IBN Intent-Based Networking

- IBN builds on software-defined networking to move away from a network of individual devices which are manually managed one-by-one to a controller-led network that is managed as an integrated whole.
- It captures business intent and translates it into policies that can be automated and applied consistently across the network.
- It continuously monitors and adjusts network performance to help assure desired business outcomes.



Cisco Software Defined Architecture

- 3 of the main building blocks of Cisco Software Defined Architecture are:
 - Catalyst Center
 - SD-Access
 - SD-WAN



Catalyst Center

- Catalyst Center (formerly 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)



Catalyst Center Appliance

- Catalyst Center runs as a virtual appliance in the cloud or on-premises, or as a physical appliance on Cisco UCS server hardware
- The underlying operating system is Linux
- It can be clustered for redundancy





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



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



Intent Based Networking:

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



cication Policies Discretion Policy Name* Scope 0 Sites LAN Queuing Profiles CVD_QUEUING_PROFILE SP Profiles 0 Profiles Host Tracking Off iness Relevant (16) Default (6) Business irrelevant (16)	ΞQ
Default (6) LAN Queuing Profiles CVD_QUEUING_PROFILE SP Profiles 0 Profiles Host Tracking Off Default (6) Business Irrelevant (16)	ΞQ
ness Relevant (16) Default (6) Business Irrelevant (ΞQ
	6)
Authentication-Services 39 applications File-Sharing 32 applications Consumer-Brow 223 applications	
Backup-And-Storage 14 applications General-Browsing 9 applications Consumer-File 38 applications	Sharing ×
Collaboration-Apps 42 applications General-Media 12 applications Consumer-Gam 15 applications	ing ×
Database-Apps 33 applications General-Misc 485 applications Consumer-Med 98 applications	ia 🔻 🛪
Desktop-Virtualization-Apps 18 applications Software-Updates 15 applications Custom-Apps Custom-Apps	×
1 applications	
Email Tunneling Consumer-Soci 13 applications Consumer-Soci 13 applications	al-Networking ×



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



Traditional Networking:

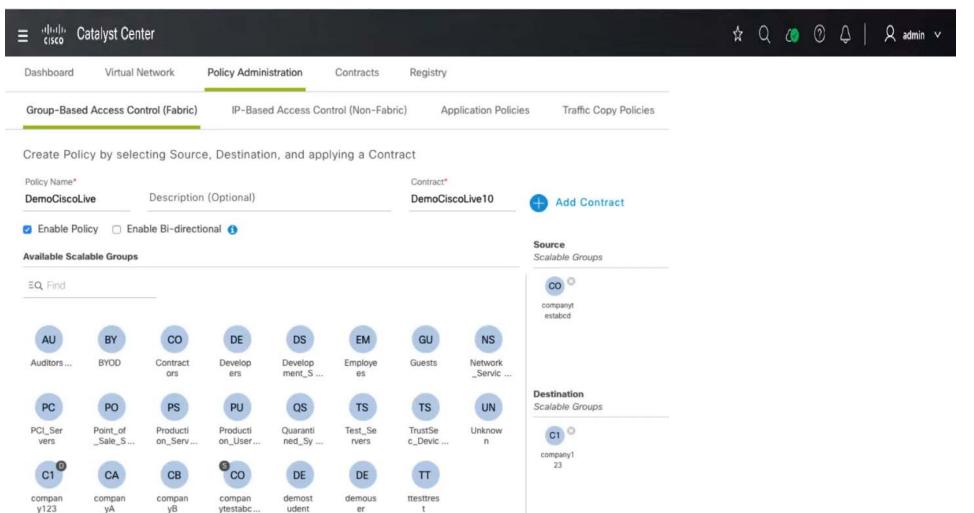
- The network team plans the VLAN, IP subnet and ACL implementation, then configures each switch individually.
- Users are expected to stay plugged in to the same access port. They are assigned a VLAN and IP Address based on their physical location
- This method is very time consuming, liable to mistakes,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



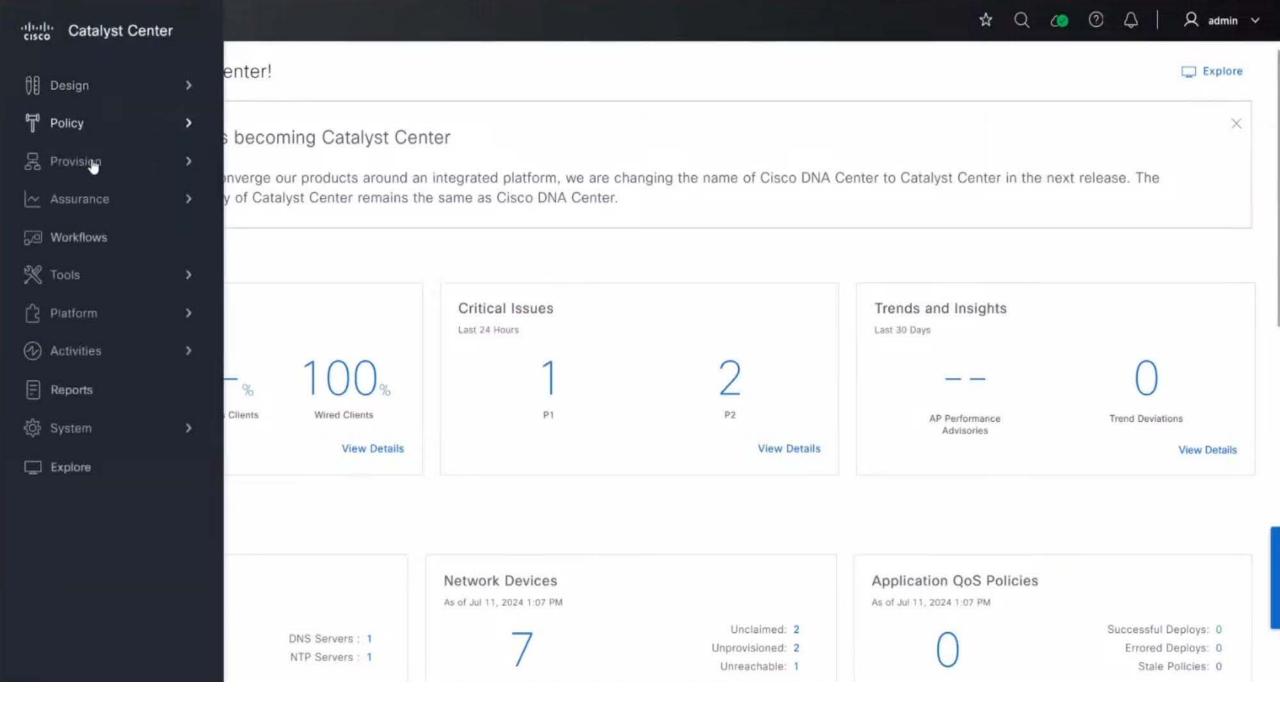
Intent Based Networking:

- The network team creates a Group-Based Access Control Policy in Catalyst 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





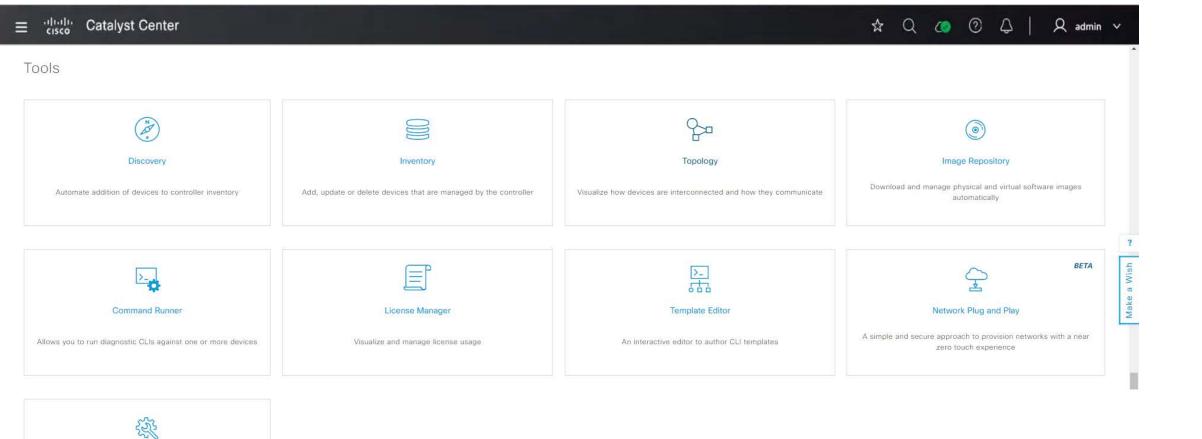




Catalyst Center Dashboard - Tools

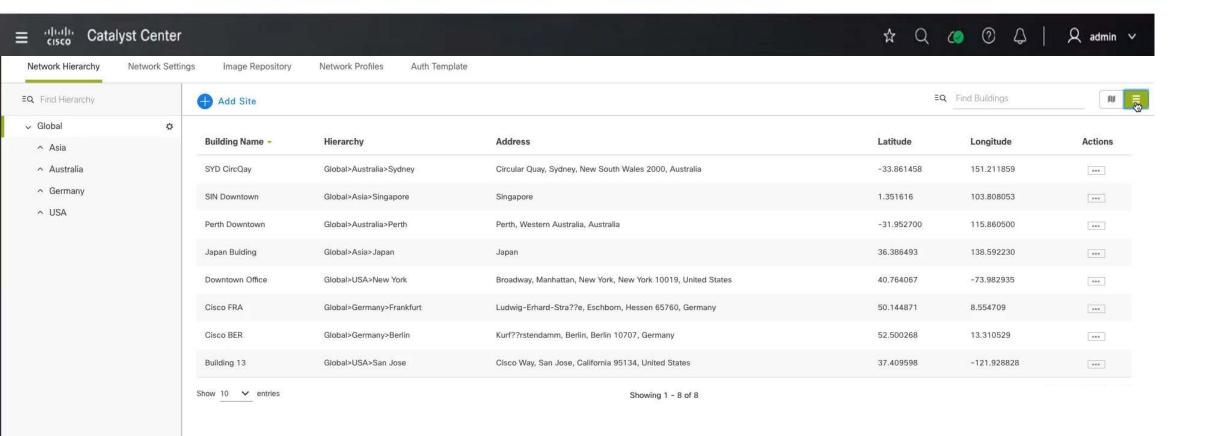
Telemetry

Telemetry Design and Provision



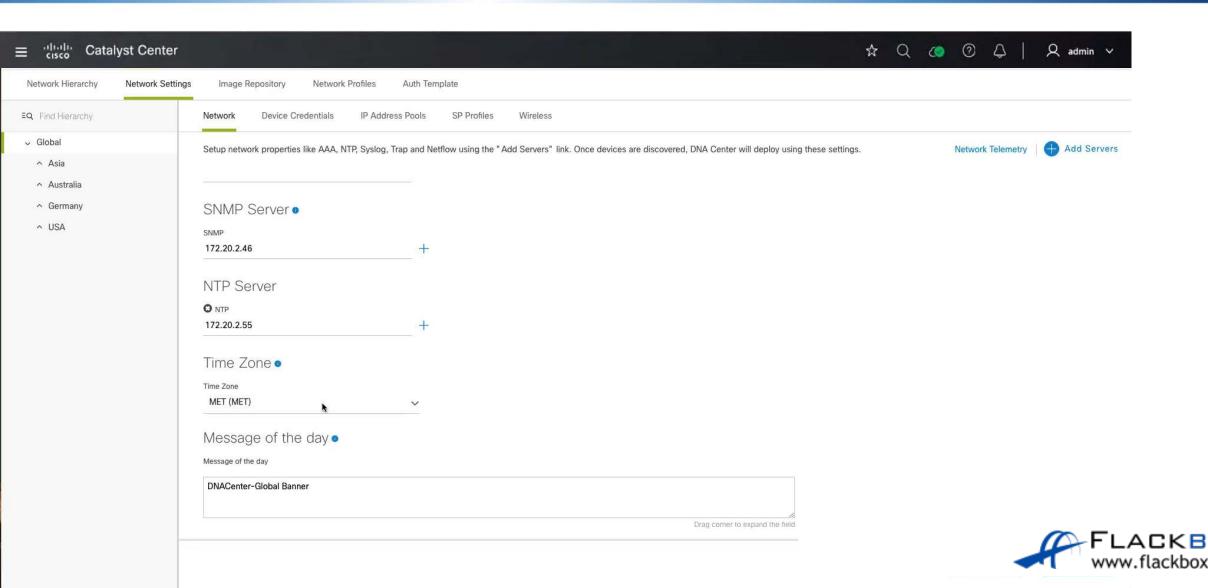


Design – Network Hierarchy

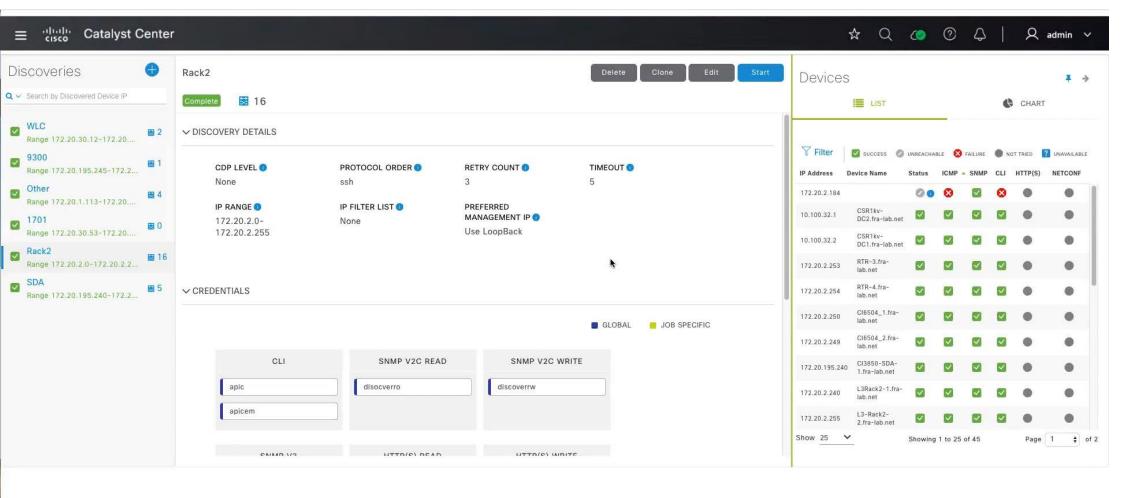




Design – Network Settings

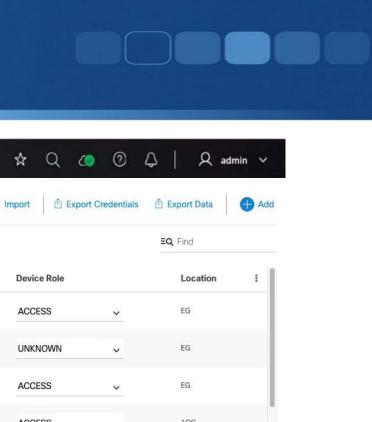


Tools - Discovery





Provision - Inventory



					Last updated: 11:25 am	Refresh 😃	Import 🖺 Export C	redentials	♠ Export Data	⊕ Add
₹ Filter Actions →									EQ Find	
Device Name -	IP Address	MAC Address	IOS/Firmware	Platform	Serial Number	Config	Device Role		Location	1
☐ AP2802_1 ♂	172.20.199.13	00:f2:8b:26:ef:30	8.5.110.0	AIR-AP2802I-E-K9	RDPP1B2K182	N/A	ACCESS	~	EG	
☐ AP3802i_1 🗗	172.20.199.21	00:81:c4:41:2a:a0	8.5.110.0	AIR-AP3802I-E-K9	FCW2024NYTA	N/A	UNKNOWN	~	EG	
AP3802i_2-Sensor 🗗	172.20.199.14	00:2a:10:1b:c9:20	8.5.110.0	AIR-AP3802I-E-K9	FCW20 2 €NWVM	N/A	ACCESS	~	EG	
☐ Cl2960S_1.fra-lab.net 🗗	172.20.2.146	6c:9c:ed:f5:e2:80	15.2(2)E	WS-C2960S-48TS-L	FOC1540Y05Q	View	ACCESS	~	10G	
Cl2960S_2.fra-lab.net 🗗	172.20.2.154	d4:d7:48:7e:1d:80	15.2(2a)E1	WS-C2960S-24PS-L	FOC1543Y3FJ	View	ACCESS	~	10G	
☐ Cl2960SF_1.fra-lab.net 🗗	172.20.2.138	20:3a:07:b1:ff:00	15.2(2)E	WS-C2960S-F48TS-L	FOC1634W12V	View	ACCESS	~	10G	
☐ Cl3650_1.fra-lab.net 🗹	172.20.2.247	c0:67:af:ee:0a:00	16.3.3	WS-C3650-48PD-E	FDO1736Q02G	View	DISTRIBUTION	~	10G	
☐ Cl3650-SDA1.fra-lab.net ☑	172.20.195.241	d8:b1:90:25:03:80	16.6.2s	WS-C3650-48TD-E	FDO1921E2HJ	View	ACCESS	~	EG	
☐ Cl3650-SDA2.fra-lab.net ♂	172.20.195.242	d8:b1:90:04:4d:00	16.6.2s	WS-C3650-48TD-E	FDO1921E2JW	View	ACCESS	~	EG	*
☐ Cl3650-SDA3.fra-lab.net ☑	172.20.195.243	d8:b1:90:3a:9f:00	16.6.2s	WS-C3650-48TD-E	FDO1921E24W	View	ACCESS	~	EG	Feedbac
Show 50 ✓ entries				Showing 1 - 28 of 28					Previous	1 Next

Cisco Catalyst Center

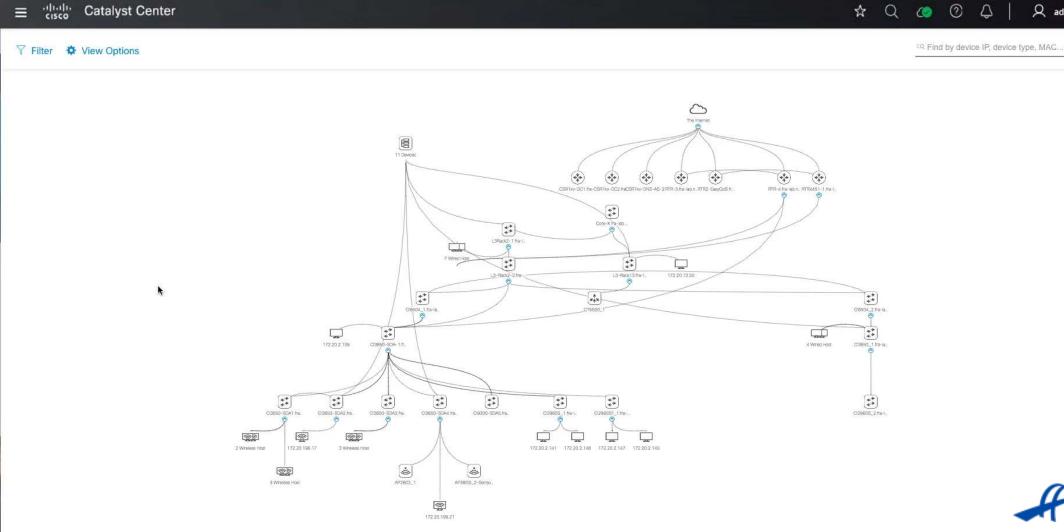
Showing 1 - 28 of 28

Previous 1 Next

Tools - Topology

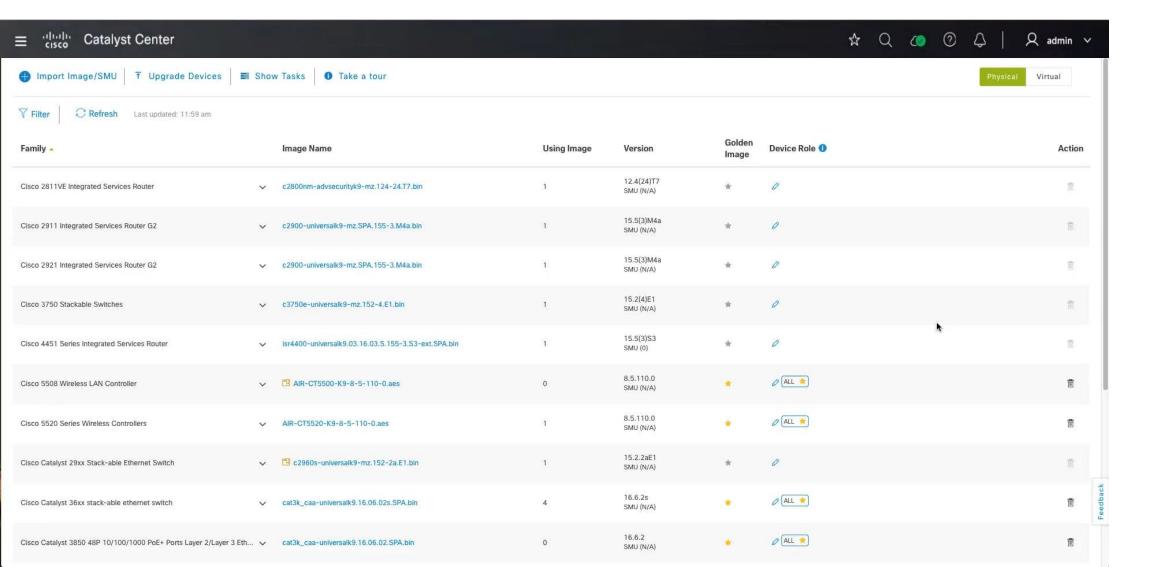


Q admin v





SWIM Software and Image Management



Catalyst 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



Catalyst Center Features – Network Plug and Play

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

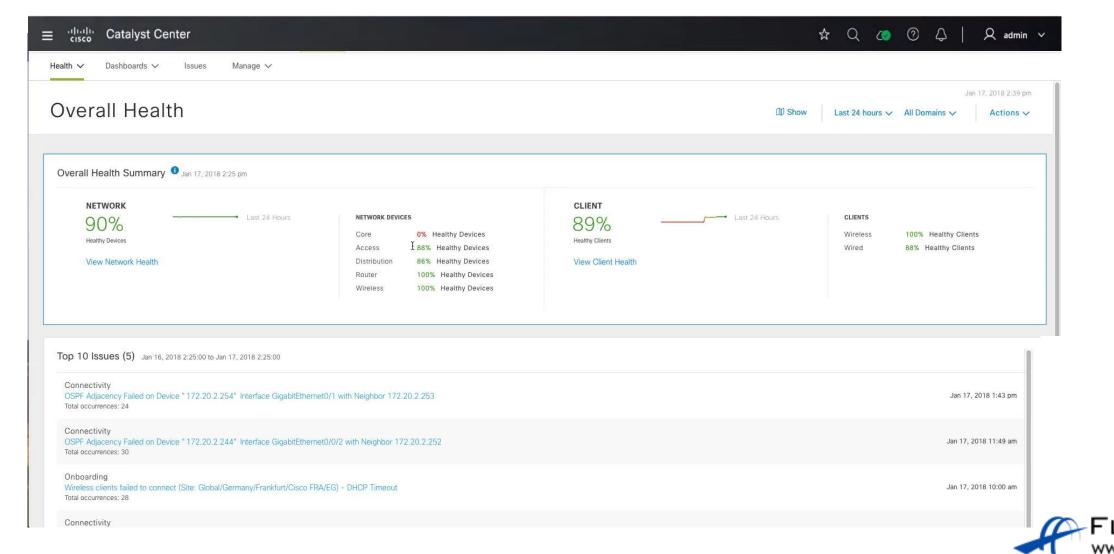


Assurance

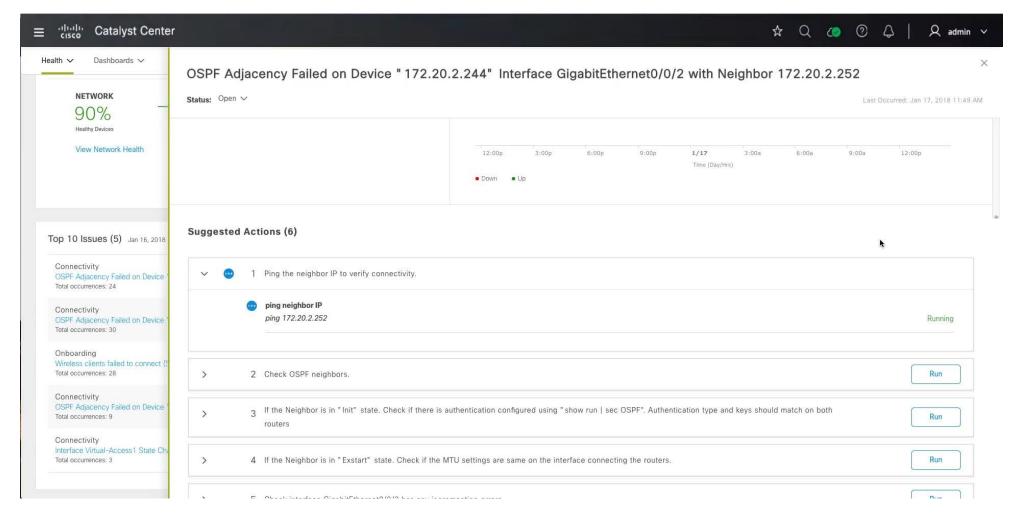
- Assurance guarantees that the infrastructure is doing what you intended it to do
- Catalyst Center receives information from all the network devices and ISE etc.
- Catalyst Center reports problems and provides recommended remediation actions.
- 'Al Network Analytics' uses Artificial Intelligence and Machine Learning enhanced capabilities



Assurance

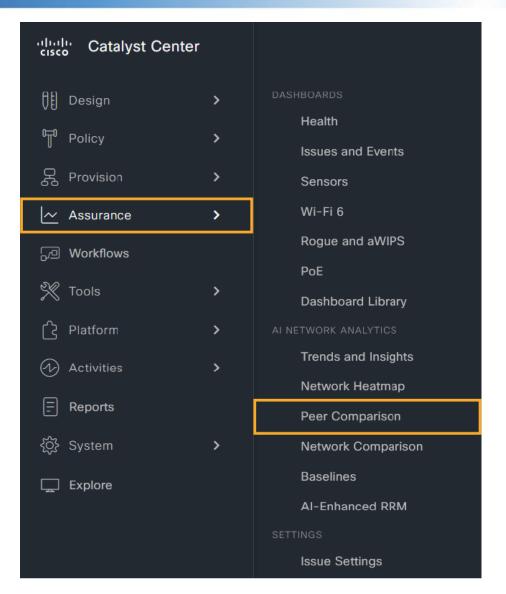


Assurance





Assurance – Peer Comparison



- Compares wireless network quality with comparable size peer networks
- KPIs include Received Signal Strength Indicator (RSSI), Radio Throughput and Onboarding Error Source



Assurance – Peer Comparison



SUMMARY

Comparing Roaming Error Source in your network to your peers in the past couple of months.

2.4

Network: The most common error is Network Association MaxStations

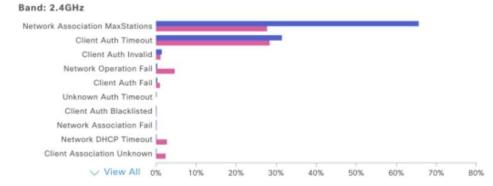
Peers: The most common error is Client Auth Timeout

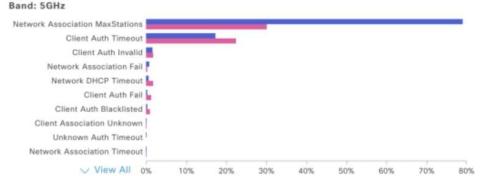
5 GHz Network: The most common error is Network Association MaxStations

Peers: The most common error is Network Association MaxStations

rimeout

Distribution of Roaming Error Source





Blue: you

Pink: peers



API Support

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

