



Say hello
to the future.

Cisco Connect 2019

Hanoi, Vietnam . 4 April 2019

#CiscoConnectVN



Delivering Network Automation & Assurance with AI and Machine Learning

Sanjay K Kundnani

Regional Manager, Cisco Systems

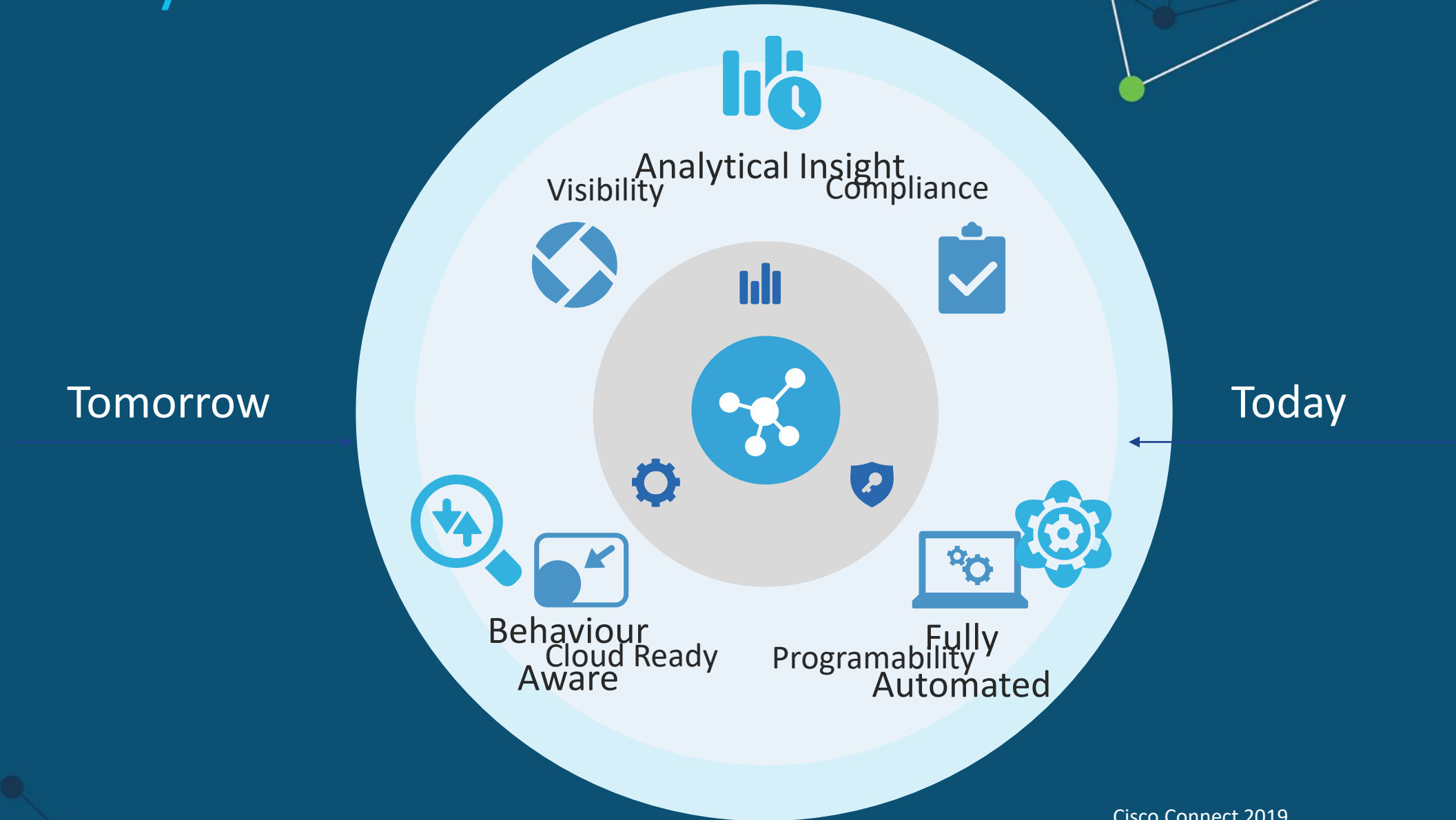
Yesterday's Networks

Yesterday's Network



Today

Today's Networks



High Network Costs

\$60B

Annually spent on
Network Operations,
Labor & Tools¹



95%

Network changes are
performed manually

75%

of Opex spent on changes
and troubleshooting

70%

of Policy Violations are
due to human errors



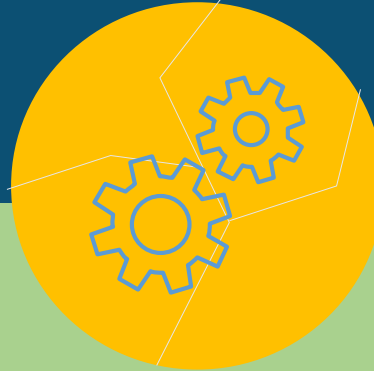
Key Challenges for Traditional Networks



Difficult to Segment

Ever increasing number of users and endpoint types

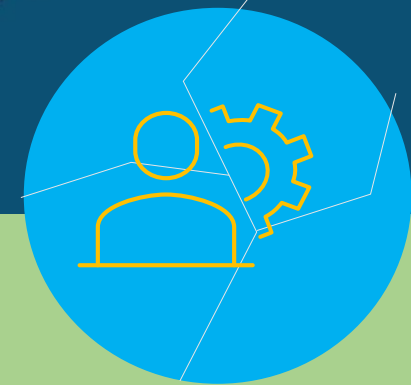
Ever increasing number of VLANs and IP Subnets



Complex to Manage

Multiple steps, user credentials, complex interactions

Multiple touch-points



Slower Issue Resolution

Separate user policies for wired and wireless networks

Unable to find users when troubleshooting

Traditional Networks Cannot Keep Up!

A Platform Approach



Platforms for Digital Business

Business Applications



Managed Services



Application Development



Integrations

Business Benefits and Differentiation

Software Agility



Automation



Policy



Analytics

Value beyond Connectivity

Core



Secure



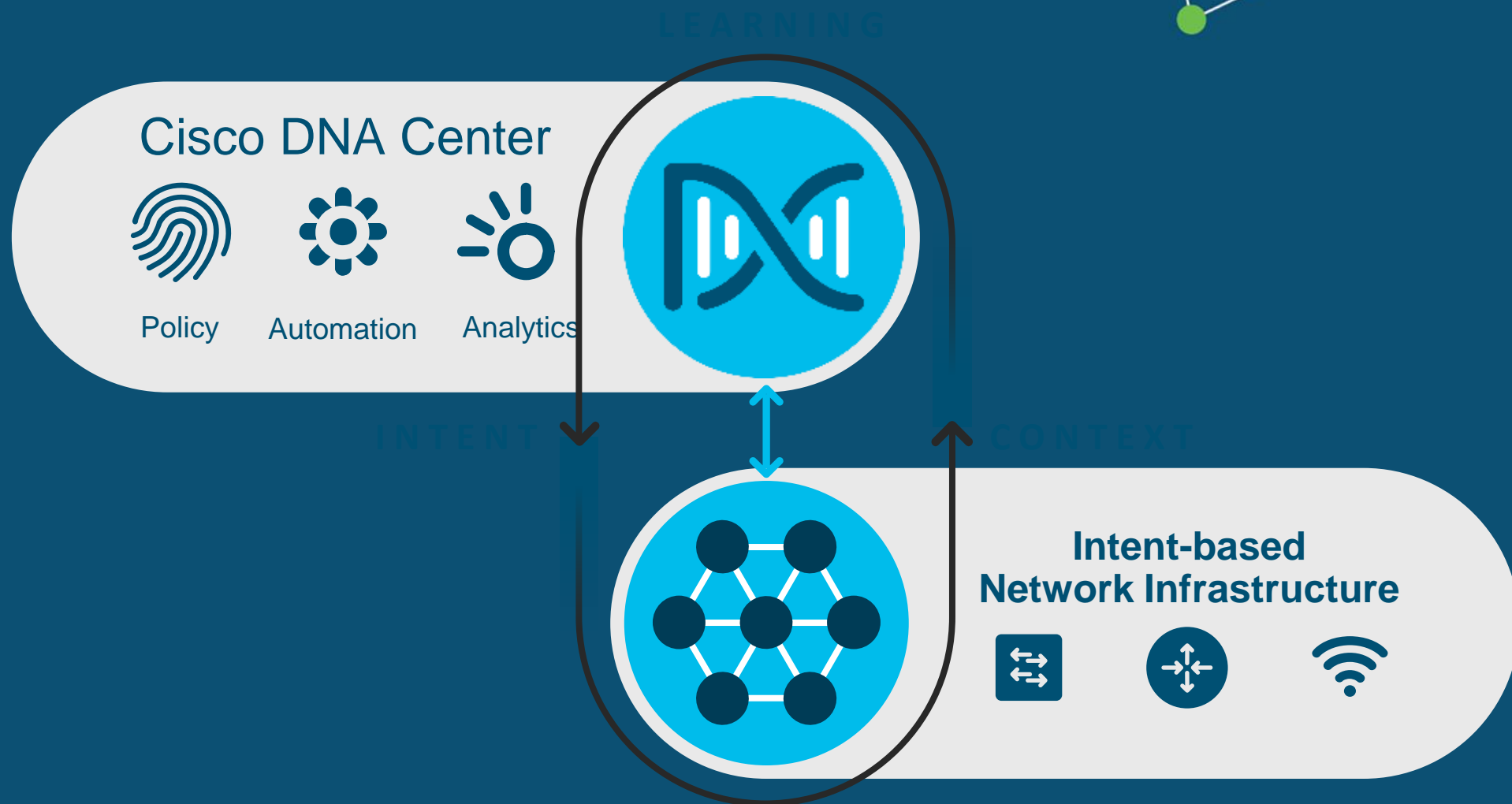
Resilient



Scalable

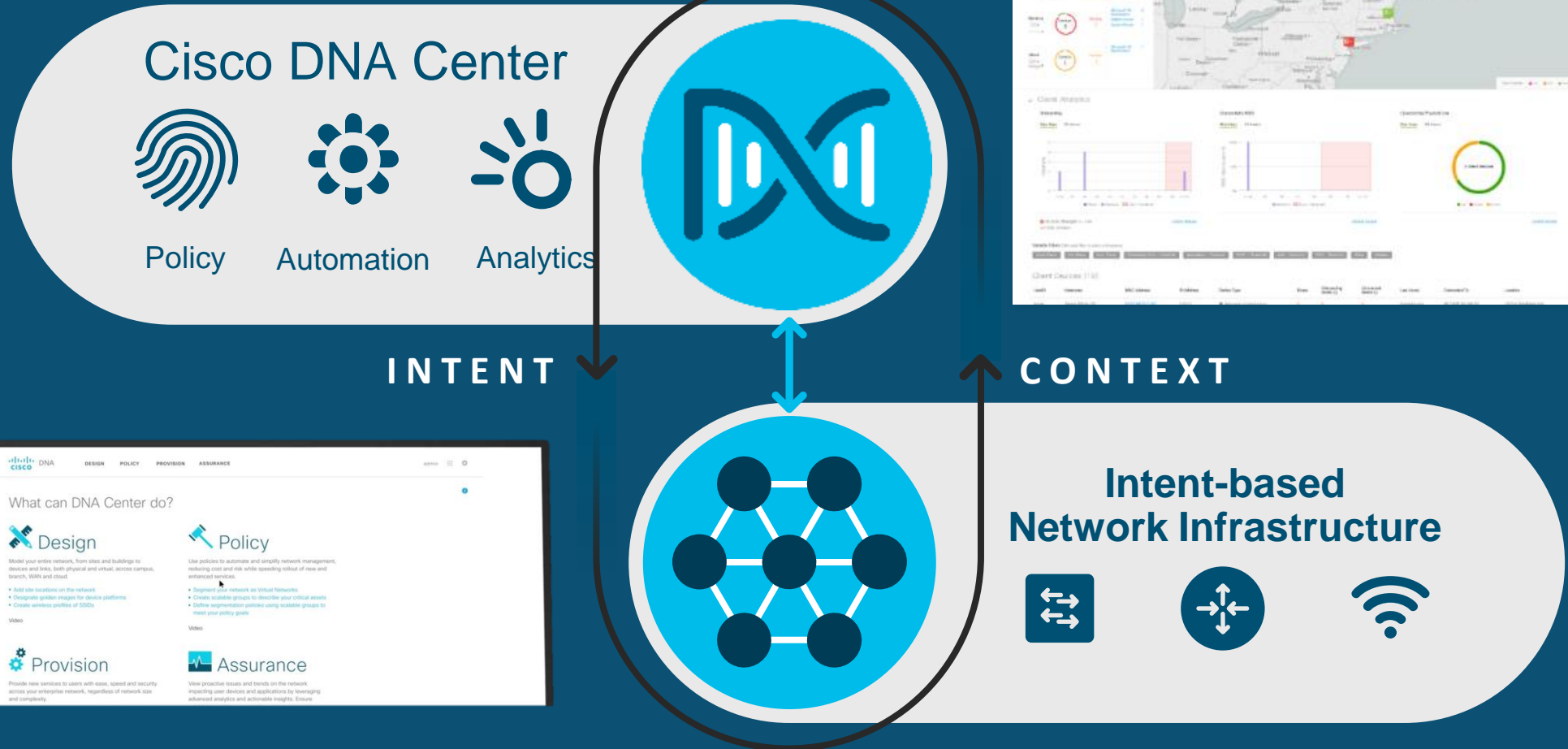
Intent-based Network Infrastructure

Cisco Intent Based Networking



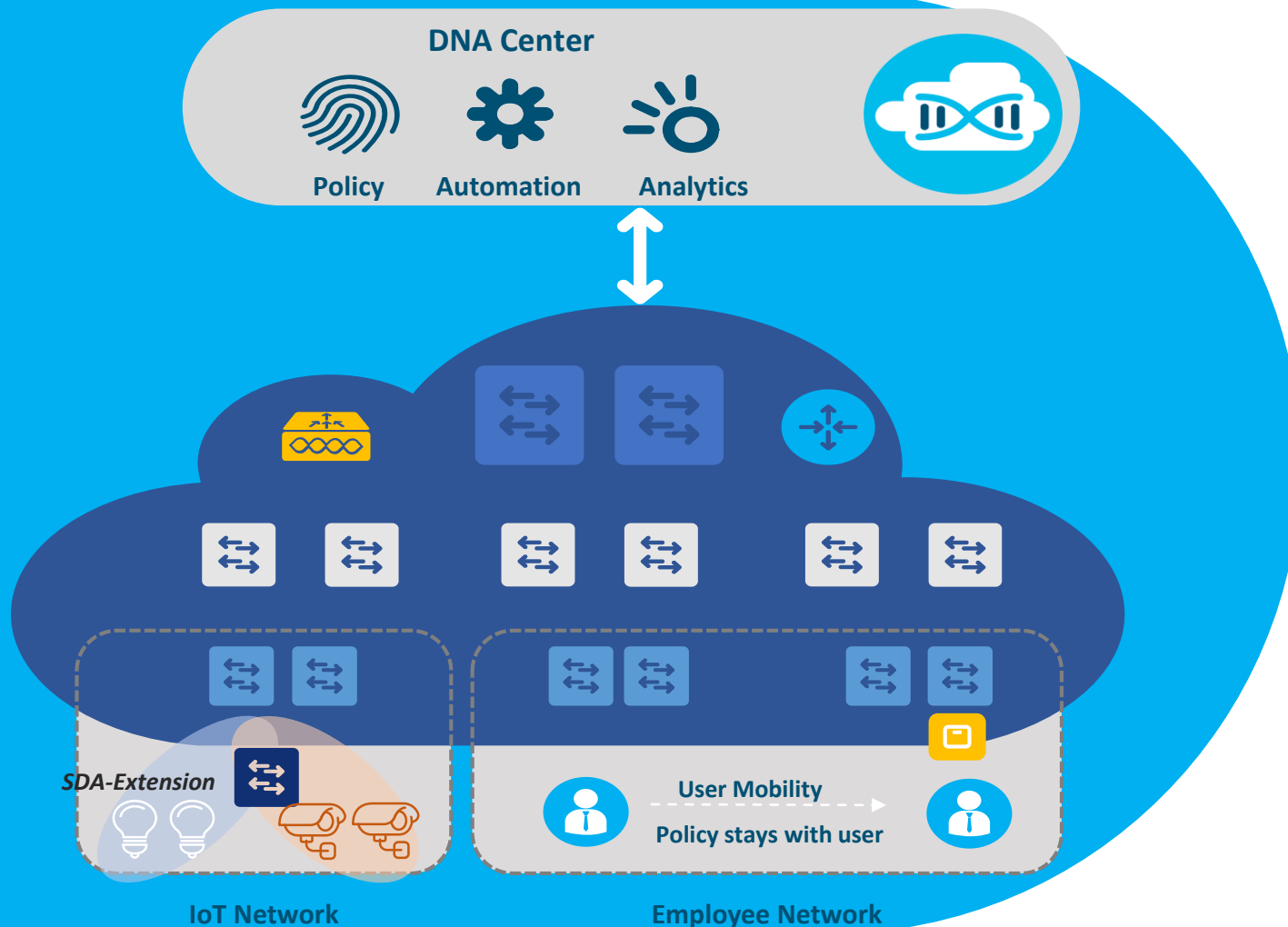
Cisco DNA Center

The Network Management and Command Center of Cisco DNA



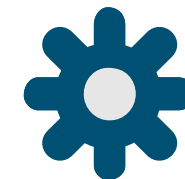
Cisco Software-Defined Access

Networking at the speed of Software!



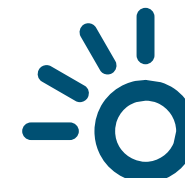
Identity-based Policy & Segmentation

Decoupled security policy definition from VLAN and IP Address



Automated Network Fabric

Single Fabric for Wired & Wireless with Workflow-based Automation

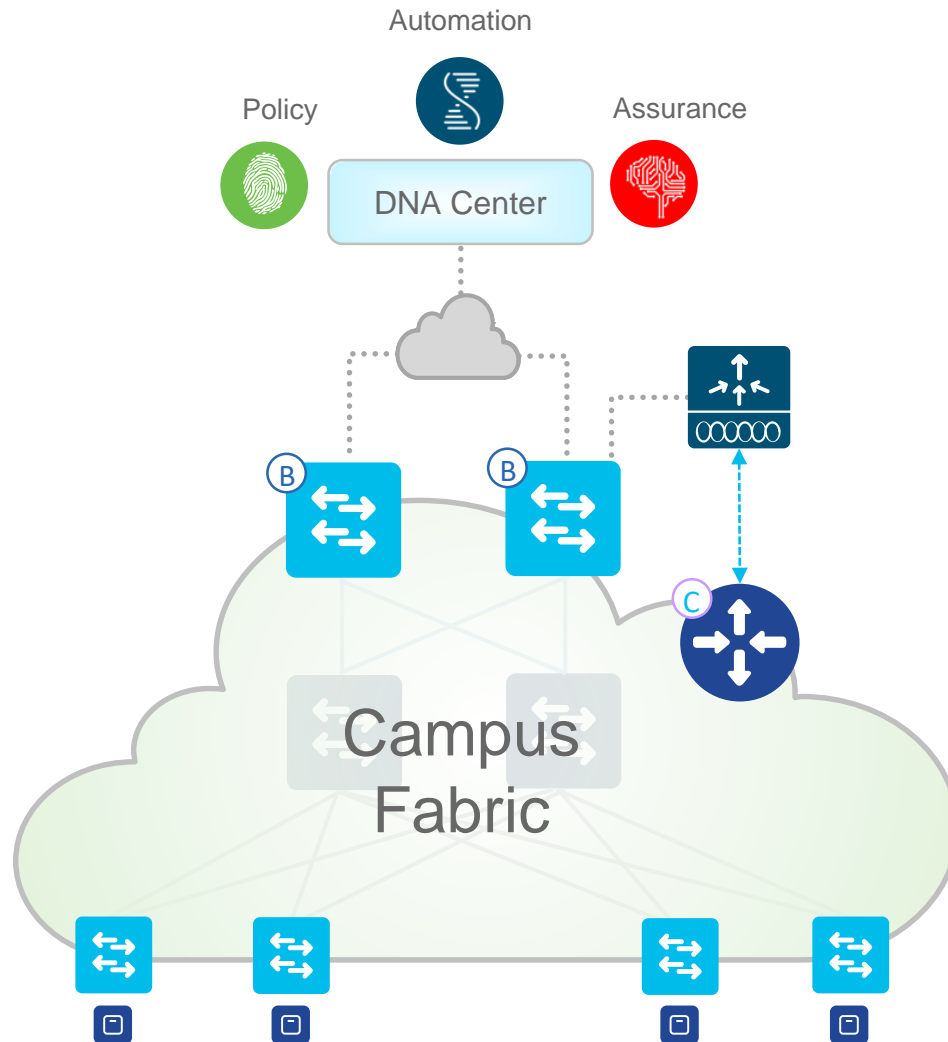


Insights & Telemetry

Analytics and insights into user and application behavior

What is SD-Access?

Campus Fabric + DNA Center (Automation & Assurance)



▪ SD-Access

GUI approach provides automation & assurance of all Fabric configuration, management and group-based policy

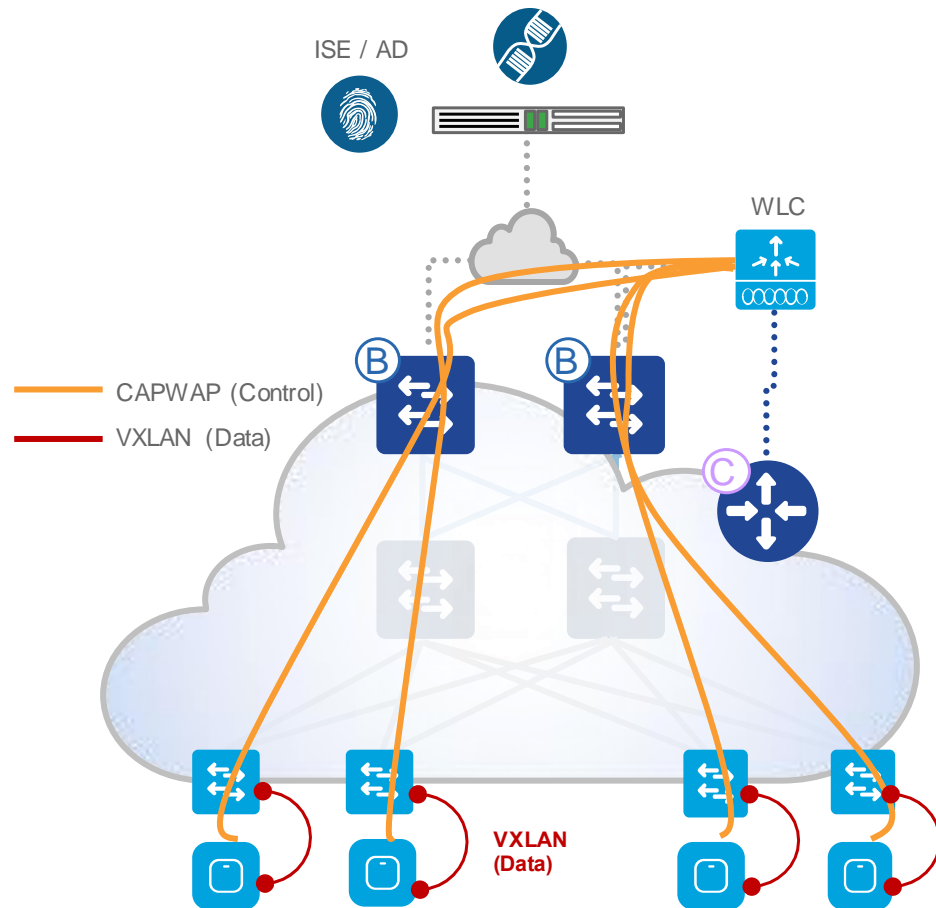
DNA Center integrates multiple systems, to orchestrate your LAN, Wireless LAN and WAN access

▪ Campus Fabric

An **Overlay network** is a **logical topology** used to **virtually connect** devices

Separated management systems

SD-Access Wireless – Fabric Enabled Wireless



One Consistent Policy with native segmentation

Wired/Wireless

Centralized Control Plane

Simple Operations

Centralized Management Plane

Easier Troubleshoot

Distributed Data Plane with L2 roam and easy IP addressing

Scale and Consistency

Improved Guest Access

Scale and Consistency

Software Defined Automation

Reduce the time and complexity in getting your network connected and doing what you intended it to do.

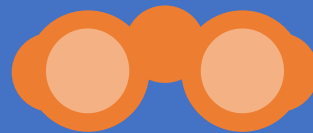
Deploy



Policy, Design, Provision,
Integrate Platforms

Successful IT
Rollouts

Manage



SW Image Management,
Changes, Routing, Security,
Compliance

Minimize Downtime,
User Productivity

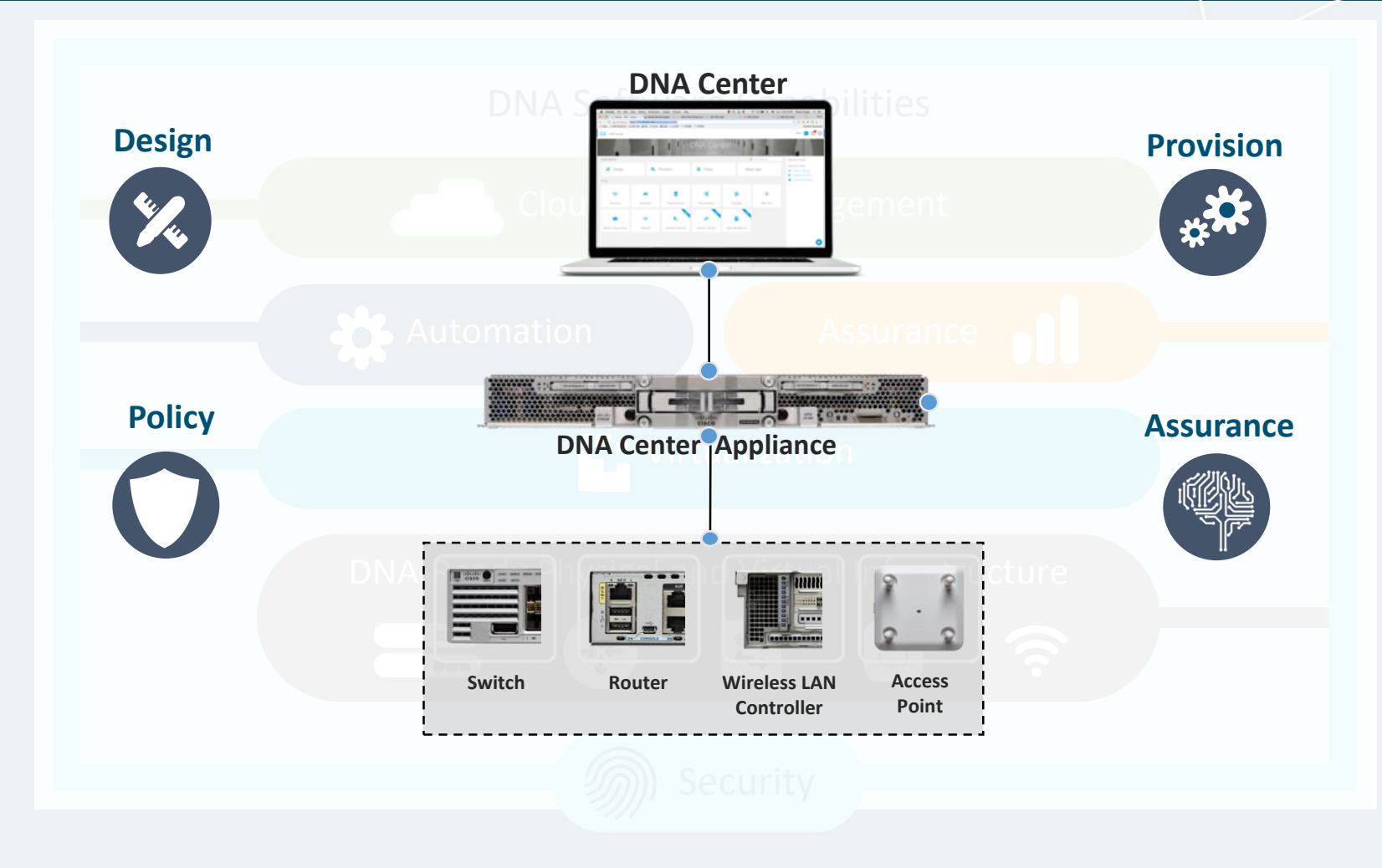
Assure



Guided Remediation,
Automated Updates,
System optimization

Network Intent
IT Productivity

Cisco DNA Center



Get your Intent-Based Network in Motion Today

Greenfield Network Savings



Policy

6 complex steps
reduced to two simple
clicks

Before



4 hours

Now



5 minutes



Design

12 find & define tasks
now auto-discover &
import.

Before

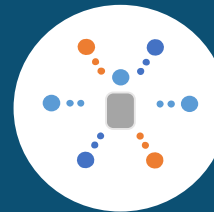


2 hours

Now



15 minutes



Provision

8 manual config steps
reduced to select &
drop.

Before



5 hours

Now



5 minutes



Savings

Workflow time per
device:

Before



11 hours

Now



25 minutes

Automated deployment of Network Devices

Direct Costs

- Pre-staging & Shipping costs
- Travel costs

Complexity

- Configuration errors
- Different products, IOS Releases

Security

- 3rd party not secure
- Rogue devices

Time/Productivity

- Manual process
- Shipping, Storage, Travel



Order Equipment



Staging Site



Manual Installer



Technician



Deploy device on site



Order Equipment



DNA Center Automation
With Plug & Play



Deploy device on site

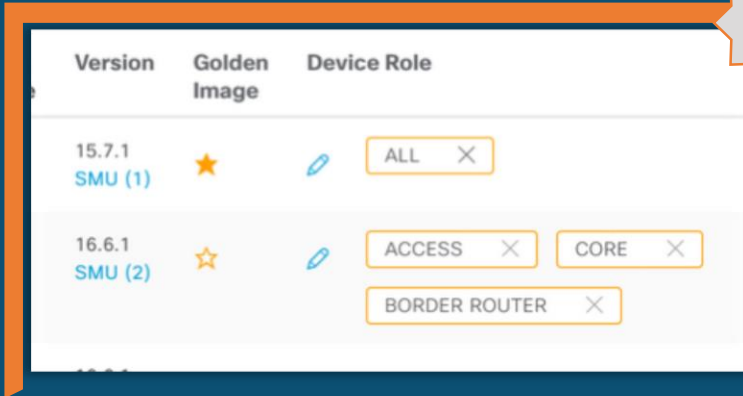
~50%

Day 0 OPEX Savings*

- Drop Ship devices
- Centralized device discovery (DHCP, DNS, Cloud)
- Non-technical installer at site
- Template based configurations
- Secure SUDI Authentication

Network Changes made Easy with SDA Automation

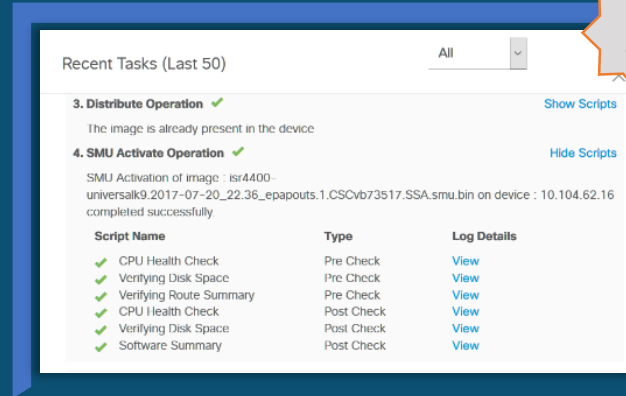
1



Intent based Network Upgrades

Intent based network upgrades allows for image standardization, much desired by all network admins.

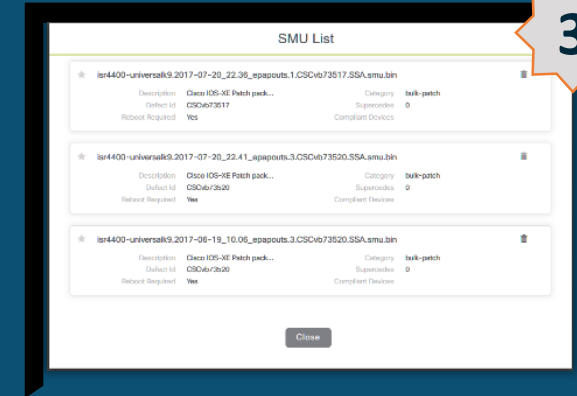
2



Upgrade Pre/Post Checks

Pre and post checks allows network admins more control and visibility over network upgrades

3



Patching Support

Patches are supported in DNA Center from intent to pre-post checks in same way we manage regular images

Software Image Management

Intent Based Network Upgrades



Captures your upgrade intent to automate process and drive consistency

Streamlined Upgrade Process



Upgrade base image, patches, and other add-ons in one single flow

Trustworthiness Integration

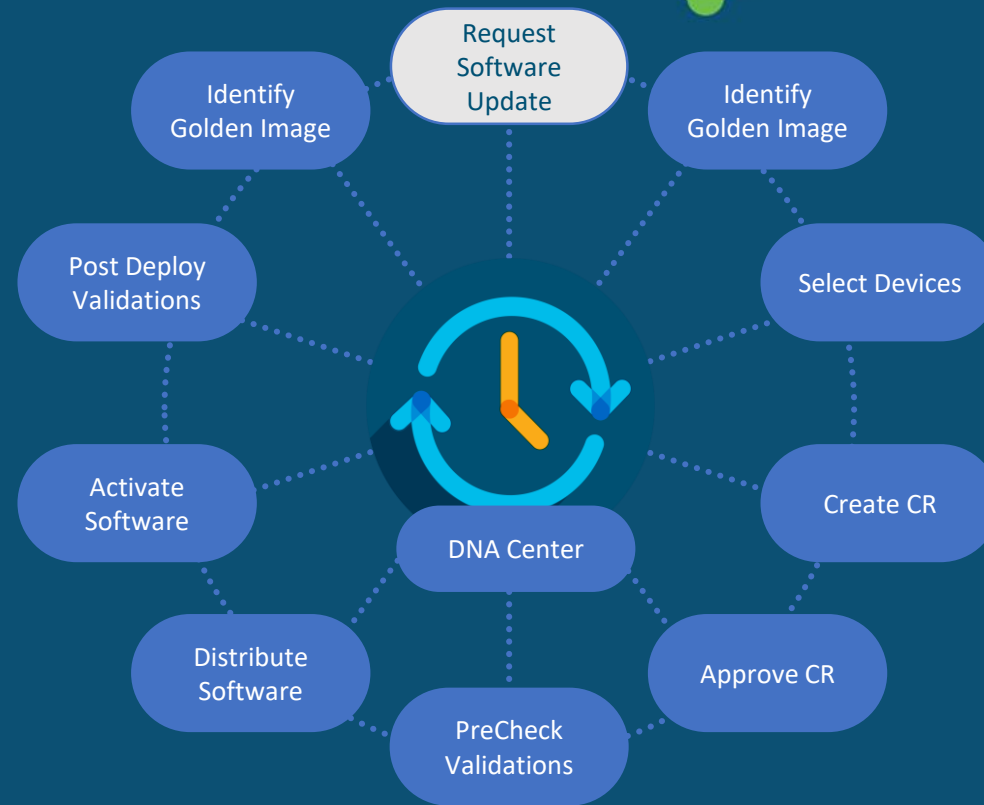


Assures that device images are not compromised in any way.

Patching Support



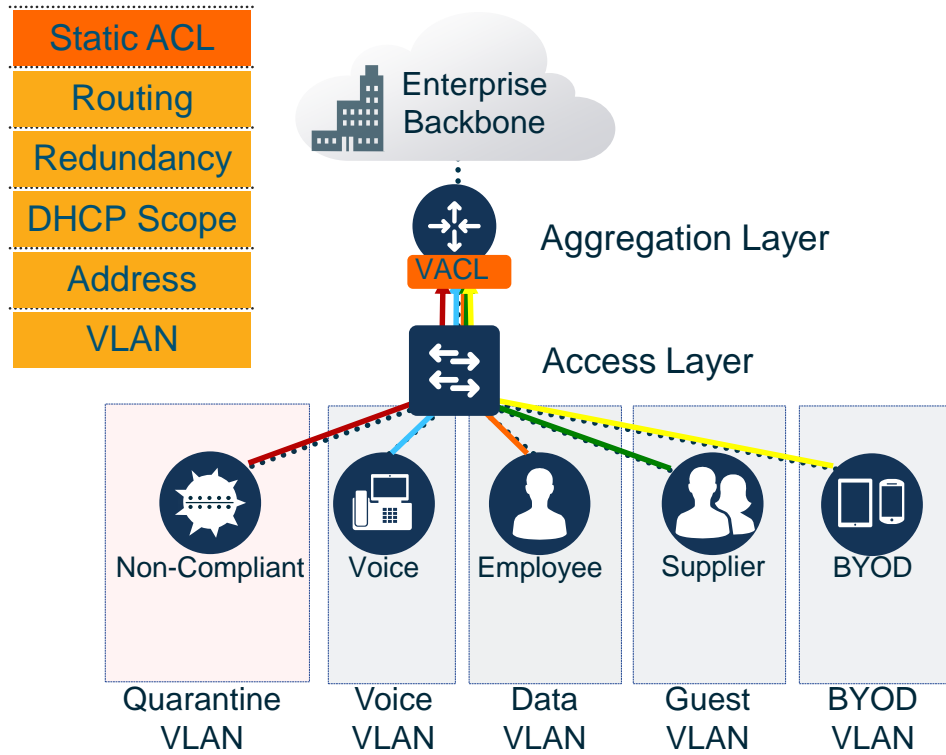
Pre/Post check ensures updates do not have adverse effects on network



Automate your software upgrade cycle

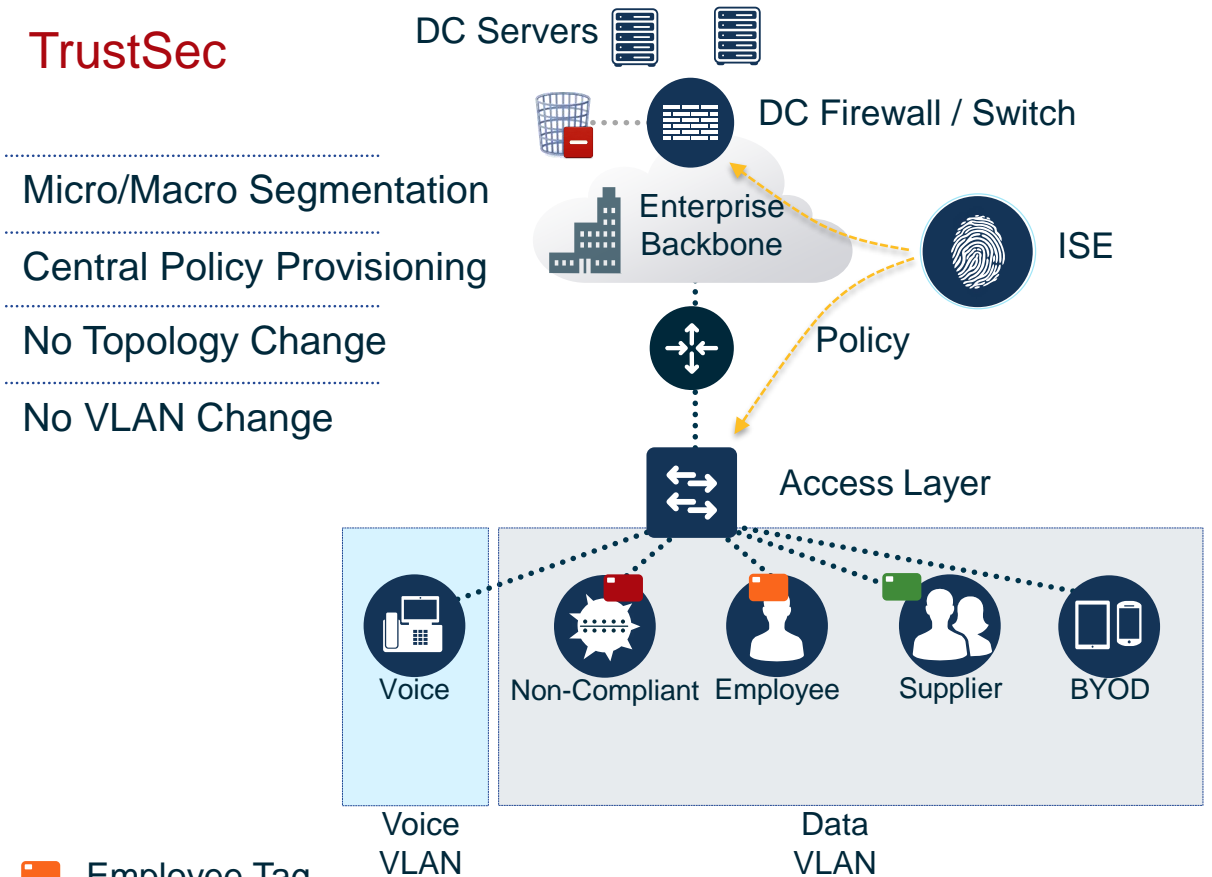
How SDA Simplifies Network Segmentation

Traditional Segmentation



Security Policy based on Topology
High cost and complex maintenance

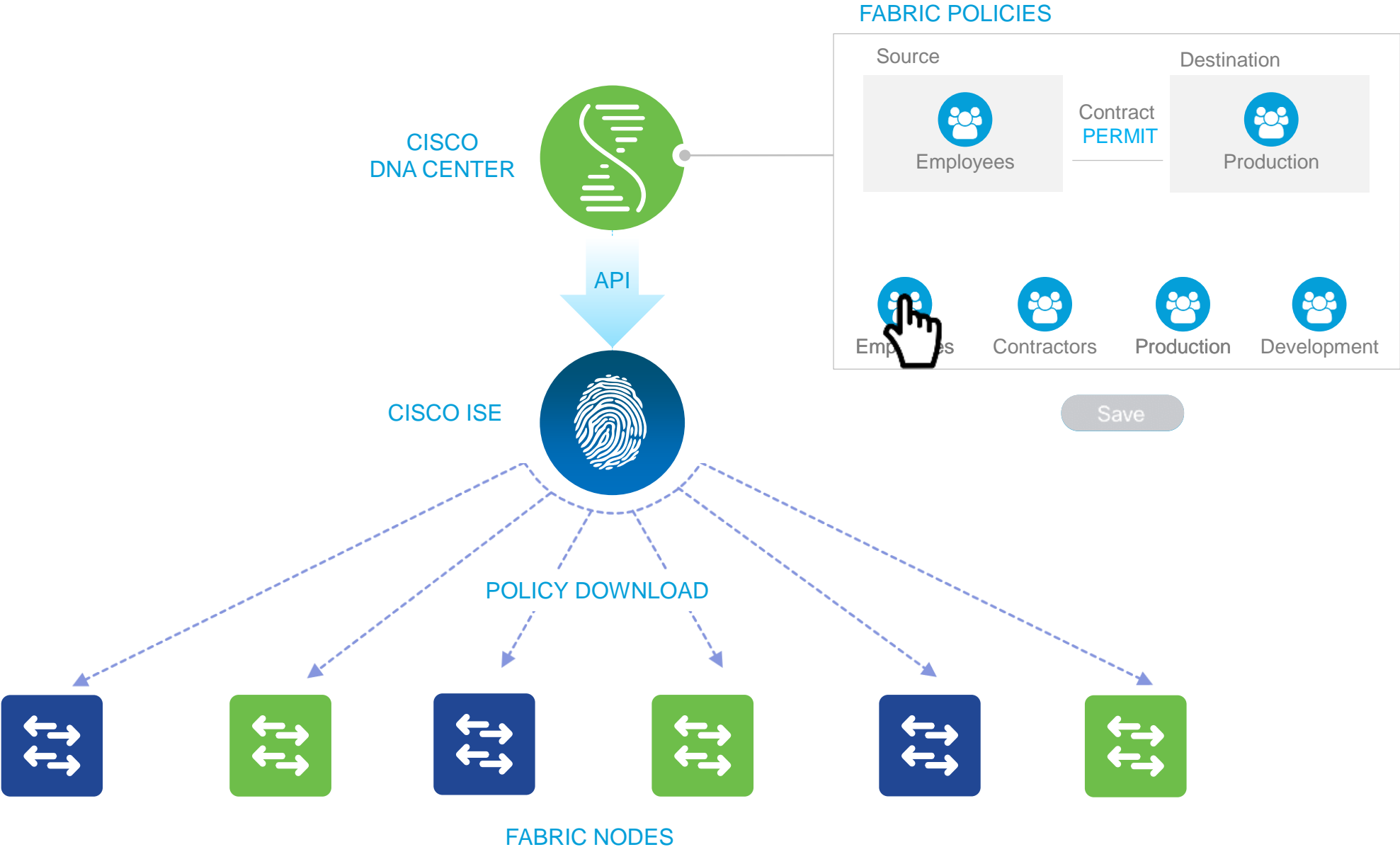
TrustSec



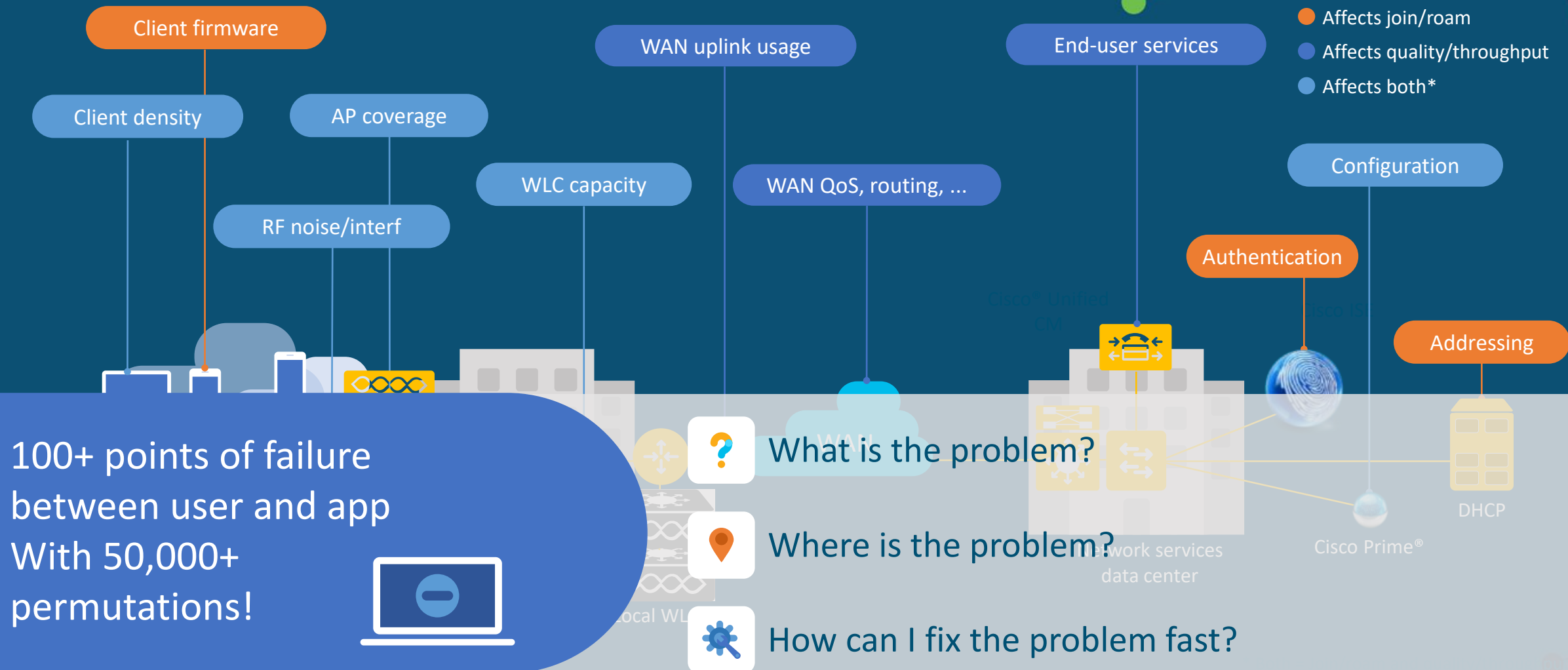
Micro/Macro Segmentation
Central Policy Provisioning
No Topology Change
No VLAN Change

Use existing topology and automate security policy to reduce OpEx

SDA Segmentation Policy Automation



Network Quality: a complex end-to-end problem



43%



of IT Time spent on Troubleshooting



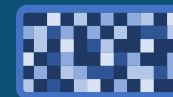
Data collection

Network operators spend **4x more time collecting data** than analyzing while troubleshooting



Replication challenge

It's **impossible for IT to troubleshoot** if they cannot replicate the issue or see it in real time



Slow resolution

Half of Wi-Fi issues take **more than 30 minutes to resolve**

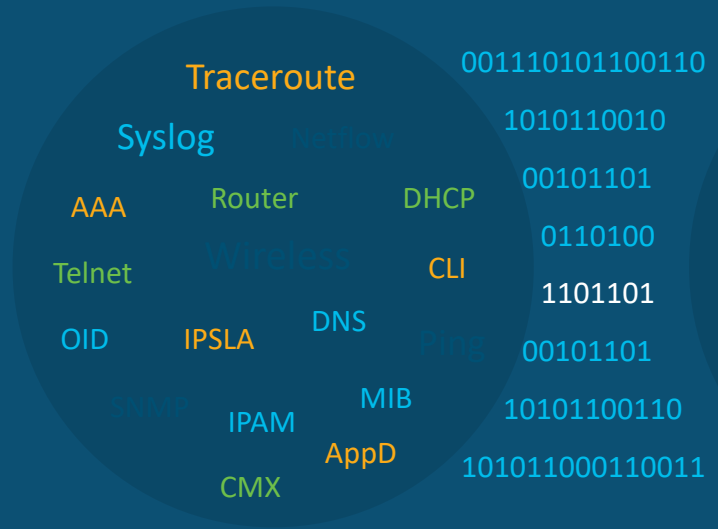
Cisco DNA Assurance

Network Telemetry
Contextual Data

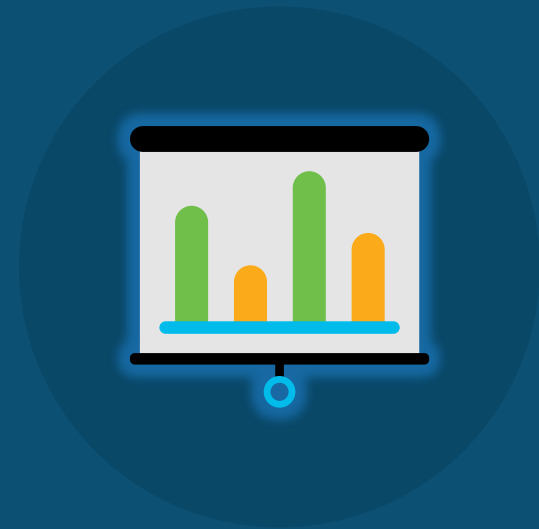
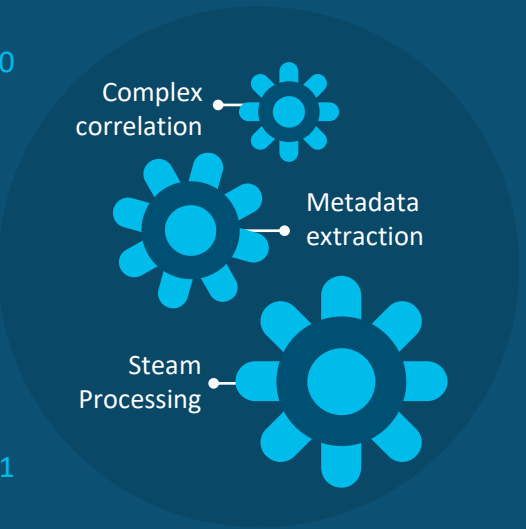
Correlation
Complex Event
Processing

Issues Insights

Guided Remediation



001110101100110
1010110010
00101101
0110100
1101101
00101101
10101100110
101011000110011



Telemetry and Sensors at Source
Clients | Applications | Wireless | Switching | Routing

Network Time Travel

History shows critical events and Identifies when issues occurred

Ability to go back in time when an issue is observed

All information in the relevant 360 page changes to that point of time

Go back in time to understand the network state when an issue occurred !!

The screenshot displays the Cisco Connect Client 360 interface. At the top, there are navigation tabs for Health, Dashboards, Issues, and Manage. The main header shows 'Client 360' with a time range of '24 Hours: Jan 26, 1:50 pm – Jan 27, 1:50 pm' and options for 'All Domains' and 'Intelligent Capture'. Below this, the client's name 'daphne.blake' is shown with a score of 10/10. A list of devices is displayed, including 'Daphne-iPad', 'LAPTOP-8DGBK756' (highlighted), 'B8:27:EB:CA:AA:88', and 'Daphne-iPhone'. The client's details include: Device: Microsoft-Workstation, OS: MSFT 5.0, MAC: 54:8C:A0:9E:92:99, IPv4: 10.30.100.30, IPv6: ::, VNID: 0, Status: Connected, Last seen: Jan 27, 2019 1:50 pm, and Connected Network Device: LA1-AP4800-1. A line graph shows the client's health score over time, with a notable dip at 2:20 am. Below the graph, a table of events is shown, with a highlighted event from Jan 27, 2019 2:20 am - 2:25 am. The event details include: Client Health: 4, Onboarding Status: Passed, Connectivity (RSSI, SNR, Data Rate, Tx, Rx), Connection Details (Status: Active, SSID: LA-Corporate-4800, AP: LA1-AP4800-1, Channel: 52 (20 MHz), Band: 5 GHz), and Major Events (Onboarding, Broadcast Rekey - KeyExchange Failed). A detailed event log at the bottom shows: 'P4 Onboarding Wireless client took a long time to connect (SSID: LA-Corporate-4800, AP: LA1-AP4800-1, Band: 5.0 GHz) - Excessive time for Authentication due to RF issues' occurring on Jan 27, 2019 10:05 am.

SDA Ready Platforms

SWITCHING

NEW

Catalyst 9200



NEW

Catalyst 9400



Catalyst 9300



NEW

Catalyst 9500



NEW



Catalyst 4500E



Catalyst 6K



Nexus 7700



Catalyst 3850 and 3650

ROUTING



ASR-1000-X



ASR-1000-HX



ISR 4430



ISR 4450



CSR 1000V

WIRELESS

NEW



Catalyst 9800



AIR-CT5520



AIR-CT8540



AIR-CT3504

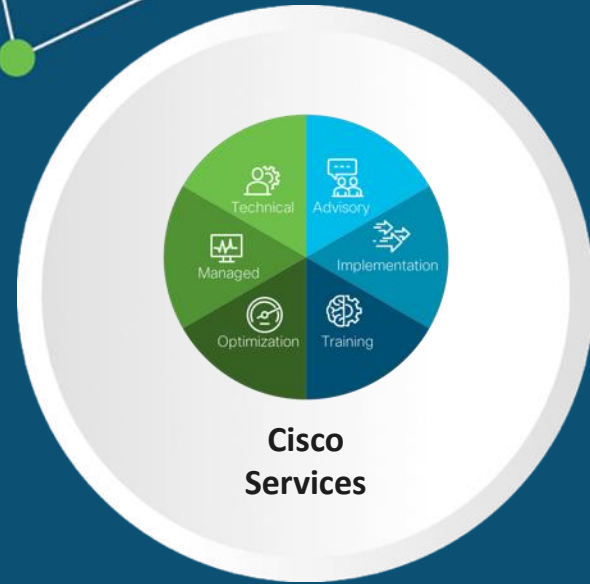
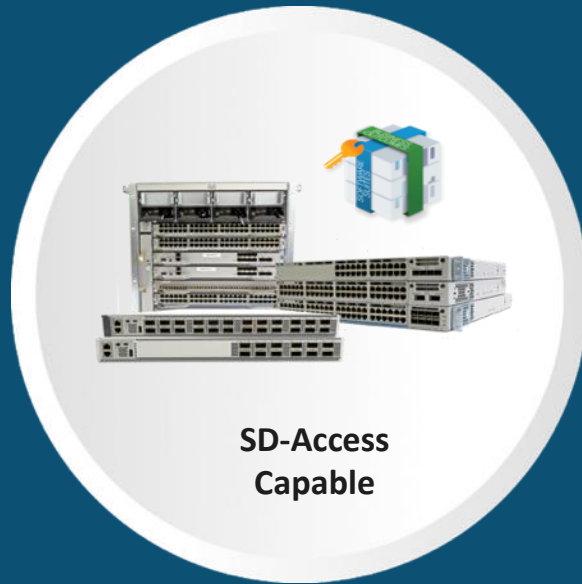


Wave 2 APs (1800, 2800,3800)



Wave 1 APs* (1700, 2700,3700)

What to Do Next?



Refresh your
Hardware & Software

Deploy the
Cisco DNA Center

Engage with
Cisco Services

Get **SD-Access Capable Devices**
with **Cisco DNA Advantage OS License**

Get **Cisco DNA Center Appliances**
with **Cisco DNA Center Software**

Cisco Services can help you
to **Test - Migrate - Deploy**



Cisco DNA Center Demo

Nguyen Tien Hoang

Systems Engineer

Cisco Systems Vietnam



Cisco Customer Experience (CX)

Professional Services

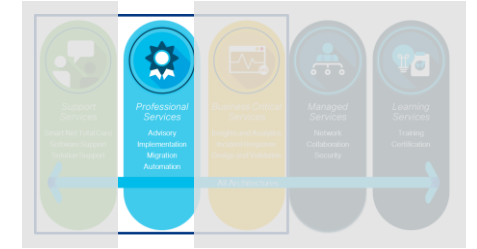
SDA Case Study

Jayvee Borja

Services Solutions Executive, Cisco Systems

Cisco Professional Services


Experts who speed time-to-value



Value of Cisco Engagement



Global Experience and Best Practices



Proven Methodology



Cutting Edge Expertise



Consultancy & Advisory

Envision your **roadmap**. Strategic advice from **advisory, assessment, consulting** to detailed **design** and **validation**



Implementation & Migration

Migrate and **deploy**. Expertise, tools, and processes to **de-risk & speed** deployment

Complementing Partner Capabilities

- Bridge to New Technologies
- Support Complex Solutions

➔ Consult, Advice, Implementation & Migration

SG FSI Customer Case Study – SDA

Customer's Challenge

- FSI customer's challenge is to transform from Traditional to Secured Software Defined Network with agility, consistency and faster provisioning capabilities

Proposed Solutions

- Secured automated network to discover and provision elements including switches, access points, wireless LAN controllers
- Security posturing, interoperability with existing 3rd party solution ForeScout
- Segmentation of users and applications by Business functions using Security Group Tag to allow context aware traffic segregation
- Assurance Analytics and Proactive monitoring with guided troubleshooting

Impact on Customer

- Faster users and services provisioning with reduced downtime from human errors
- Improved Security and Compliance
- Single Policy Dashboard for Wired and Wireless networks
- Seamless campus mobility and location independent policy enforcement for users
- Simplified troubleshooting with faster time to restore



Say hello
to the future.

Cisco Connect 2019

Hanoi, Vietnam . 4 April 2019

#CiscoConnectVN