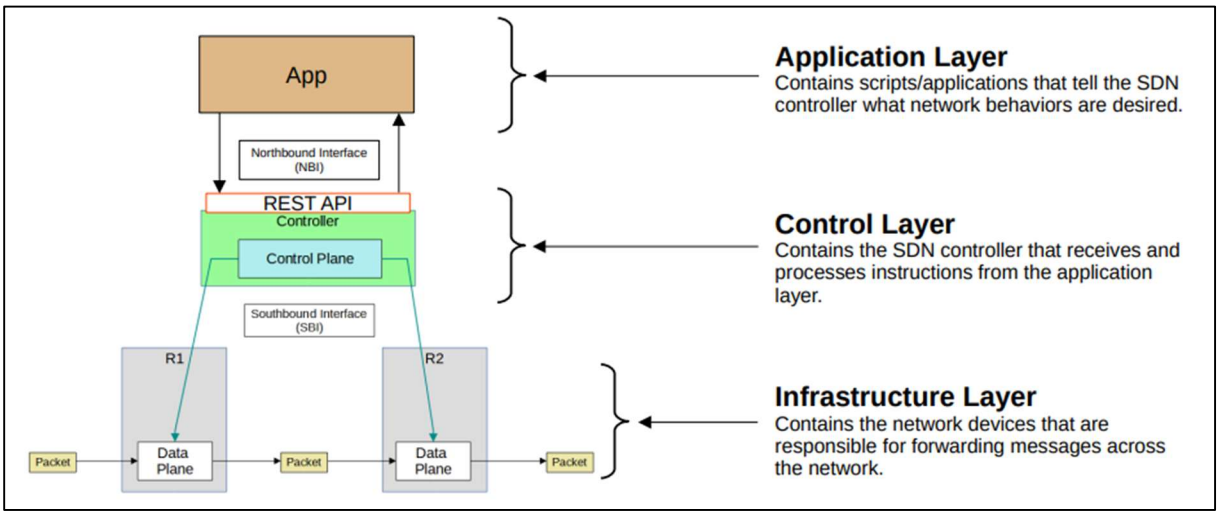
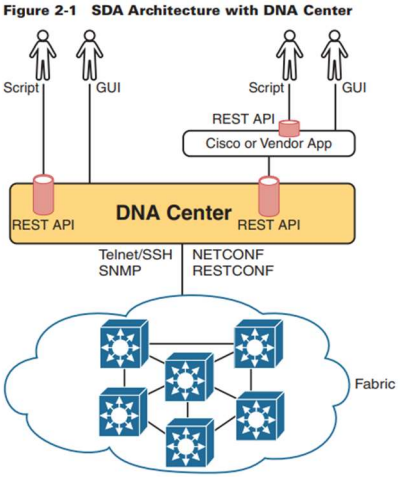
SDN Architecture - Layers

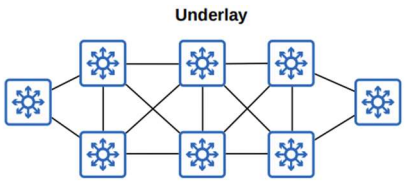


Cisco Software-Defined Access (SDA-Access)

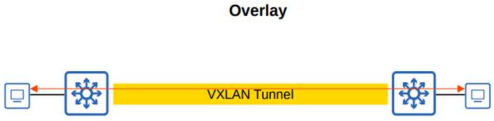
- Cisco SD-Access is Cisco's SDN solution for automating campus LANs.
  - ACI (Application Centric Infrastructure) is their SDN solution for automating data center networks.
  - SD-WAN is their SDN solution for automating WANs.
- **Cisco DNA (Digital Network Architecture) Center** is the controller at the center of SD-Access.
- SDA uses a controller and application programming interfaces (APIs) to communicate via southbound interfaces (SBIs) with the network infrastructure, as shown in Figure 2-1. Cisco DNA Center is an example of a controller. SBIs include Telnet/SSH, SNMP, NETCONF, and RESTCONF.



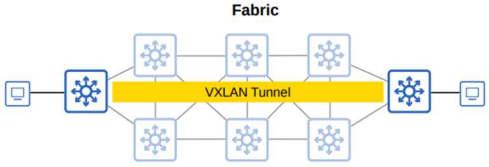
- The **underlay** is the underlying physical network of devices and connections (including wired and wireless) which provide IP connectivity (ie. using IS-IS).
  - Multilayer switches and their connections.
- The underlay's purpose is to support the VXLAN tunnels of the overlay.
- There are three different 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.



- The **overlay** is the virtual network built on top of the physical underlay network.
  - SD-Access uses VXLAN (Virtual Extensible LAN) to build tunnels

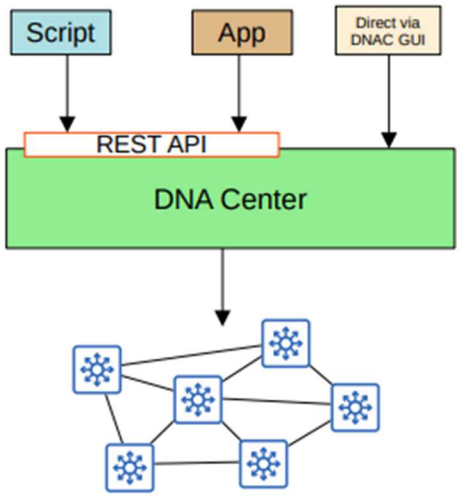


- The **fabric** is the combination of the *overlay* and *underlay*; the physical and virtual network as a whole.



SD-Access could be added on top of existing network (*brownfield deployment*) or a brand-new network (*greenfield deployment*).

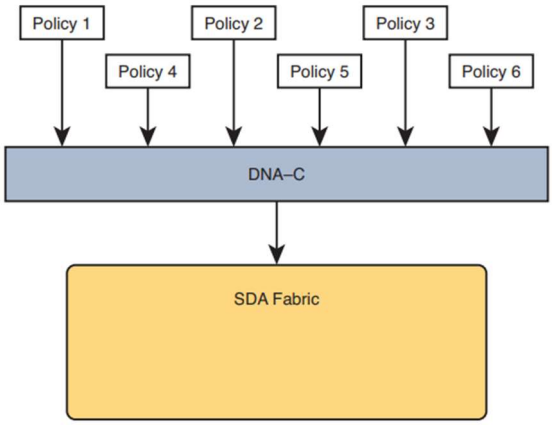
CISCO DNA CENTER



- 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.

- 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.

Figure 2-5 Six Policies Implemented by DNA Center



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.