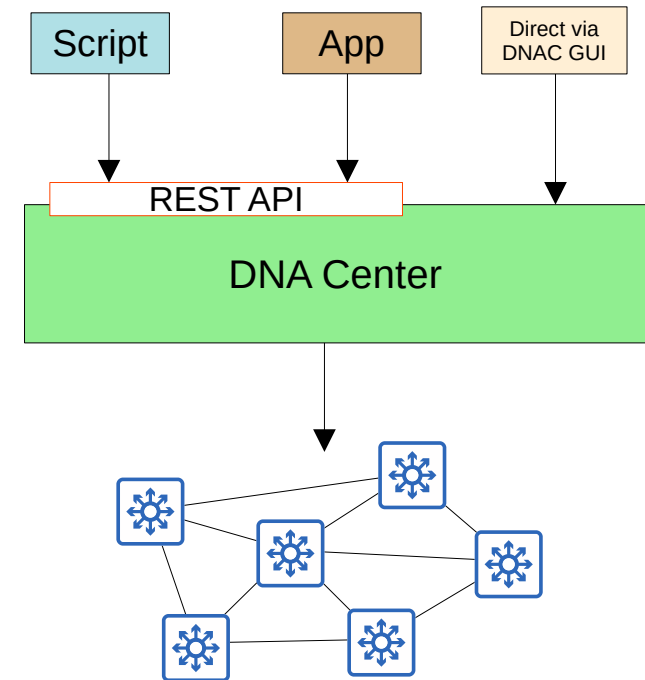
SD-Access Overlay

- LISP provides the control plane of SD-Access.
 - A list of mappings of EIDs (endpoint identifiers) to RLOCs (routing locators) is kept.
 - EIDs identify end hosts connected to edge switches, and RLOCs identify the edge switch which can be used to reach the end host.
 - There is a LOT more detail to cover about LISP, but I think you can see how it differs from the traditional control plane.
- Cisco TrustSec (CTS) provides policy control (QoS, security policy, etc).
- VXLAN provides the data plane of SD-Access.



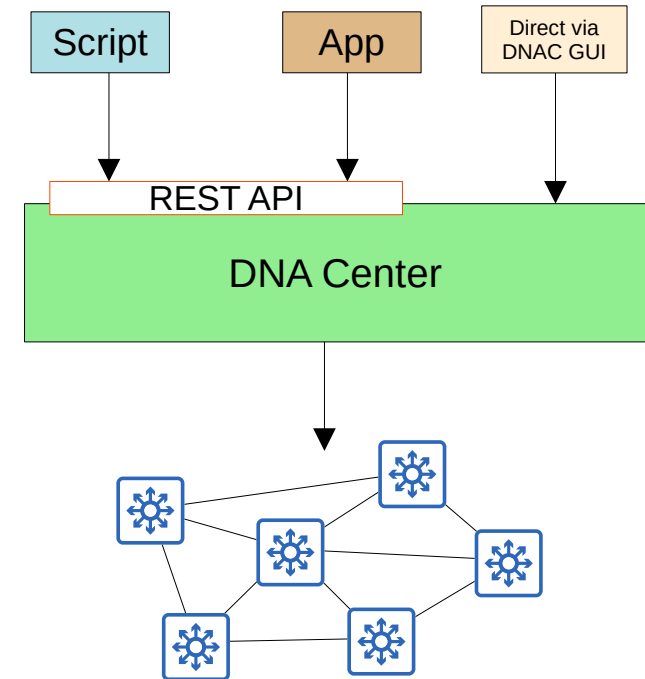
Cisco DNA Center

- Cisco DNA Center has two main roles:
 - The SDN controller in SD-Access
 - A network manager in a traditional network (non-SD-Access)
- DNA Center is an application installed on Cisco UCS server hardware.
- It has a REST API which can be used to interact with DNA center.
- The SBI supports protocols such as NETCONF and RESTCONF (as well as traditional protocols like Telnet, SSH, SNMP).
- DNA Center enables *Intent-Based Networking* (IBN).
 - More buzzwords! Yay!
 - The goal is to allow the engineer to communicate their intent for network behavior to DNA Center, and then DNA Center will take care of the details of the actual configurations and policies on devices.



Cisco DNA Center

- Traditional security policies using ACLs can become VERY cumbersome.
 - ACLs can have **thousands** of entries.
 - The intent of entries is forgotten with time and as engineers leave and new engineers take over.
 - Configuring and applying the ACLs correctly across a network is cumbersome and leaves room for error.
- DNA Center allows the engineer to specify the intent of the policy (this group of users can't communicate with this group, this group can access this server but not that server, etc.), and DNA Center will take care of the exact details of implementing the policy.



Policies (0) ⇄ Exit full screen

 Filter Refresh

■ Permit ■ Deny ■ Custom □ Default

Source

Auditors

BYOD

Contractors

Developers

Development_Se...

Employees

Extranet

Guests

Destination

Auditors

BYOD

Contractors

Developers

Development
Employees

Extranet

Guests

Intranet

Network_Servi...
PCI_S...

PCI_Servers

Point_of_Sale
Prodi:

Production_Ser...

Production_Us...
Quaran...

Quarantined_S...

TrustSec_Servers

Unknown

--	--

Cisco DNA Center

Cisco DNA Center

 Design >

 Policy >

 Provision >

 Assurance >

 Workflows >

 Tools >


 Platform >

 Activities >

 Reports >

 System >

 Explore >

 devnetuser <<

Network Hierarchy

Network Settings

Image Repository

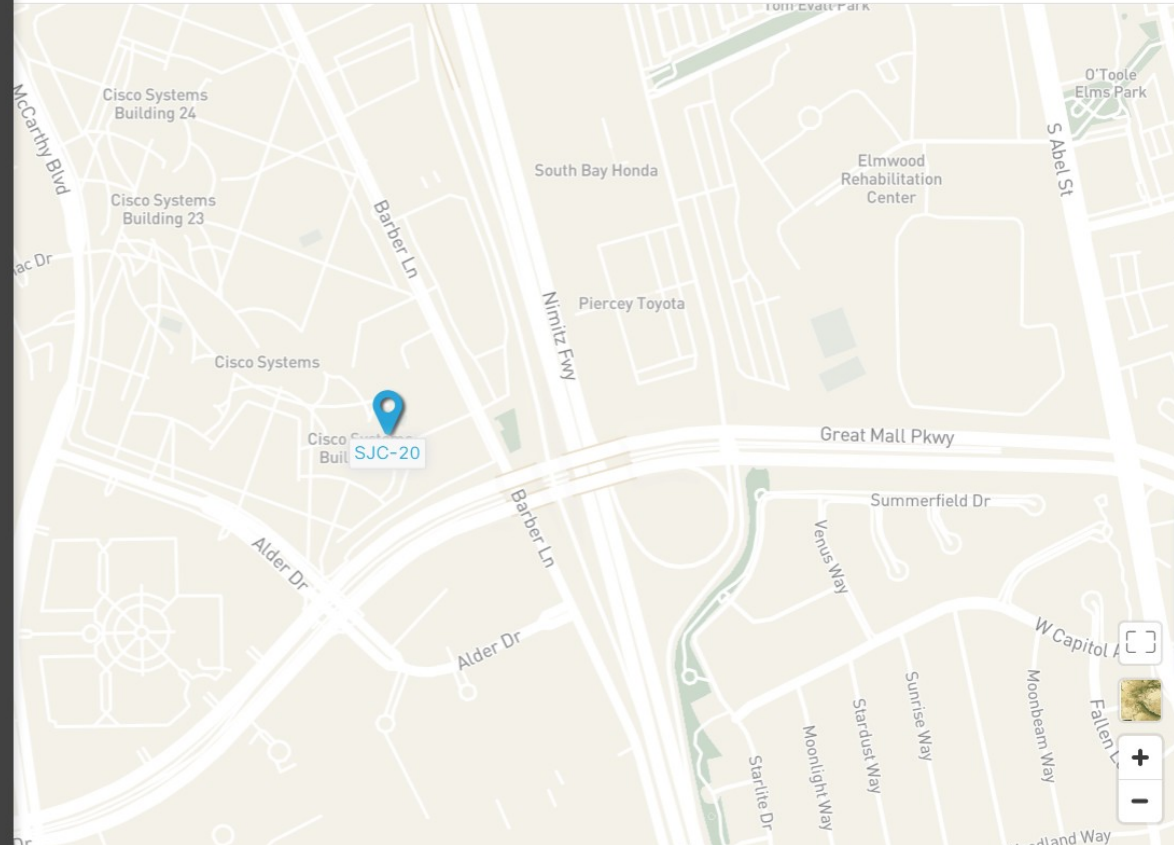
Network Profiles

Authentication Template

Design • Network Hierarchy



Find Buildings



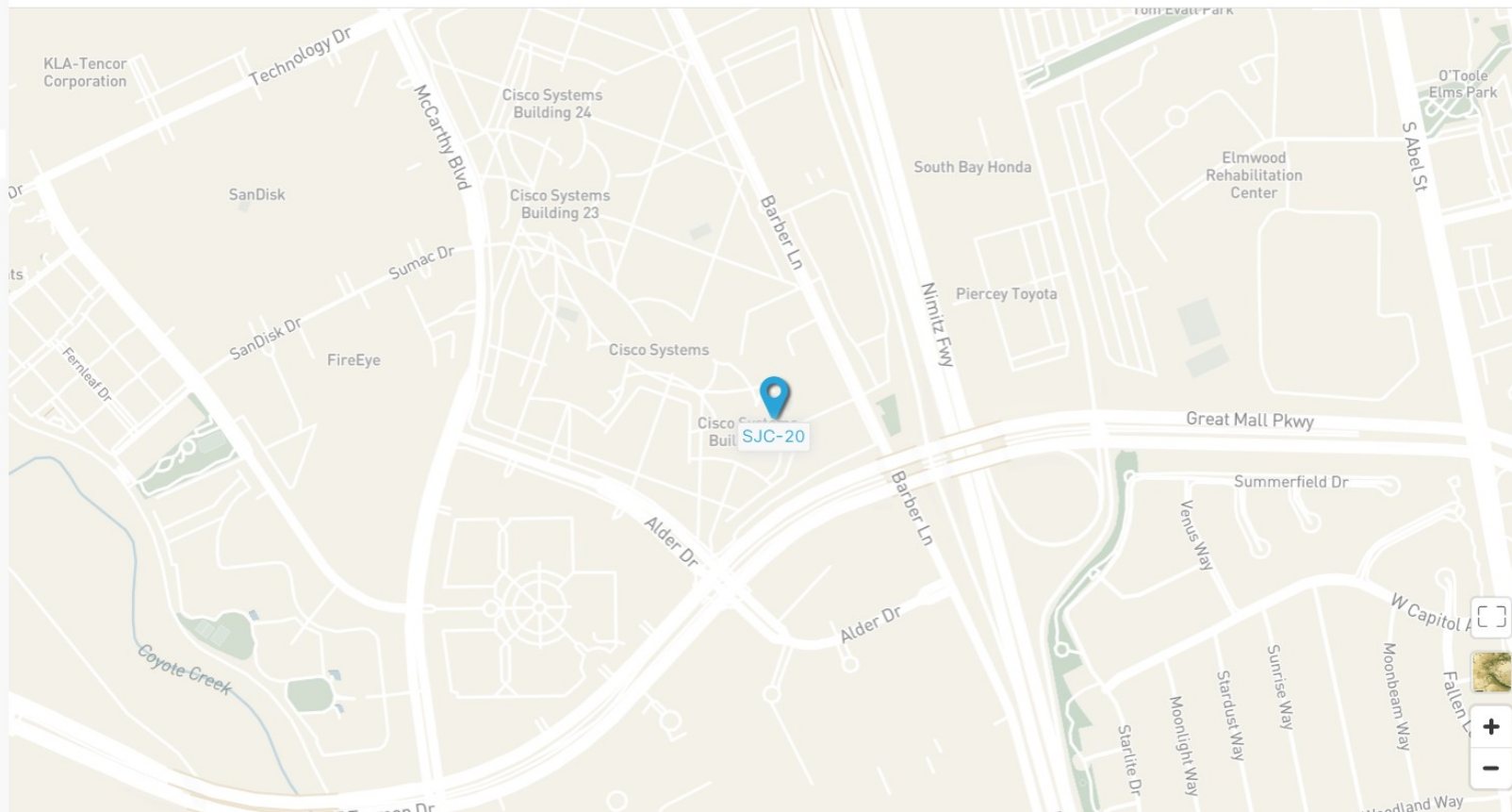
🔍 Find Hierarchy

▼ 🌐 Global

▼ 🌐 San Jose

🏢 SJC-20

🔍 Find Buildings



Cisco DNA Center

 Design >

 Policy >

 Provision >

 Assurance >

 Workflows

 Tools >


 Platform >

 Activities

 Reports

 System >

 Explore

 devnetuser <<

AI Endpoint Analytics

Group-Based Access Control

IP Based Access Control

Application

Traffic Copy

Virtual Network

Group-Based Access Control



Integrate ISE (2.4.0.357 Patch(es) 7 or 2.6.0.156 Patch(es) 1 or above) to Cisco DNA Center in You have to policies in ISE.

Default: [Permit IP](#)



Production_Ser...
Production_Us...
Quarantined_S...
Test_Servers
TrustSec_Devic...
Unknown



Expand Minimap 



Identity Services Engine (ISE) has not been integrated, or is currently not available. Integrate ISE (2.4.0.357 Patch(es) 7 or 2.6.0.156 Patch(es) 1 or above) to Cisco DNA Center in You have to come back and enable synchronization so that Cisco DNA Center could distribute policies in ISE.

Policies Scalable Groups Access Contracts Analytics

Policies (0)  Enter full screen

Default: Permit IP



Filter



Refresh

☒ Permit ☐ Deny ☐ Custom ☐ Default


Source	Destination															
	Auditors	BYOD	Contractors	Developers	Development_S...	Employees	Extranet	Guests	Intranet	Network_Servi...	PCI_Servers	Point_of_Sale...	Production_Ser...	Production_Us...	Quarantined_S...	Test_Servers
Auditors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
BYOD	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Contractors	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Developers	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>


Expand Minimap 

Cisco DNA Center

 Design >

 Policy >

 Provision >

 Assurance >

 Workflows >

 Tools >

 Platform >

 Activities >

 Reports >

 System >

 Explore >

NETWORK DEVICES

[Inventory](#)

Plug and Play

Fabric

SERVICES

Service Catalog

Cisco User Defined Network

Application Visibility


Stealthwatch Security Analytics

App Hosting for Switches

IoT Services

Umbrella

Cloud

 devnetuser

<<

on • Network Devices • Inventory

Preview New Page



Devices that don't have netconf, configure the netconf port in the Inventory credentials for these devices and Update Push.







 Global > San Jose > SJC-20



[Take a Tour](#)

As of: 7:28 PM

 Refresh

Device Family	Reachability 	Manageability 	Compliance 	Health Score	Site	
Switches and Hubs (WLC Capable)	 Reachable	 Managed	 Non-Compliant	10	.../San Jose/SJC-20	

Showing 1 of 1

⚠ To provision subscriptions on [devices that don't have netconf](#), configure the netconf port in the Inventory credentials for these devices and Update Telemetry Settings with Force Config Push.

Global > Unassigned Devices

DEVICES (3)

FOCUS: Inventory

Filter

Tag Device

Actions

Take a Tour

As of: 7:55 PM

Refresh

<input type="checkbox"/>	Device Name	IP Address	Device Family	Reachability	Manageability	Compliance	Health Score	Site	MAC Address
<input type="checkbox"/>	c3504.abc.inc	10.10.20.51	Wireless Controller	✓ Reachable	✓ Managed	✓ Compliant	NA	Assign	ac:4a:56:6
<input type="checkbox"/>	leaf2.abc.inc	10.10.20.82	Switches and Hubs (WLC Capable)	✓ Reachable	✓ Managed	✗ Non-Compliant	8	Assign	68:ca:e4:3
<input type="checkbox"/>	spine1.abc.inc	10.10.20.80	Switches and Hubs (WLC Capable)	✓ Reachable	✓ Managed	✗ Non-Compliant	8	Assign	70:1f:53:7

Show 25 entries

Showing 3 of 3

[All Devices](#) > [leaf2.abc.inc](#)

🔄 leaf2.abc.inc

🔧 [Run Commands](#)

📄 [View 360](#)

Last updated: 7:59 PM

🔄 [Refresh](#)

✅ Reachable | ✅ Managed | IP Address: 10.10.20.82 | Device Model: Cisco Catalyst 9300 Switch | Role: DISTRIBUTION | Uptime: 35 days 9 hrs 8 mins | Site: -

DETAILS

Interfaces



Ethernet Ports

VLANs

Hardware & Software

Configuration

Power

Fans

User Defined Fields

Config Drift

SECURITY

Advisories

Compliance Summary

No events detected to trigger compliance check

✅ **Startup vs Running Configuration** ⓘ
Compliance last run on: Dec 5th, 2021, 08:00:00 AM
149 days since in sync
Lines added: 0
Lines removed: 0
Lines modified: 0

❌ **Software Image** ⓘ
Non-Compliant since Oct 23rd, 2021, 05:22:01 AM
Compliance last run on: Dec 5th, 2021, 08:00:00 AM
17.03.03 Golden Image Version
Version: **16.11.1c**

❌ **Critical Security Advisories** ⓘ
Non-Compliant since Jul 15th, 2021, 09:00:44 AM
Compliance last run on: Dec 5th, 2021, 08:00:02 AM


4

Cisco DNA Center

 Design >

 Policy >

 Provision >

 Assurance >

 Workflows

 Tools >

 Platform >

 Activities

 Reports

 System >

 Explore

DASHBOARDS

Health

Issues

Sensors

Wi-Fi 6

Rogue and aWIPS

PoE

Dashboard Library

AI NETWORK ANALYTICS

Network Insights

Network Heatmap

Peer Comparison

Network Comparison

Baselines

MANAGE


Issue Settings

Health Score Settings

Sensors

Assurance • Dashboards • Health



 devnetuser



Overall **Network** Client Application

📍 Global ▾ ⌚ 24 Hours ▾ 🌐 All Domains ▾

Dec 4, 2021 7:30 PM - Dec 5, 2021 7:30 PM



Actions ▾

LATEST TREND

Network Devices

75% ⓘ

Healthy Network Devices

TOTAL DEVICES 4

Good Health 3

Fair Health --

Poor Health --

No Health Data 1

Router (0)

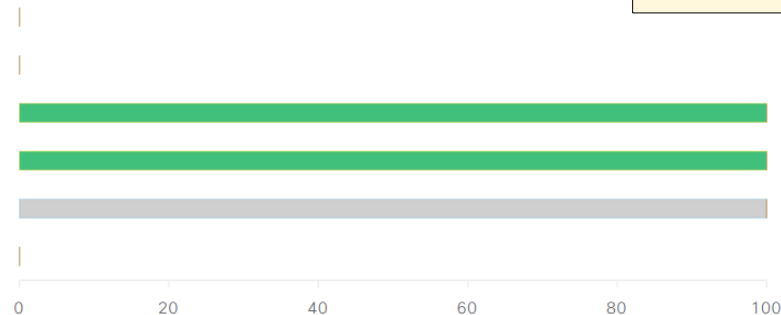
Core (0)

Distribution (1)

Access (2)

Wireless Controller (1)

Access Point (0)



sandboxdnac.cisco.com

User: devnetuser

Password: Cisco123!

DNA Center vs Traditional Network Management

- Traditional network management:
 - Devices are configured one-by-one via SSH or console connection.
 - Devices are manually configured via console connection before being deployed.
 - Configurations and policies are managed per-device. (distributed)
 - New network deployments can take a long time due to the manual labor required.
 - Errors and failures are more likely due to increased manual effort.
- DNA Center-based network management:
 - Devices are centrally managed and monitored from the DNA Center GUI or other applications using its REST API.
 - The administrator communicates their intended network behavior to DNA Center, which changes those intentions into configurations on the managed network devices.
 - Configurations and policies are centrally managed.
 - Software versions are also centrally managed. DNA Center can monitor cloud servers for new versions and then update the managed devices.
 - New network deployments are much quicker. New devices can automatically receive their configurations from DNA Center without manual configuration.

Things we covered

- SDN Review
- Cisco SD-Access
- Cisco DNA Center
- DNA Center network management vs traditional

Which of the following terms describes the network of devices and physical connections?

- a) Underlay
- b) Fabric
- c) Overlay
- d) Tunnel

In which of the following layers would you expect to find scripts that interact with the controller?

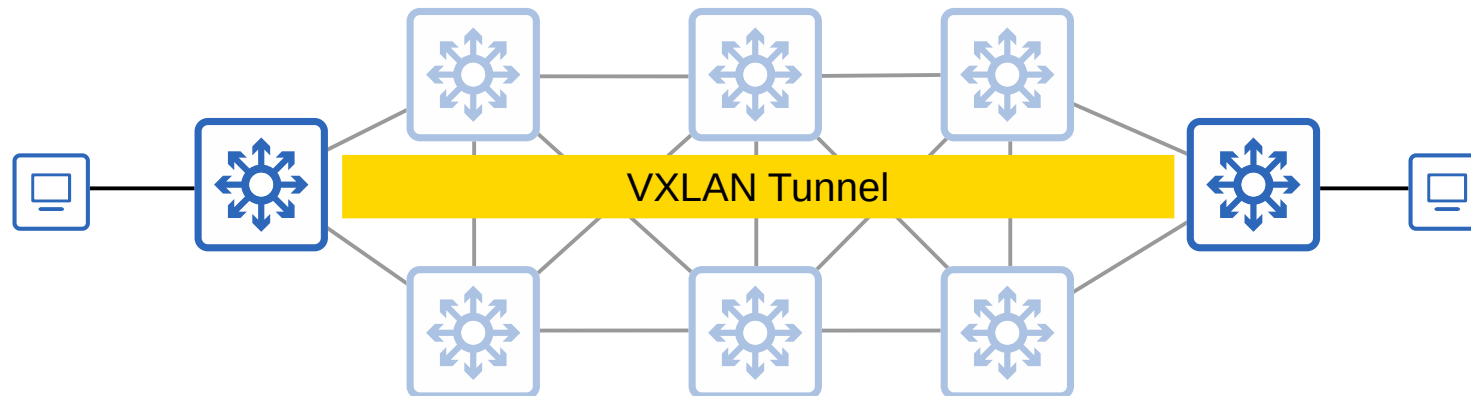
- a) Infrastructure
- b) Application
- c) REST
- d) Control

Which of the following is a characteristic of an optimal SD-Access underlay network as configured by DNA-Center?

- a) All switch are Layer 3 and use OSPF as their routing protocol.
- b) All links between switches are Layer 3.
- c) An FHRP is used to provide a redundant default gateway for end hosts.
- d) All links between switches run Cisco proprietary Rapid-PVST+.

Which protocol is used to create virtual tunnels in the SD-Access overlay?

- a) LISP
- b) IPsec
- c) GRE
- d) VXLAN



Which of the following are valid switch roles in Cisco SD-Access? (select three)

- a) Control node
- b) Management node
- c) Border node
- d) Edge node