Network Automation

- Automation can be used for:
- Device configuration
- Initial device provisioning
- Software version control
- Collecting statistics from devices
- Compliance verification
- Reports
- Troubleshooting

Which Automation Method to Use

- There are multiple methods that can be used to automate network management – Python scripts, NETCONF, RESTCONF, Ansible, Puppet, SDN, Cisco DNA Center etc.
- Not all methods are supported by all devices
- You should choose the method(s) which is most suitable for your environment and skills

Data Serialization

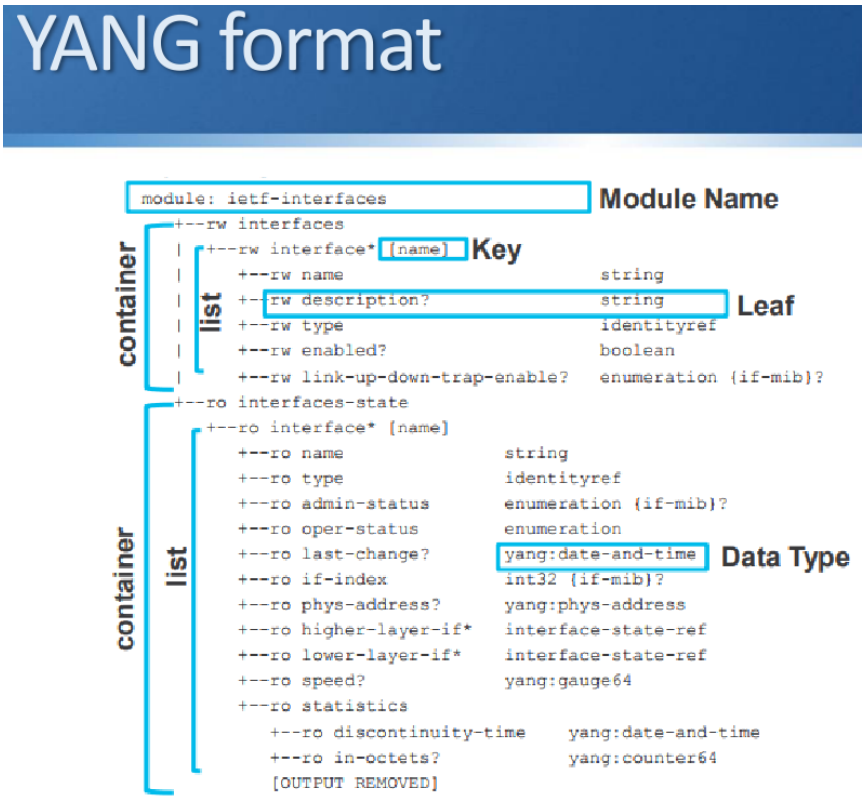
- Data serialization is the process of converting structured data to a standardized format that allows sharing or storage of the data in a form that allows recovery of its original structure
- It allows transfer of the data between different systems, applications and programming languages
- XML, JSON and YAML are human and machine readable, plain text data encoding formats

API Application Programming Interfaces

- An API is a way for a computer program to communicate directly with another computer program
- It is typically used to perform CRUD operations
- The two main types of APIs for web services (can run over the Internet, typically use HTTP) are SOAP and REST
- NETCONF and RESTCONF are APIs specifically designed to work with network devices

YANG Yet Another Next Generation

- YANG (IETF, 2010) is a data modelling language which provides a standardized way to represent the operational and configuration data of a network device.
- It can be used both internally and when packaged for transmission.



Network Management Transport

- The configuration and operational status of a network device's components and services can be remotely read or written to.
- NETCONF, RESTCONF and gRPC are APIs which describe the protocols and methods for transport of network management data.

Configuration Management Tools

- Configuration management systems are designed to make controlling large numbers of devices easy for administrators and operations teams.
- They allow you to control many different systems in an automated way from one central location.

- Popular options (open source and free, with paid for Enterprise editions available):
    - Ansible
    - Puppet
    - Chef

SDN

Router and Switch Planes

- Data (Forwarding) Plane: Traffic which is forwarded through the device.
- Control Plane: Makes decisions about how to forward traffic. Control plane packets such as routing protocol or spanning tree updates are destined to or locally originated on the device itself.
- Management Plane: The device is configured and monitored in the management plane. For example at the CLI through Telnet or SSH, via a GUI using HTTPS, or via SNMP or an API (Application Programming Interface).

SDN - Data and Control Plane Separation

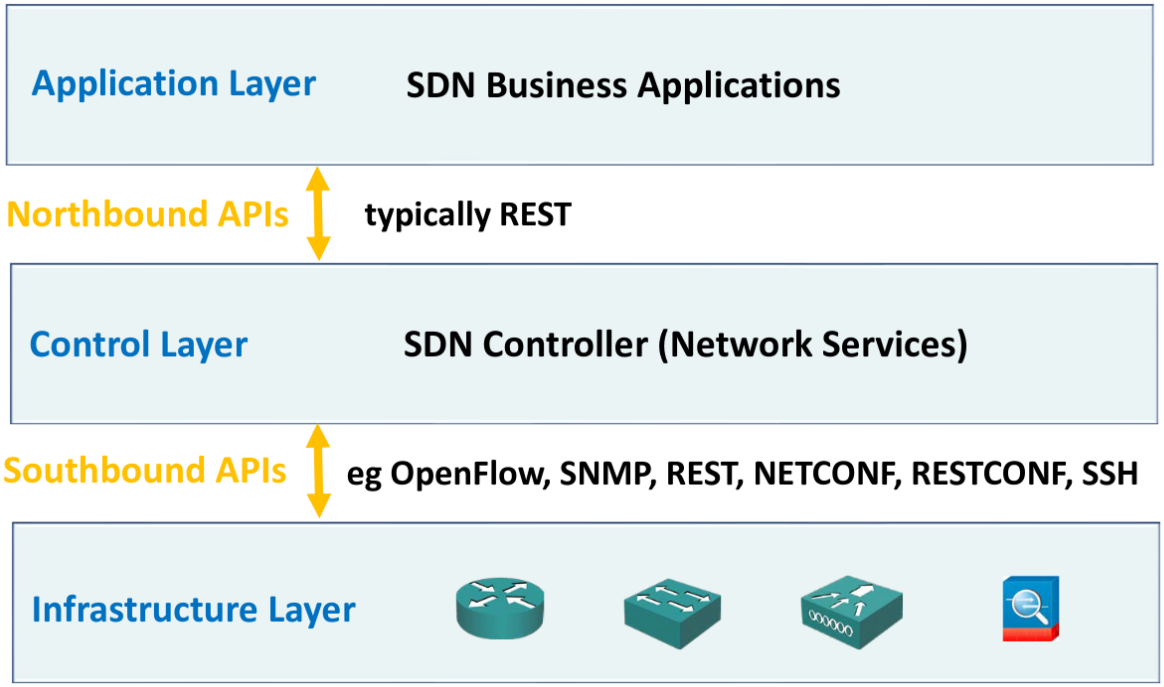
- Network infrastructure devices are responsible for their own individual control and data planes in a traditional environment.
- Software Defined Networking decouples the data and control planes.
- The network infrastructure devices are still responsible for forwarding traffic, but the control plane moves to a centralised SDN controller.
- Rules for packet handling are sent to the network infrastructure devices from the controller.
- The network infrastructure devices query the controller for guidance as needed, and provide it with information about traffic they are handling.

Pure vs Hybrid SDN

Pure SDN vs Hybrid SDN

- With a pure SDN the control plane runs purely on an SDN controller, and the data plane runs purely on the network devices.
- With a hybrid SDN the majority of the control plane intelligence is provided by an SDN controller, but the network devices retain some control plane intelligence as well as the data plane operations.
- Most implementations use a hybrid SDN.

SDN Architecture



Cisco SDN Controllers: APIC

- APIC (Application Policy Infrastructure Controller)
- The main component of the Cisco ACI (Application Centric Infrastructure) solution
- Designed to manage data center environments with Nexus switches

- (DNA: Digital Network Architecture)
- Designed to manage enterprise environments – campus, branch and WAN
- You can think of it as an upgrade to the APIC-EM (Application Policy Infrastructure Controller – Enterprise Module)

Cisco DNA Digital Network Architecture

- "Cisco DNA enables you to streamline operations and facilitate IT and business innovation.
- Intent-based networking (IBN) built on Cisco DNA takes a software-delivered approach to automating and assuring services across your WAN and your campus and branch networks."

3 of the main building blocks of Cisco DNA and Software Defined Architecture are:

- DNA Center
- SD-Access
- SD-WAN

DNA Center

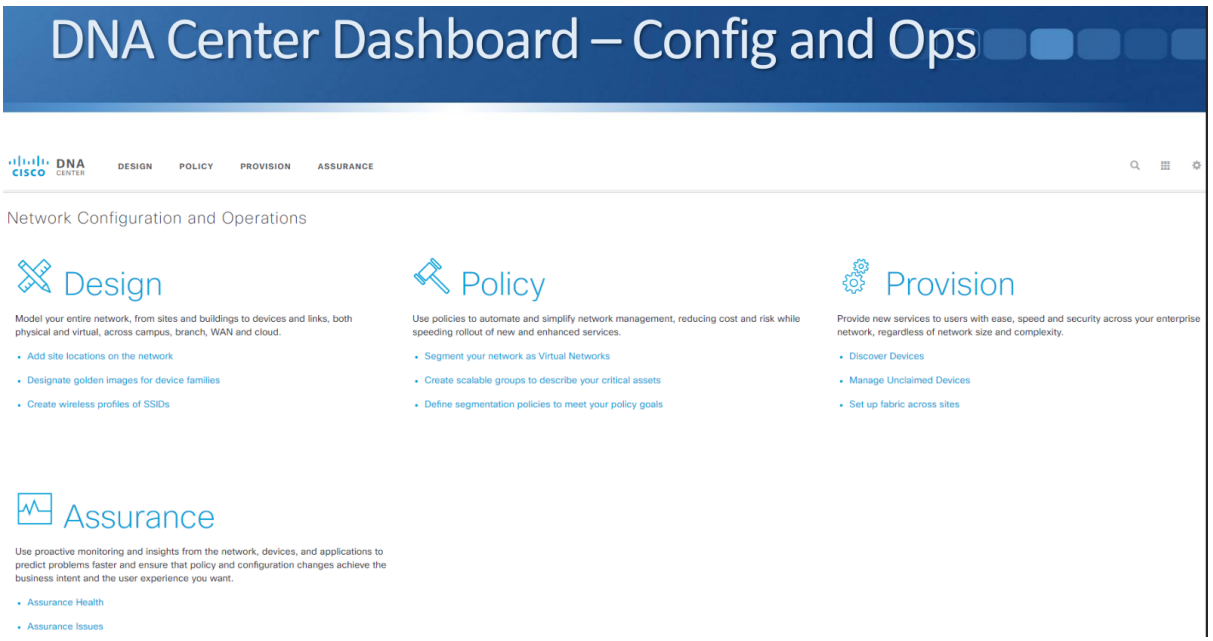
- DNA Center is a Cisco SDN controller which is designed to manage enterprise environments – campus, branch and WAN
- (As opposed to the APIC which manages data center environments with Nexus switches)
- You can think of DNA Center as an upgrade to the APIC-EM (Application Policy Infrastructure Controller – Enterprise Module

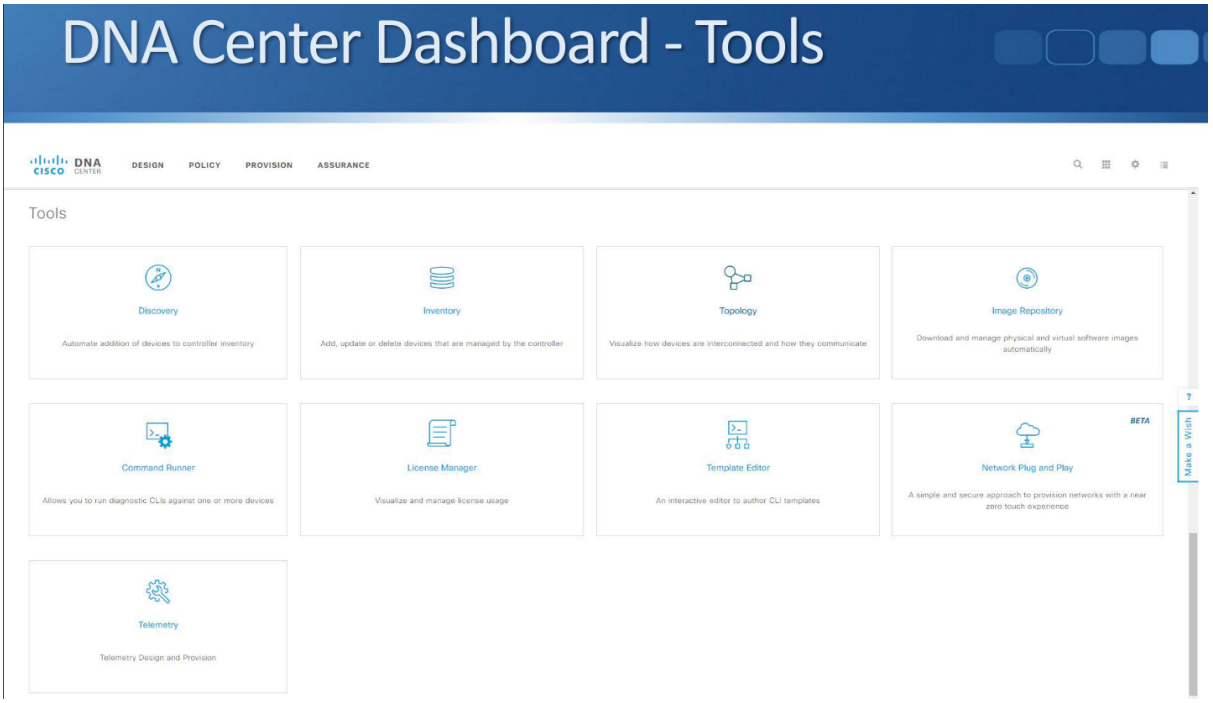
IBN Intent Based Networking (IBN)

- Intent Based Networking transforms a traditional manual network into a controller led network that translates the business needs into policies that can be automated and applied consistently across the network.

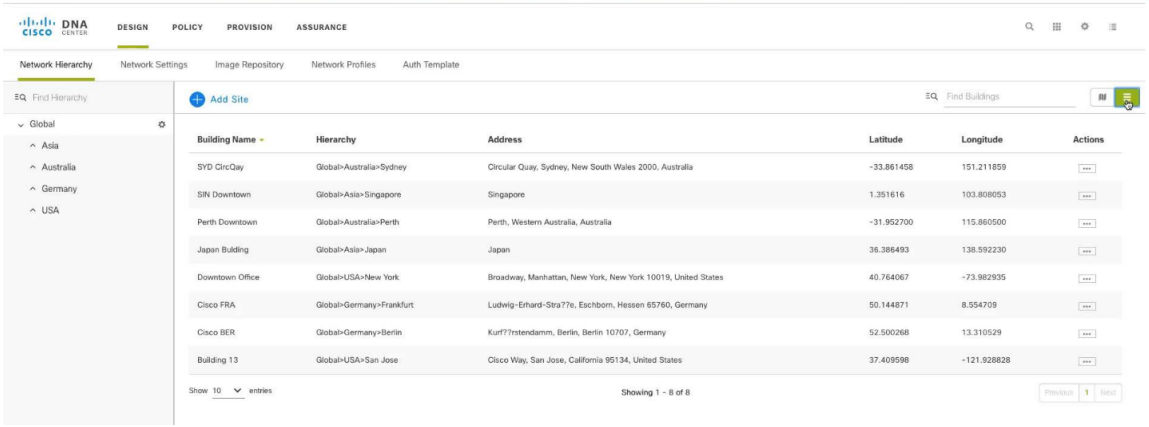
- The goal is to continuously monitor and adjust network performance to help assure desired business outcomes.

UI

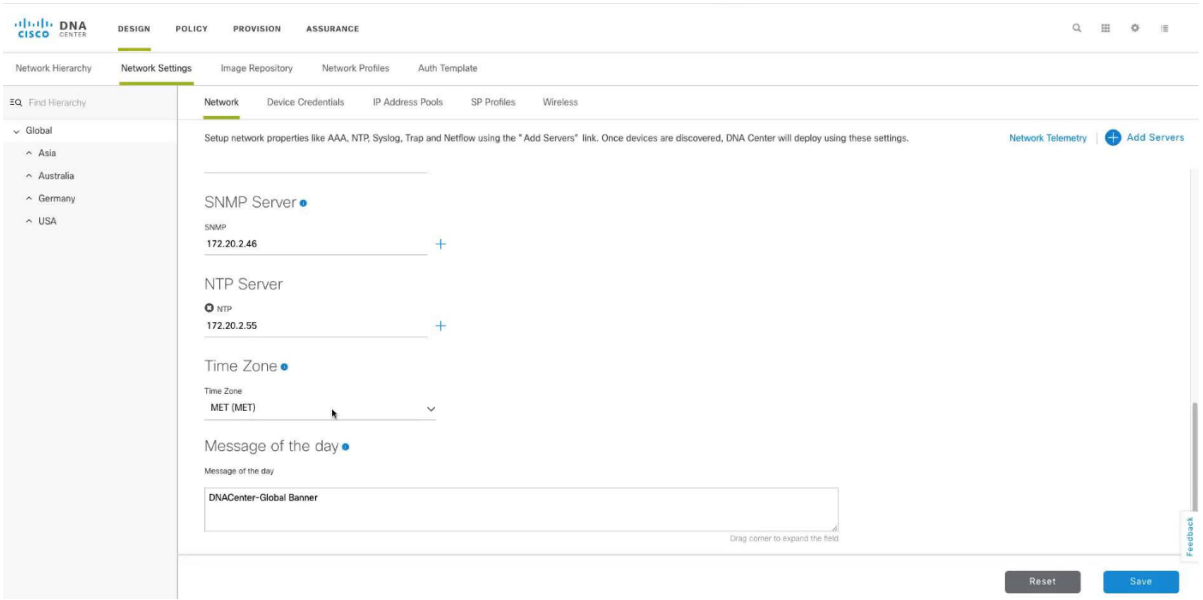




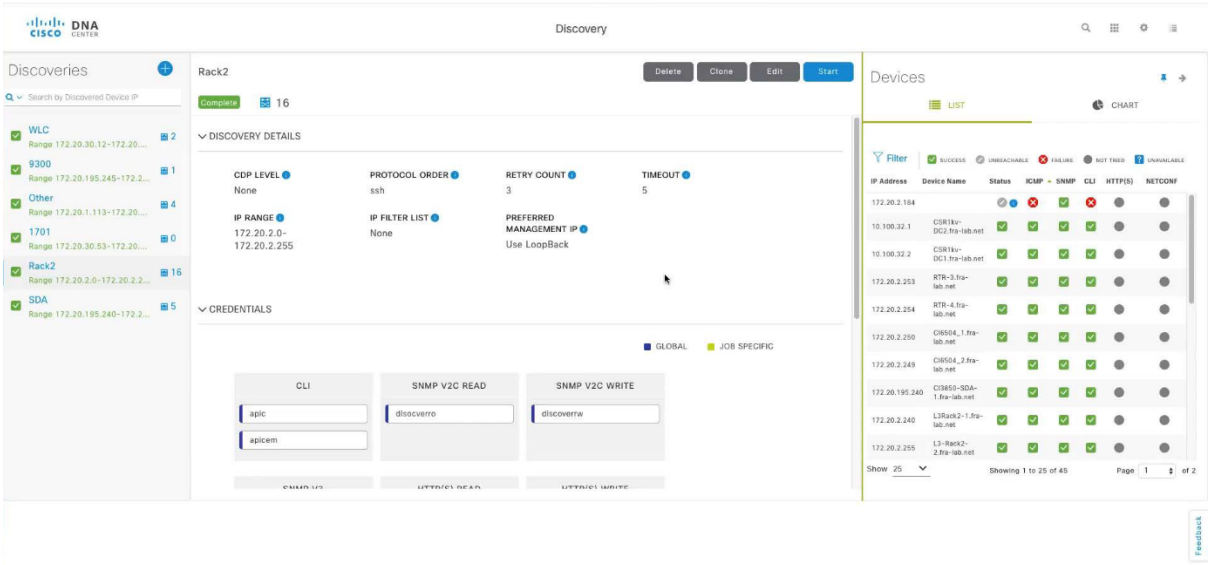
Design – Network Hierarchy



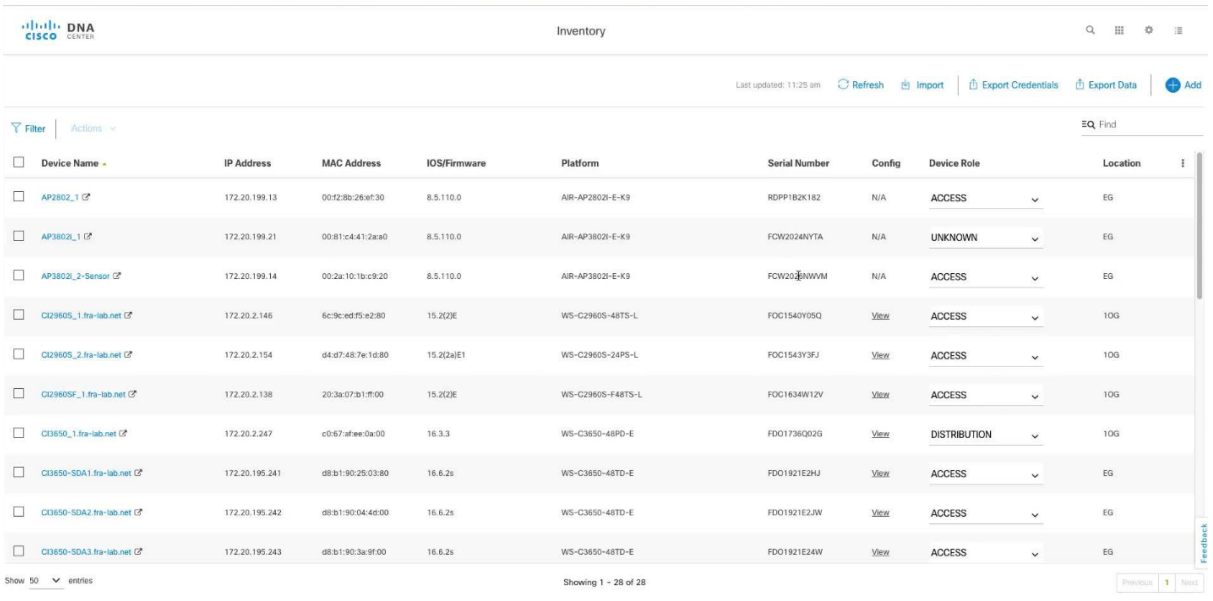
Design – Network Settings



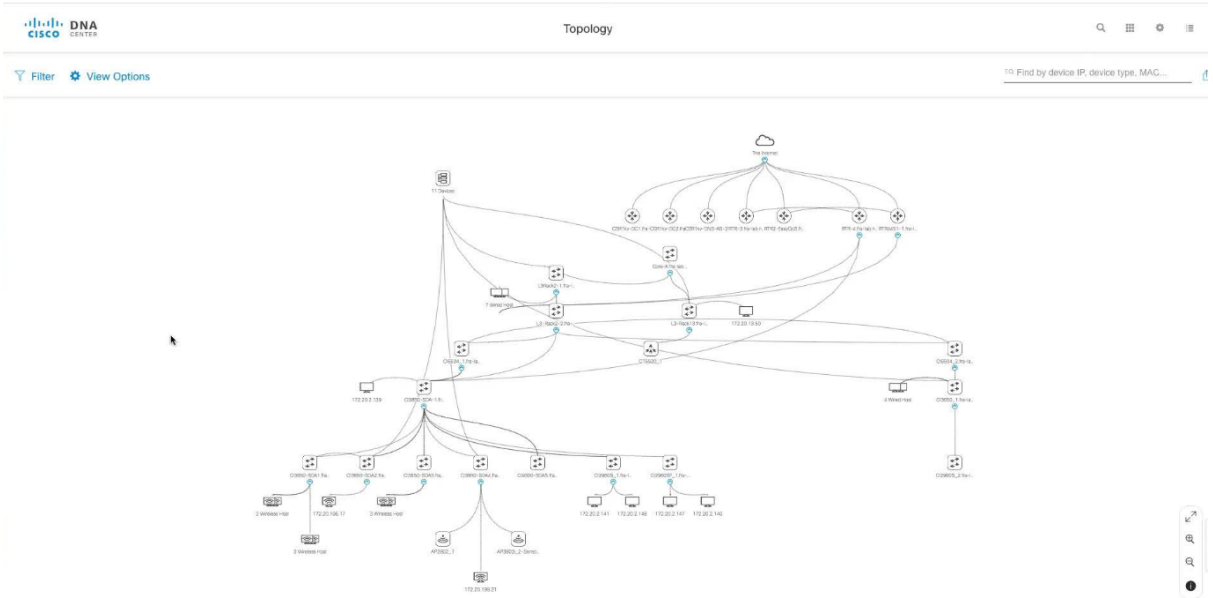
Tools - Discovery



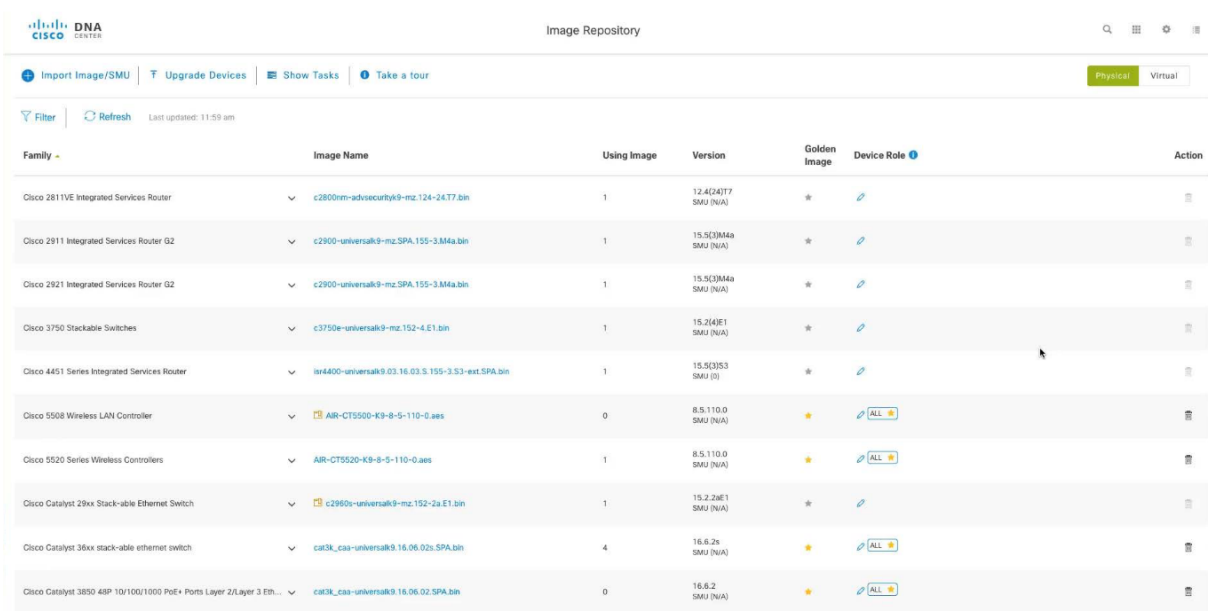
Tools - Inventory



Tools - Topology



SWIM Software and Image Management



SD-Access Software Defined Access

- SD-Access is a newer method of network access control which solves the limitations of the traditional implementation
- Traffic flow security is based on user identity, not physical location and IP address

- Users log in from and can move to any physical location in the network
- Two components are required for SD-Access:
- Users are authenticated by the ISE Identity Services Engine
- The security policy (permitted and denied communication between groups) is configured on the DNA Center

Underlay and Overlay Network

- SD-Access uses an underlay and overlay network
- An underlay network is the underlying physical network. It provides the underlying physical connections which the overlay network is built on top of.
- An overlay network is a logical topology used to virtually connect devices. It is built over the physical underlay network.
- The combination of underlay and overlay forms the SD-Access 'network fabric'

- When SD-Access is deployed into an existing ('brownfield') network, any configuration can be used for the underlying physical network. Links between devices can be layer 2 or layer 3 and any routing protocol can be used
- DNA Center can be used to automatically provision the underlay network in new ('greenfield') sites. In this case layer 3 links are used between devices and IS-IS is used as the routing protocol

- LISP is used for the Control Plane
- VXLAN is used for the Data Plane
- Cisco TrustSec CTS is used for the policy
- Each technology has been optimized for SD-Access

Policy Plane – Cisco TrustSec CTS

- Users are authenticated by the ISE Identity Services Engine
- The security policy is configured on DNA Center
- Users are allocated an SGT Scalable Group Tag
- Cisco TrustSec secures traffic flows based on the security policy and SGTs
- Standard TrustSec needs end-to-end TrustSec devices, SD-Access uses overlay tunnels so can work with other devices

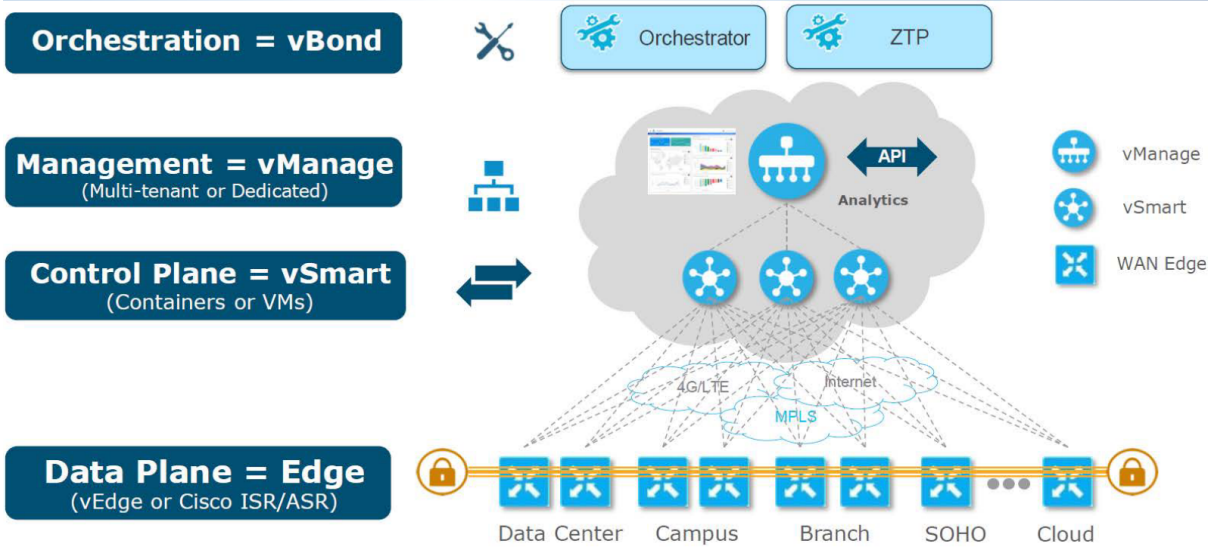
SD-WAN

- Cisco acquired Viptela in 2017 to enhance their SD-WAN solution (previously called 'IWAN')
- It provides automated setup of WAN connectivity between sites
- Monitoring and failover is automated
- Traffic flow control is application aware

SD-WAN Benefits

- Automated, standardized setup of connectivity between sites
- Transport independent
- Simplified, integrated operations
- More flexibility and easier to migrate WAN services
- The required, predictable performance for important applications
- Integration with the latest cloud and network technologies
- Lower cost

SD-WAN Architecture – Horizontal Scaling



Data Plane - vEdge Routers

- vEdge routers run the data plane.
- They are physical or virtual routers.
- They form an IPsec encrypted data plane between each other.
- A site can have 2 vEdge routers for redundancy.

Control Plane - vSmart Controllers

- vSmart controllers run the control plane.
- They are the centralized brain of the solution.
- They run as virtual machines.
- They distribute policy and forwarding information to the vEdge routers inside TLS tunnels.
- Each vEdge router connects to two vSmart controllers for redundancy.

Management Plane – vManage NMS

- The vManage NMS provides the management plane GUI.
- It enables centralized configuration and simplifies changes.
- It provides real time alerting.
- It runs as a virtual machine.
- Multiple vManage NMS are clustered for redundancy.

Orchestration – vBond orchestrator

- The vBond orchestrator authenticates all vSmart controllers, vManage NMS and vEdge routers that join the SD-WAN network.
- It enables vEdge routers to discover each other, vManage and vSmart.
- It has a public IP address and is deployed in the DMZ.
- It runs as a virtual machine (can also run on a router in smaller deployments.)
- Multiple vBond orchestrators can be deployed with round robin DNS.

ZTP Zero Touch Provisioning service

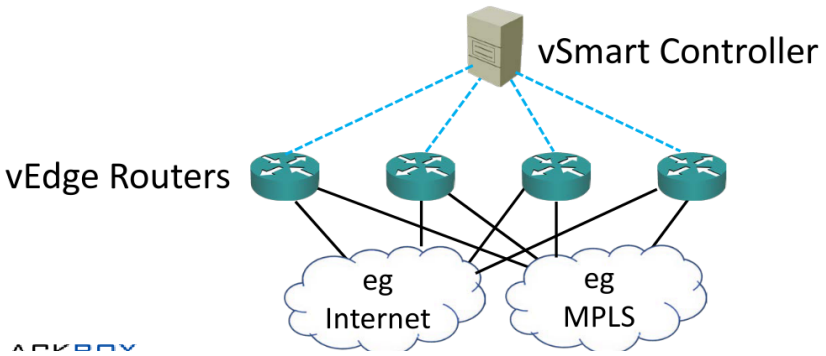
- Cloud based shared service hosted by Cisco.
- Utilized on first boot of vEdge router only.
- Directs it to vBond to orchestrate joining it to the network.

On Premises and Cloud

- vBond, vSmart and vManage can be deployed:
  - On premises
  - Hosted in Cisco (or partner) cloud
- Most deployments are in the cloud

Building the Data Plane

- The vSmart controller directs the vEdge routers to build a full mesh (by default) of IPsec VPN tunnels between themselves.
- vSmart propagates policy and routing information to the vEdge routers with OMP Overlay Management Protocol.



BF VPN Tunnel Monitoring

- Bidirectional Forwarding Detection packets are sent over all VPN tunnels
- This detects if a tunnel goes down, and also provides latency, jitter and loss statistics

Traffic Forwarding Options

- If multiple tunnels are available (for example over MPLS and Internet) traffic can be load balanced over the tunnels:
- Active/Active
- Weighted Active/Active
- Application pinning Active/Standby
- Application Aware Routing

Application Aware Routing

- BFD monitors the latency, jitter and loss across the VPN tunnels
- You can set minimum requirements for an application with Service Level Agreement SLA Classes
- SD-WAN ensures the application is sent over a link which meets its SLA requirements
- By default traffic will fall back to another link if no suitable link is available