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.”

Cisco DNA Digital Network Architecture

- 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)

DNA Center Appliance

- The DNA Center Appliance runs on Cisco UCS server hardware
- The underlying operating system is Linux
- It can be clustered for redundancy

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.

IBN Intent Based Networking Example 1

Example 1: a QoS policy roll-out

- The Intent: The network policy is first defined, for example providing guaranteed service to voice and video across network locations

IBN Intent Based Networking Example 1

Traditional Networking:

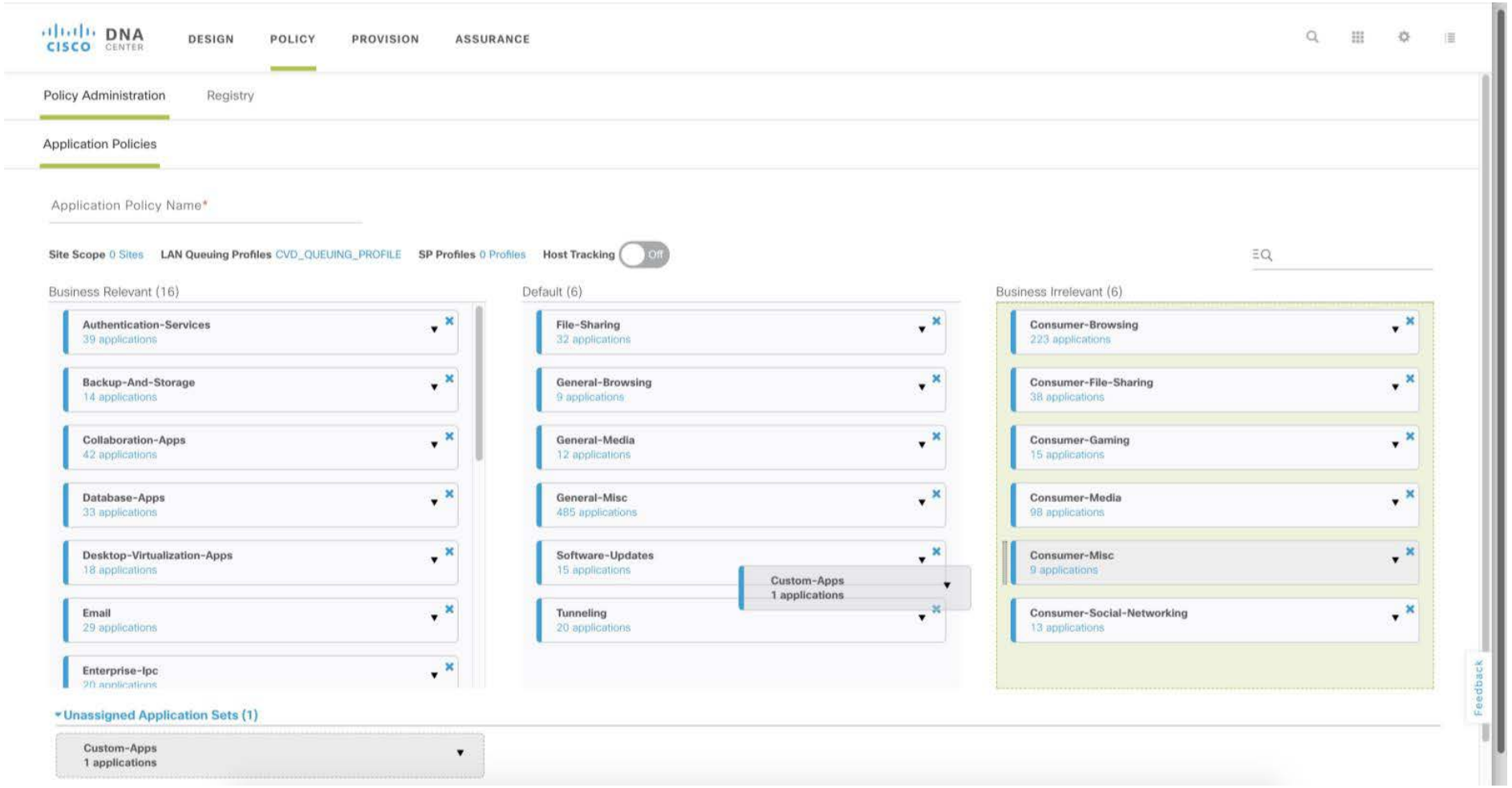
- The network team researches and plans the implementation, then configures each network device individually.
- Different network device models require different commands.
- This method is very time consuming and liable to mistakes

IBN Intent Based Networking Example 1

Intent Based Networking:

- The network team creates an Application Policy in DNA Center specifying voice and video as business relevant applications.
- DNA Center automatically configures the best practice QoS settings on the network devices.
- This can reduce total deployment time from months to minutes

IBN Intent Based Networking Example 1



IBN Intent Based Networking Example 2

Example 2: Securing traffic flows in the campus

- The Intent: Users in DeptA and DeptB must have connectivity to other users in their own department, and to the company servers. They must not have connectivity to users in the other department

IBN Intent Based Networking Example 2

Traditional Networking:

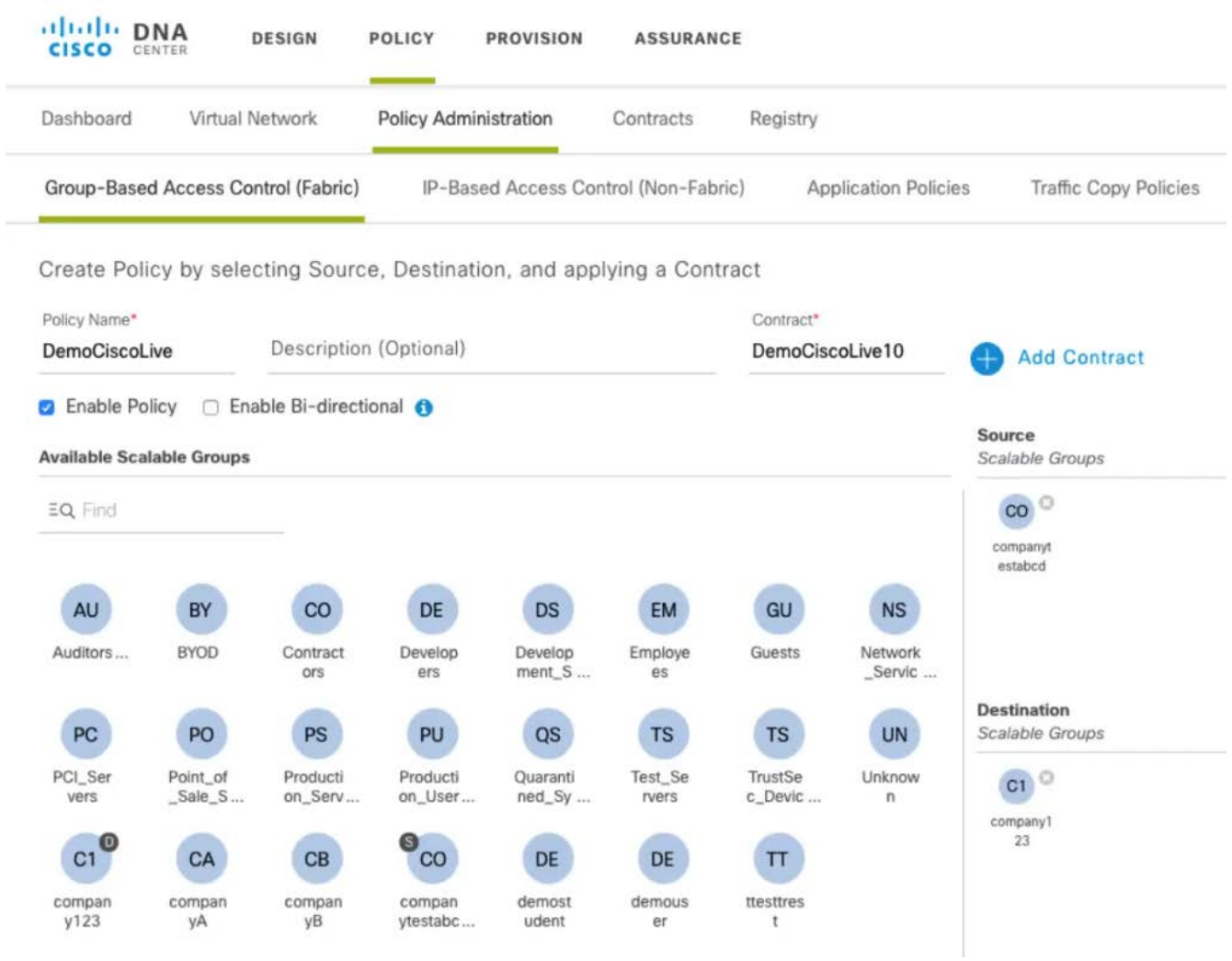
- The network team plans the VLAN, IP subnet and ACL implementation, then configures each switch individually.
- Users are expected to stay plugged in to the same access port. They are assigned a VLAN and IP Address based on their physical location
- This method is very time consuming, liable to mistakes, and does not support mobility

IBN Intent Based Networking Example 2

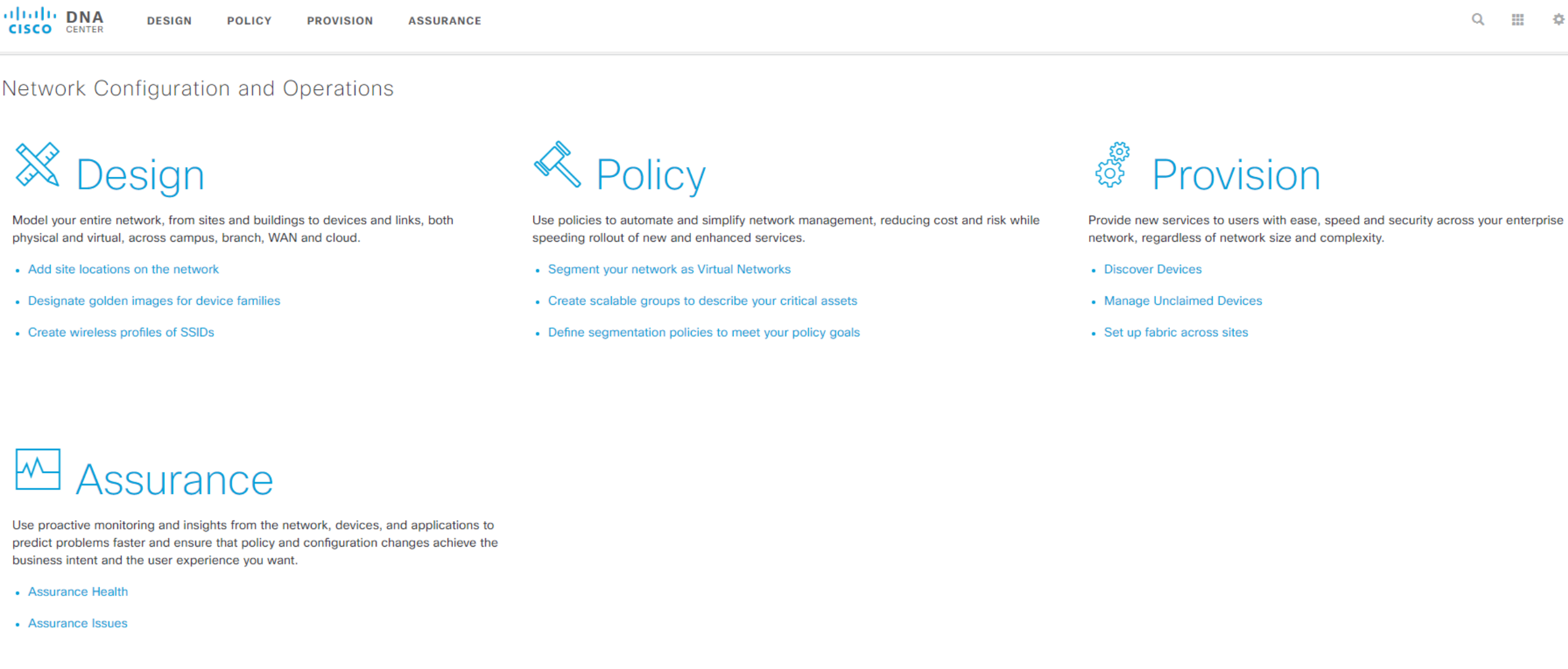
Intent Based Networking:

- The network team creates a Group-Based Access Control Policy in DNA Center which specifies the allowed traffic flows
- Users log in from and can move to any physical location on campus
- They are authenticated by Cisco ISE Identity Services Engine and assigned a Security Group Tag controlling their access

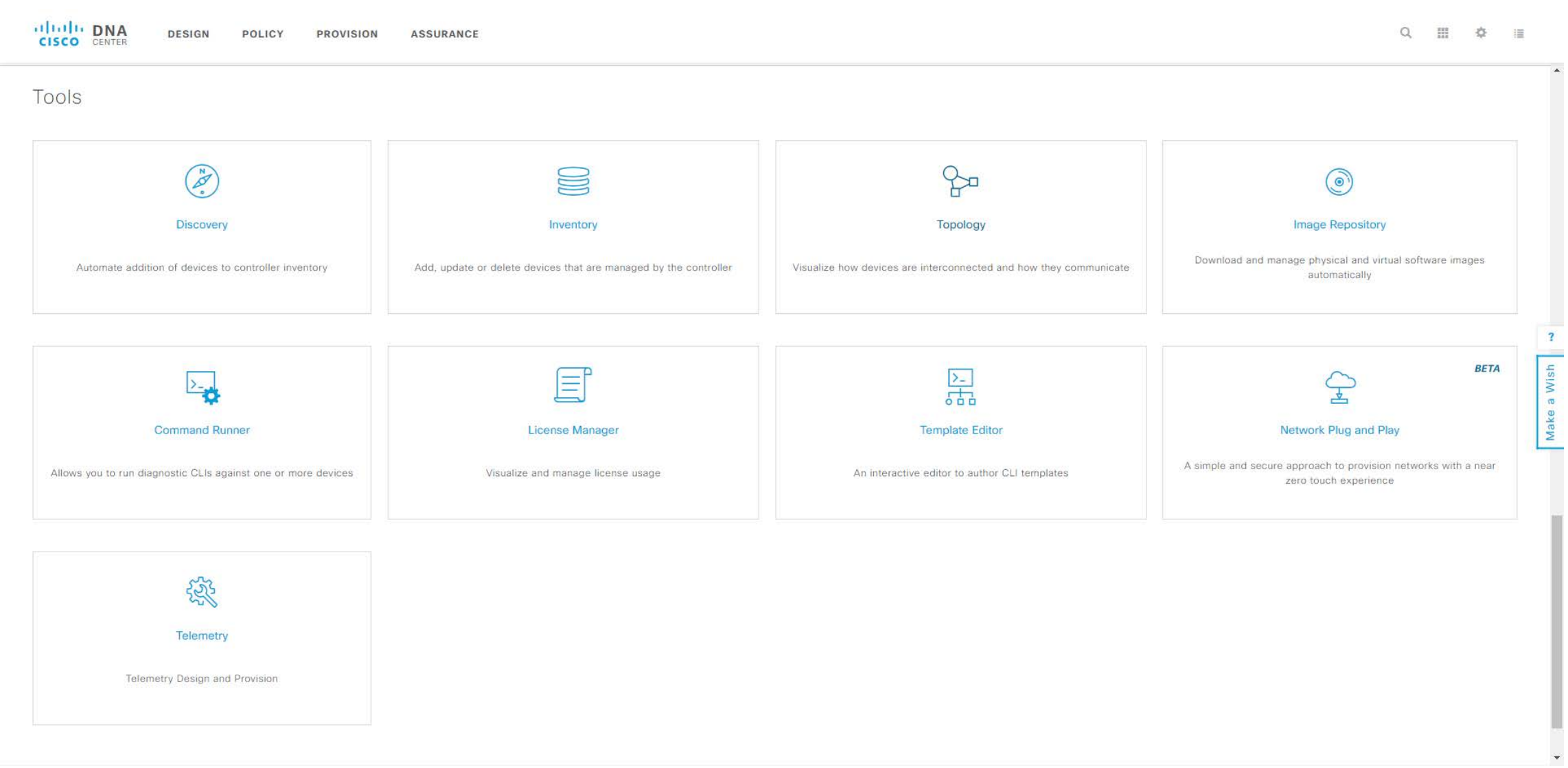
IBN Intent Based Networking Example 2



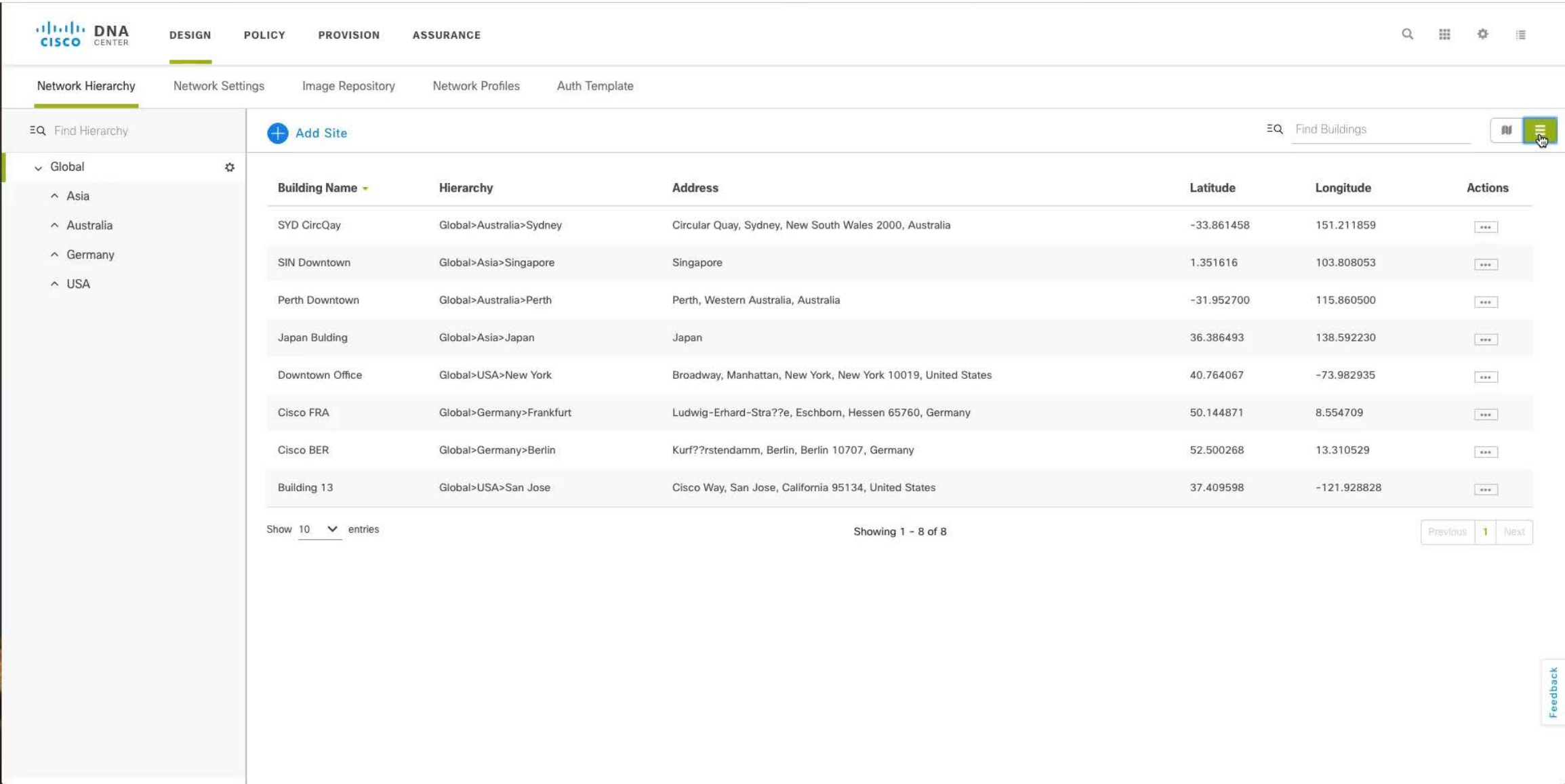
DNA Center Dashboard – Config and Ops



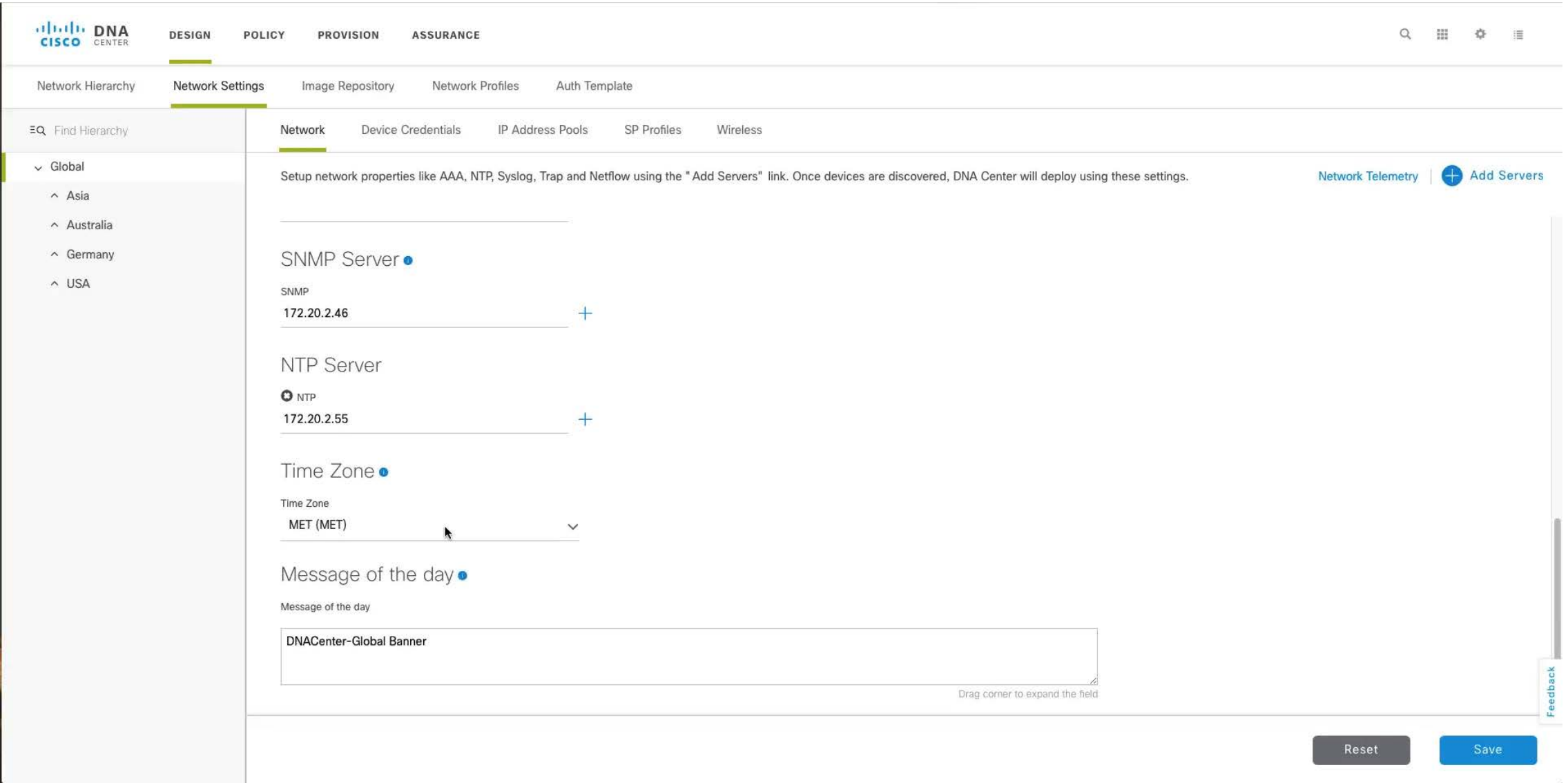
DNA Center Dashboard - Tools



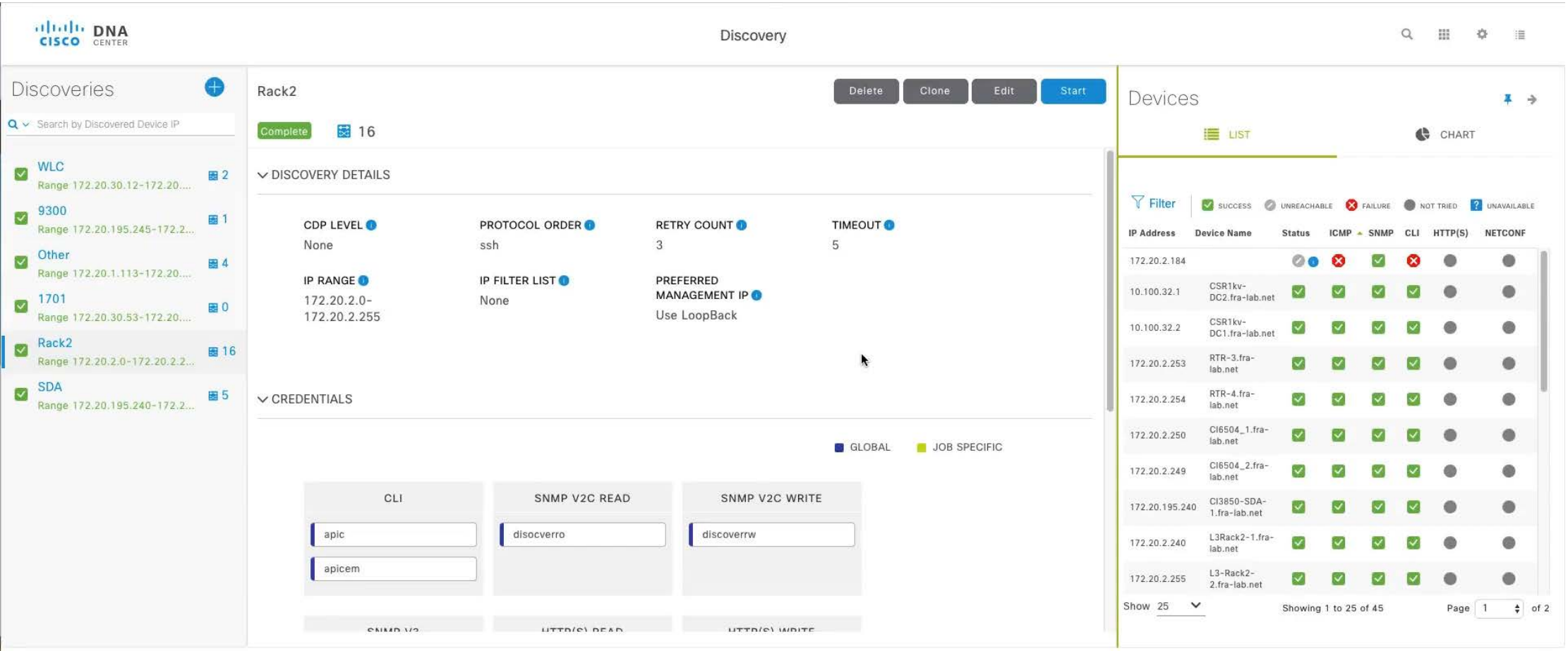
Design – Network Hierarchy



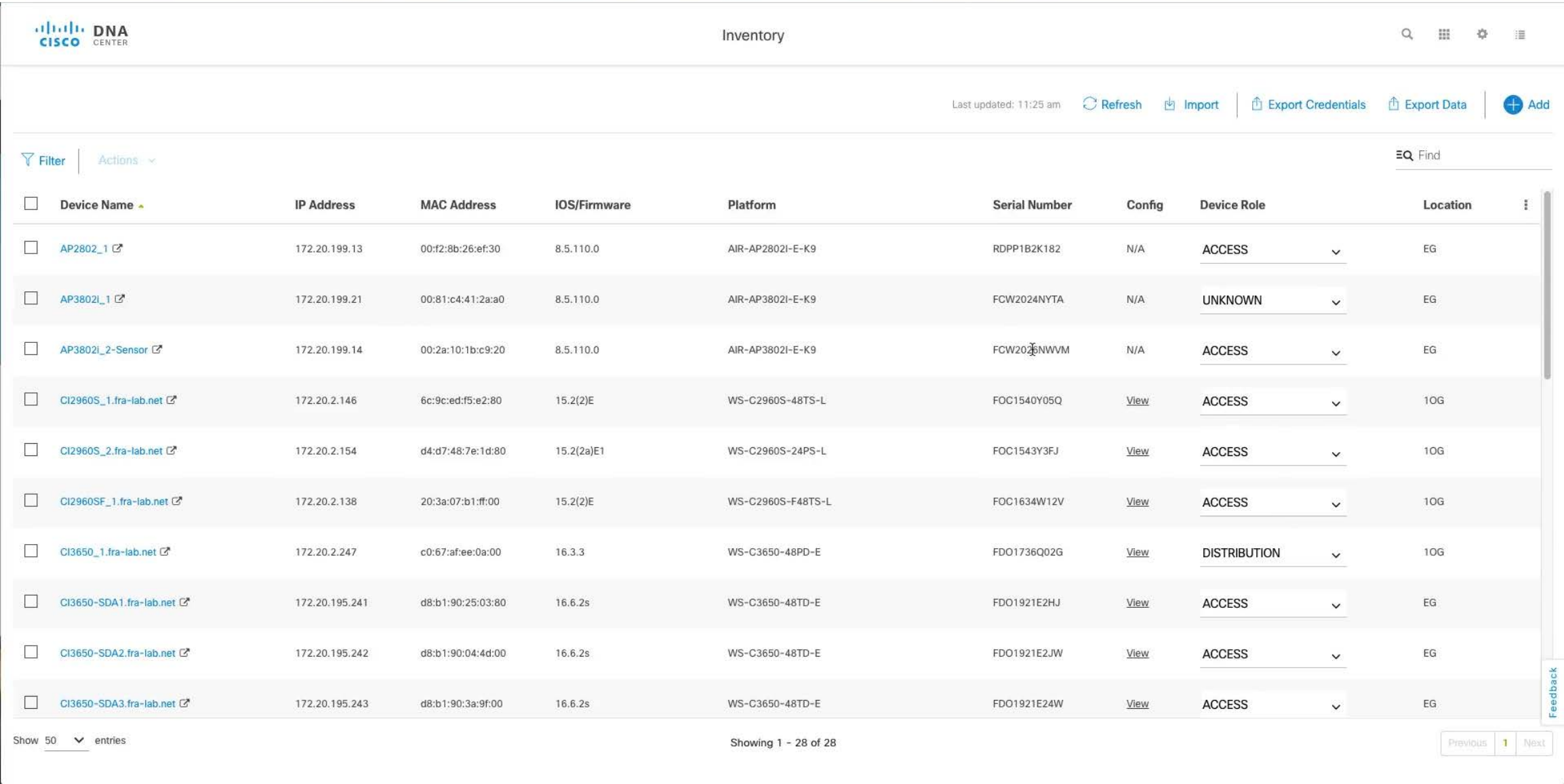
Design – Network Settings



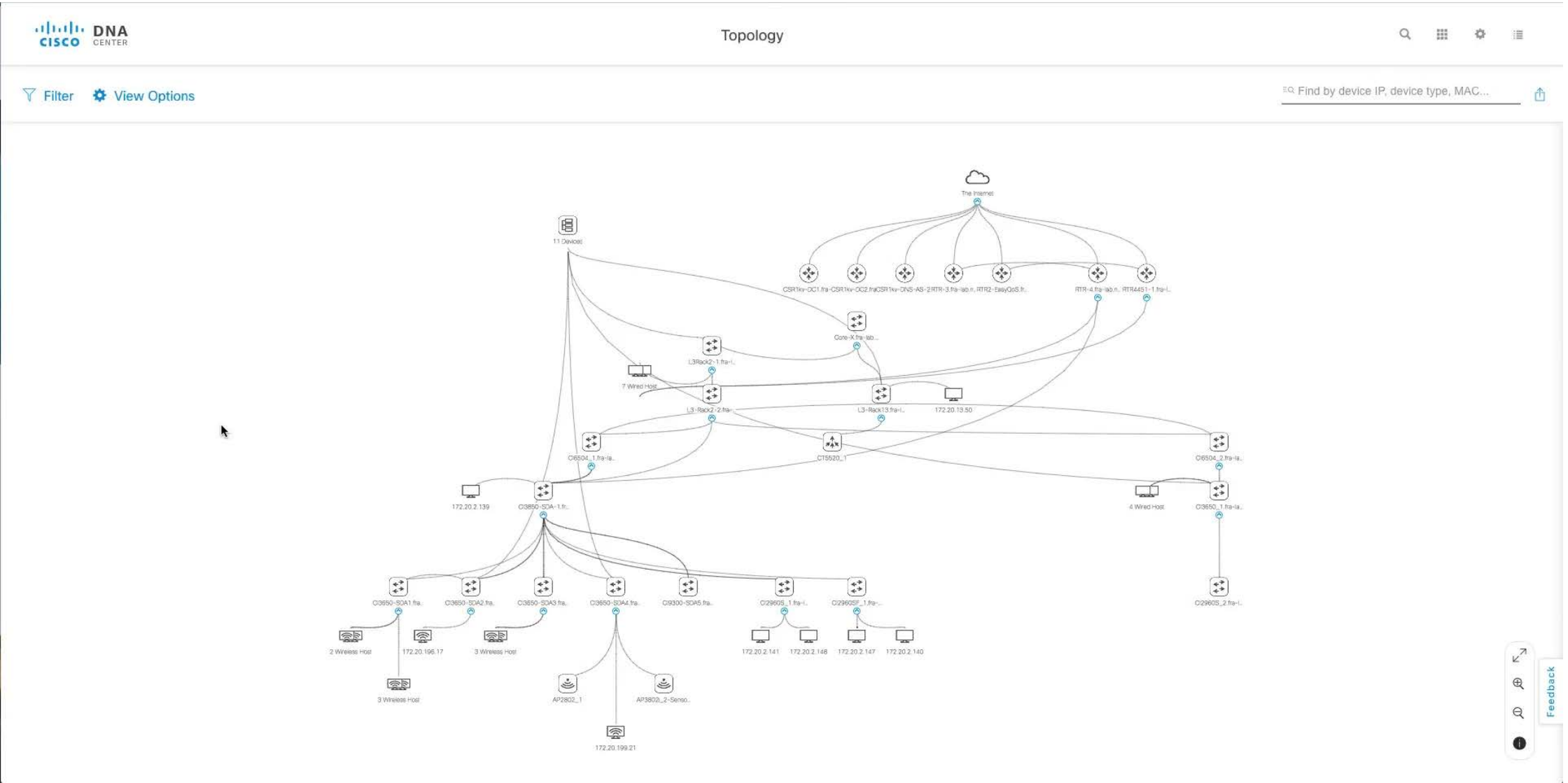
Tools - Discovery



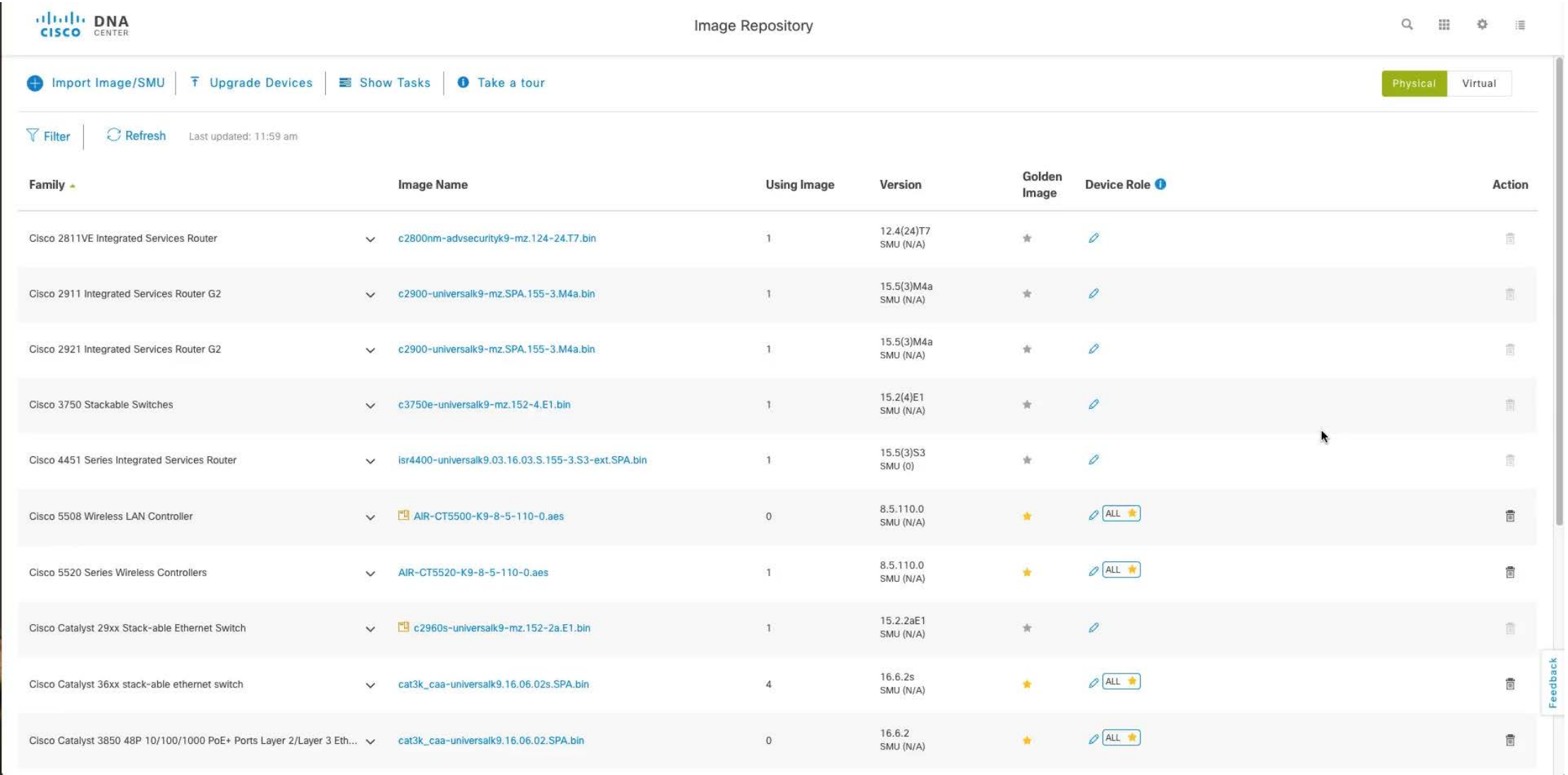
Tools - Inventory



Tools - Topology



SWIM Software and Image Management



DNA Center Features – Network Plug and Play

- Network Plug and Play allows routers, switches and wireless access points to be deployed in remote offices with zero touch configuration
- The device is physically installed in the remote office and connected to the network

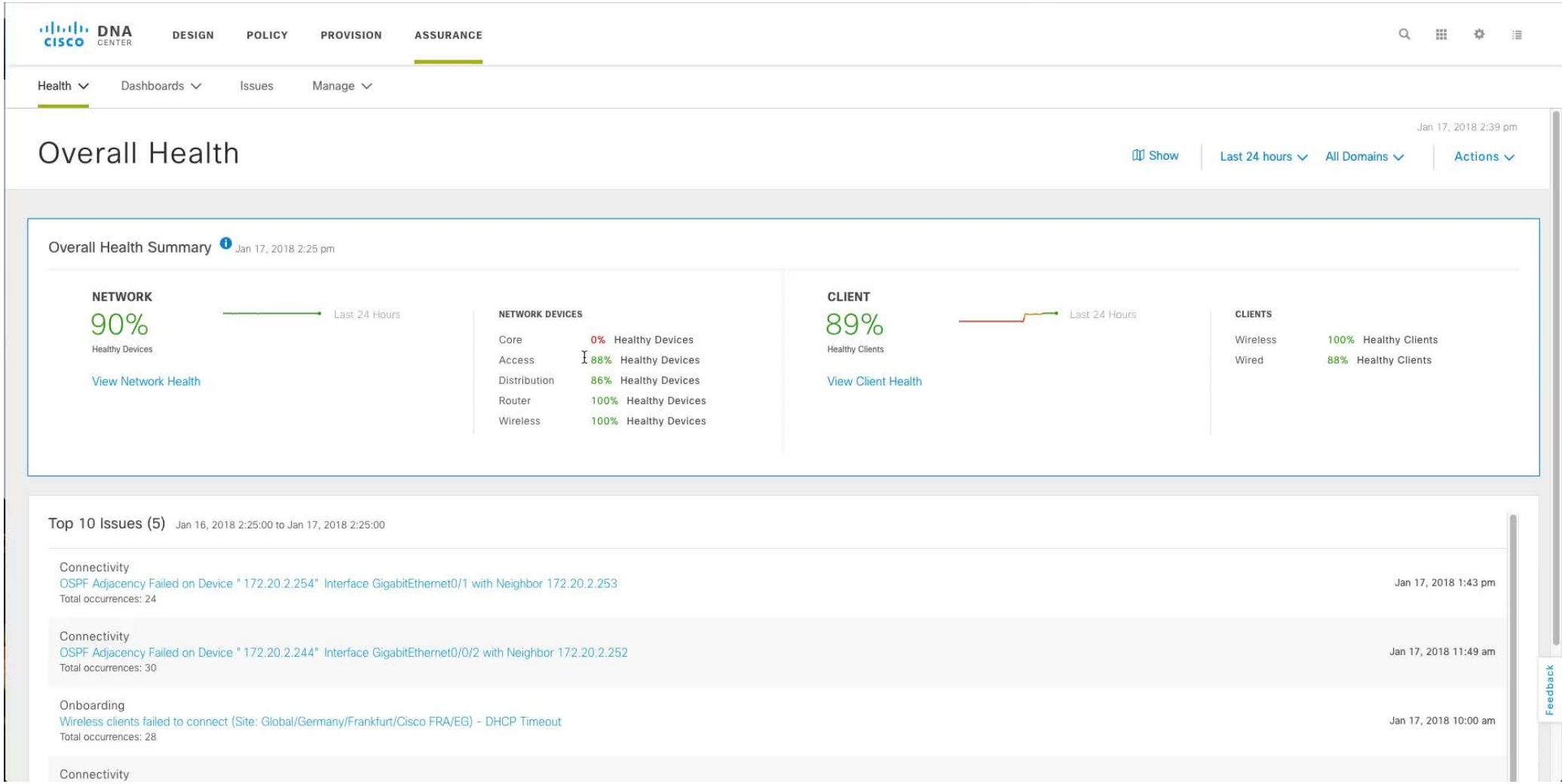
DNA Center Features – Network Plug and Play

- It discovers DNA Center through various methods including DHCP option 43 or DNS ‘pnpserver.*domain-name.com*’
- It then registers with and downloads its configuration from DNA Center
- This ensures consistent configuration of remote office devices with no need for a network engineer onsite

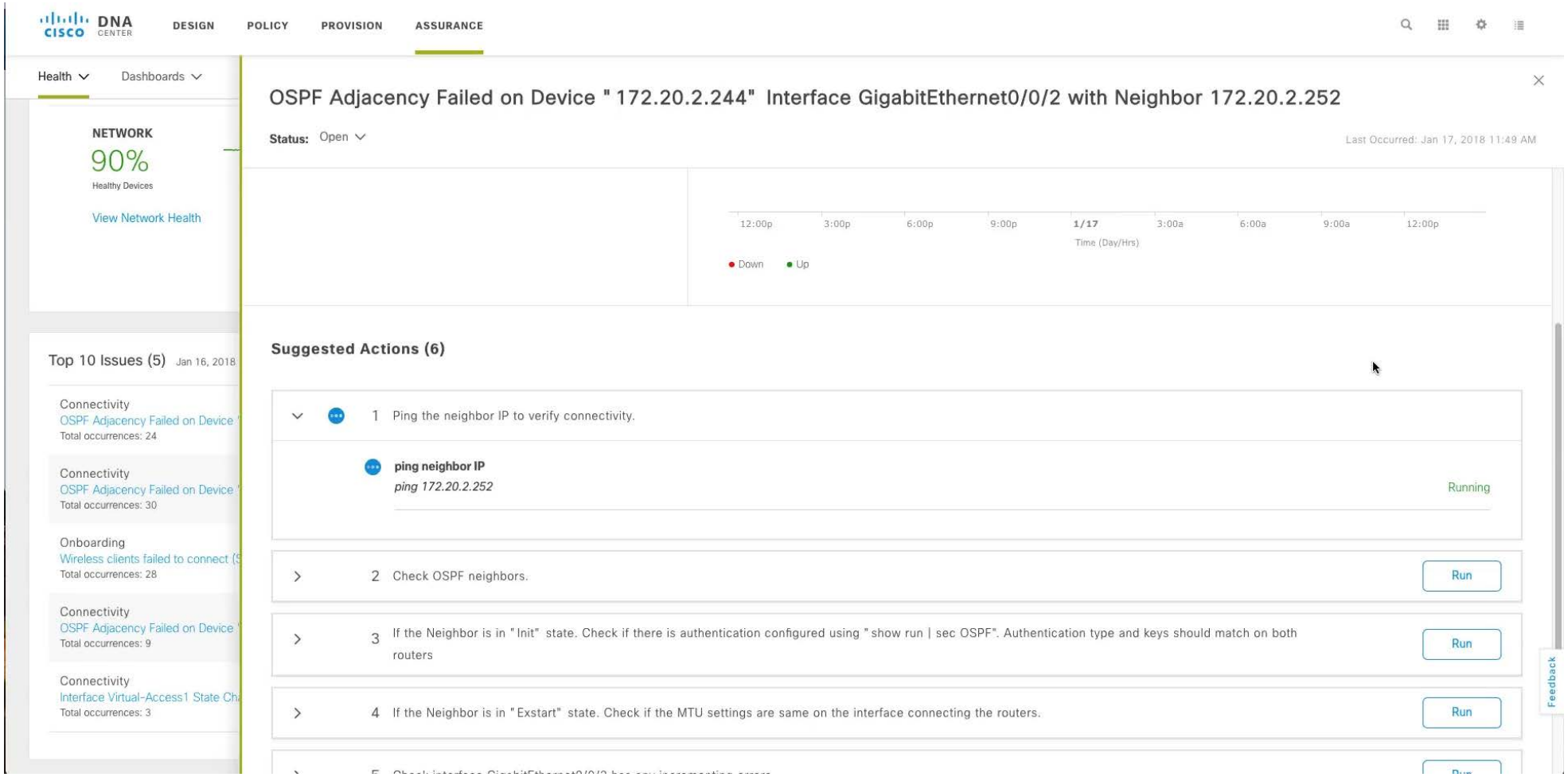
Assurance

- Assurance guarantees that the infrastructure is doing what you intended it to do
- DNA Center receives information from all the network devices and ISE etc.
- DNA Center's correlation engine can identify 150+ different types of network and client issues
- DNA Center reports the problem and provides recommended remediation actions

Assurance


DNA CENTER
DESIGN
POLICY
PROVISION
ASSURANCE
Health
Dashboards
Issues
Manage
Overall Health
Jan 17, 2018 2:39 pm
Show
Last 24 hours
All Domains
Actions
Overall Health Summary
Jan 17, 2018 2:25 pm
NETWORK
90%
Healthy Devices
Last 24 Hours
View Network Health
NETWORK DEVICES
Core 0% Healthy Devices
Access 88% Healthy Devices
Distribution 86% Healthy Devices
Router 100% Healthy Devices
Wireless 100% Healthy Devices
CLIENT
89%
Healthy Clients
Last 24 Hours
View Client Health
CLIENTS
Wireless 100% Healthy Clients
Wired 88% Healthy Clients
Top 10 Issues (5)
Jan 16, 2018 2:25:00 to Jan 17, 2018 2:25:00
Connectivity
OSPF Adjacency Failed on Device " 172.20.2.254" Interface GigabitEthernet0/1 with Neighbor 172.20.2.253
Total occurrences: 24
Jan 17, 2018 1:43 pm
Connectivity
OSPF Adjacency Failed on Device " 172.20.2.244" Interface GigabitEthernet0/0/2 with Neighbor 172.20.2.252
Total occurrences: 30
Jan 17, 2018 11:49 am
Onboarding
Wireless clients failed to connect (Site: Global/Germany/Frankfurt/Cisco FRA/EG) - DHCP Timeout
Total occurrences: 28
Jan 17, 2018 10:00 am
Connectivity
Feedback

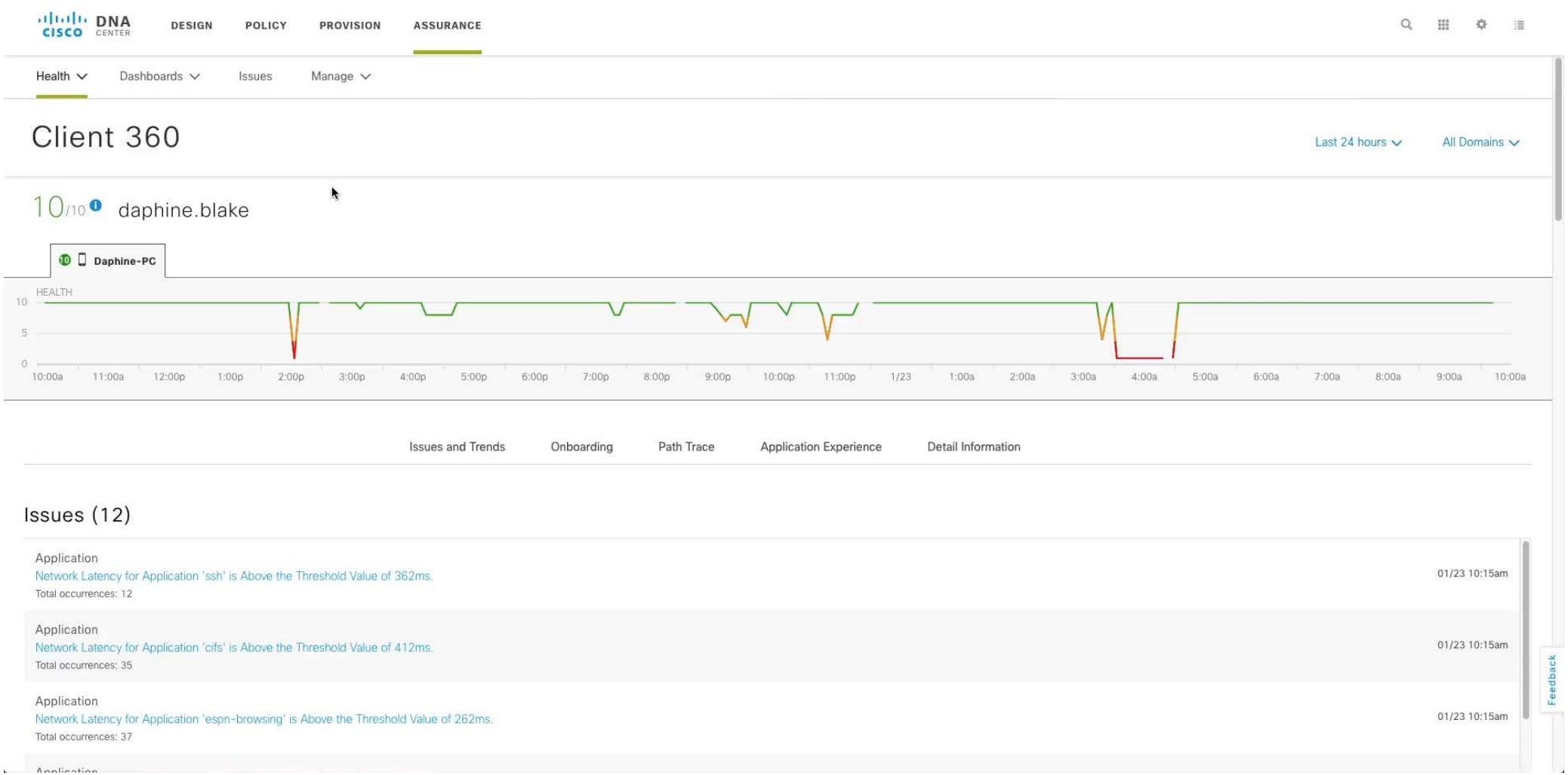
Assurance


DNA CENTER
DESIGN
POLICY
PROVISION
ASSURANCE
Health
Dashboards
NETWORK
90%
Healthy Devices
View Network Health
Top 10 Issues (5) Jan 16, 2018
Connectivity
OSPF Adjacency Failed on Device
Total occurrences: 24
Connectivity
OSPF Adjacency Failed on Device
Total occurrences: 30
Onboarding
Wireless clients failed to connect
Total occurrences: 28
Connectivity
OSPF Adjacency Failed on Device
Total occurrences: 9
Connectivity
Interface Virtual-Access1 State Ch
Total occurrences: 3
OSPF Adjacency Failed on Device " 172.20.2.244" Interface GigabitEthernet0/0/2 with Neighbor 172.20.2.252
Status: Open
Last Occurred: Jan 17, 2018 11:49 AM
12:00p
3:00p
6:00p
9:00p
1/17
3:00a
6:00a
9:00a
12:00p
Time (Day/Hrs)
Down
Up
Suggested Actions (6)
1 Ping the neighbor IP to verify connectivity.
ping neighbor IP
ping 172.20.2.252
Running
2 Check OSPF neighbors.
Run
3 If the Neighbor is in "Init" state. Check if there is authentication configured using "show run | sec OSPF". Authentication type and keys should match on both routers
Run
4 If the Neighbor is in "Exstart" state. Check if the MTU settings are same on the interface connecting the routers.
Run
Feedback

Assurance – Network Time Travel

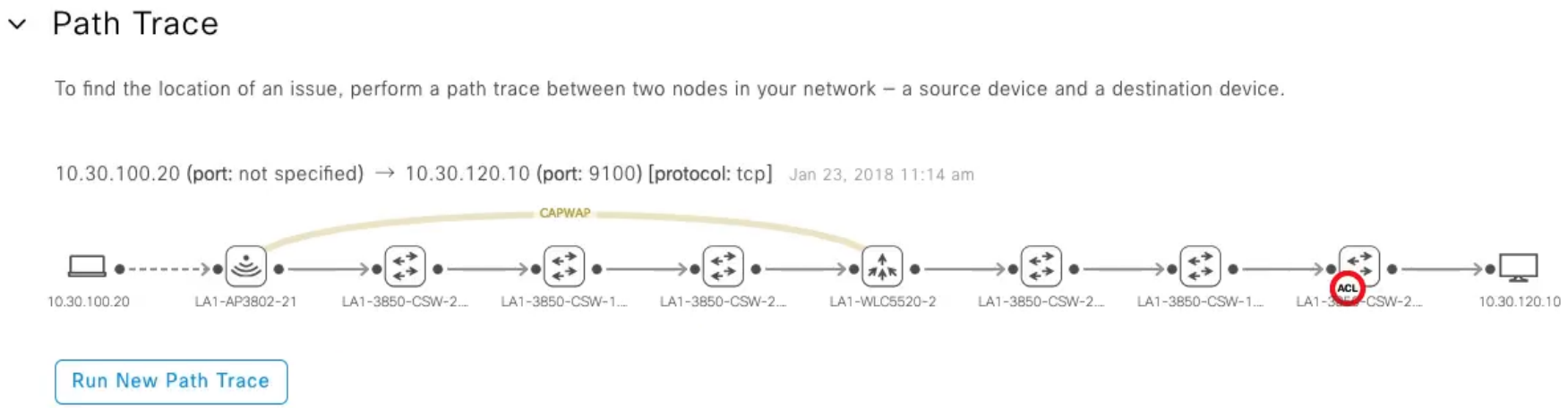
- Administrators can drill down into the health status of network devices and clients
- You can see the current status and also view historical information
- This is useful to troubleshoot intermittent problems or issues which occurred in the past

Assurance – Network Time Travel



DNA Center Features – Path Trace

- An engineer can use Path Trace to query DNA Center for the path that traffic takes over the network
- This aids troubleshooting



FLACKBOX
www.flackbox.com

API Support

- Everything that can be done through the DNA Center GUI can also be done via a northbound REST API
- DNA Center also supports ‘east’ and ‘west’ bound APIs for integration with other services such as reporting and analytics servers