Cisco Connect 2018
IT's All You
Singapore
27 March 2018
#ciscoconnectSG
Cisco Software Defined Access (SDA)

Transformational Approach to Network Design & Provisioning

Sanjay Kumar
Regional Manager- ASEAN, Cisco Systems
What is network about?

In the past...
- Voice
- Video
- Data

Today...
- Mobility
- Cloud
- IOT
- Security

What really matters !!!
The Challenge.

“I want to design and deploy a network.”

Platform choices

Best practices

Design options

Future ready

On time

Within budget

Manageable

Within budget
Typical Traditional Campus

Very powerful and feature rich but:
- Complex to operate
- Difficult to scale
- Difficult to secure
- Inflexible and closed architecture
- And you manage it all with CLI…
Traditional Network Design & Build Work Flow

Spanning Tree Protection across the LAN

Global LAN Switch Configuration

Uplink Interfaces

Mgmt VLAN 30

Voice VLAN 20

Data VLAN 10

Client Facing Interfaces

Access Layer Virtual LANs

spanning-tree mode rapid-pvst
spanning-tree portfast bpduguard default
udld enable
errdisable recovery cause all
vtp mode transparent
load-interval 30

access-list 55 permit 10.4.48.0 0.0.0.255
line vty 0 15
  access-class 55 in

! snmp-server community [SNMP RO] RO 55
snmp-server community [SNMP RW] RW 55

ntp server 10.4.48.17
ntp update-calendar
!
clock timezone PST -8
clock summer-time PDT recurring
!
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime

vlan 10
  name Data
vlan 20
  name Voice
vlan 30
  name Management

SNMPv2c access
How we build Traditional Network

Manually
Repetitive Steps

Box by Box
Manual | Error Prone

CLI
Skill | Time | Effort

ip domain-name cisco.local
no ip http server
ip http secure-server
ip ssh version 2
ip scp server enable
line vty 0 15
  transport input ssh
  transport preferred none
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!
Software-Defined Access
Networking at the speed of Software!

DNA Center
Policy Automation Analytics

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

SDA-Extension
User Mobility
Policy stays with user

IoT Network
Employee Network

CISCO CONNECT 2018 . IT’S ALL YOU
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.
Software-Defined Access

DNA Center: Simple Workflows

DNA Center

Solution Components

Automation  Assurance  Policy

Routers  Switches  Wireless AP  WLC

DESIGN  PROVISION  POLICY  ASSURANCE
SDA Network Design & Build Work Flow

Design
Network Hierarchy
Network Settings
Image Management
Network Profiles

Policy
Virtual Networks
Access Control
Application Priority
SDA Network Design & Build Work Flow

Provision
- Device Onboarding
- Host Onboarding
- Device Inventory
- Fabric Administration

Assurance
- Network Health Score
- Client 360
- Device 360
- Application 360
Network Segmentation Policy Rollout Today

1. Define Groups in AD
2. Define Policies
   - VLAN/subnet based
3. Implement VLANs/Subnets
   - Create VLANs
   - Define DHCP scope
   - Create subnets and L3 interfaces
4. Implement Policy
   - Define ACLs
   - Apply ACLs
5. Many different User Interfaces

What if You Need to Add Another Group & Policy?
How SDA Simplifies Network Segmentation

Traditional Segmentation

- Static ACL
- Routing
- Redundancy
- DHCP Scope
- Address
- VLAN

Security Policy based on Topology
High cost and complex maintenance

Access Layer

- Voice VLAN
- Data VLAN
- Guest VLAN
- BYOD VLAN

Enterprise Backbone

Aggregation Layer

VA CL

Non-Compliant

Voice

Employee

Supplier

BYOD

Quarantine VLAN

TrustSec

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

Access Layer

DC Firewall / Switch

ISE

DC Servers

Policy

Employee Tag

Supplier Tag

Non-Compliant Tag

Use existing topology and automate security policy to reduce OpEx

Voice VLAN

Non-Compliant

Employee

Supplier

BYOD

Data VLAN

Voice

Employee

Supplier

BYOD

CISCO CONNECT 2018 . IT'S ALL YOU
SDA Ready Platforms

**SWITCHING**
- Catalyst 9400
- Catalyst 9300
- Catalyst 9500
- Catalyst 4500E
- Catalyst 6K
- Nexus 7700
- Catalyst 3850 and 3650

**ROUTING**
- ASR-1000-X
- ASR-1000-HX
- ISR 4430
- ISR 4450
- CSR 1000V

**WIRELESS**
- AIR-CT5520
- AIR-CT8540
- AIR-CT3504
- Wave 2 APs (1800, 2800, 3800)
- Wave 1 APs* (1700, 2700, 3700)

*with Caveats
Catalyst 9000 Platform
World’s Most Advanced Enterprise Switches

Catalyst 9400
Modular Access

Catalyst 9300
Fixed Access

Catalyst 9500
Fixed Core

Programmable
Integrated Security
IoT Ready

Mobile Ready
Cloud Ready
Design
Gaining Momentum with the Catalyst 9000!

4000+ Customers

Wins

BRIDGEMAKER
Children's Hospital Los Angeles
Purdue University Calumet
Providence Health Plan

CISCO CONNECT 2018 . IT'S ALL YOU
Some Early Recognitions…
Catalyst 9300

New Generation of Fixed Access

- 2.5G at the Price of 1G
- 40G at the Price of 10G
- Only Stackable Switch with 8X 10G Uplinks
- Highest 2.5G/mGig Density in the Industry

Catalyst 9K Leadership

- UADP 2.0
- Open IOS-XE
- SD-Access
- X86 CPU & Containers
- Encrypted Traffic Analytics (ETA)*
- 256 bit MACSEC*
- Trustworthy Systems
- StackWise Virtual*
- IEEE1588 & AVB*
- NBAR2
- Perpetual/Fast PoE
- Model Driven Programmability
- Patching/GIR
- Streaming Telemetry

Modular Fans

Modular Uplinks

Modular Power Supplies

- 8x10G
- 2x40G
- 4x mGig
- 4x1G
- 350W
- 715W
- 1100W

Highest 2.5G/mGig Density in the Industry

24 Ports

1G Data

1G UPOE/POE+

mGig UPOE

48 Ports
Catalyst 9400
New Generation of Modular Access

Industry’s Highest PoE Scale

4-Slot*

7-Slot

10-Slot

Redundancy is now Table-stake

Catalyst 9K Leadership
- UADP 2.0
- Open IOS-XE
- SD-Access
- X86 CPU & Containers
- Encrypted Traffic Analytics*
- 256 bit MACSEC*
- Trustworthy Systems
- StackWise Virtual*
- IEEE1588 & AVB*
- NBAR2
- Perpetual PoE*
- Model Driven Programmability
- Patching/GIR
- Streaming Telemetry*

* not available at FCS
Catalyst 9500
New Generation of Purpose Built Fixed Core/Aggregation

- 40G at the Price of 10G
- 8X Buffering vs. Competition
- Industry's First 40G Enterprise Switch

Catalyst 9500-40X
Catalyst 9500-24Q
Catalyst 9500-12Q

Catalyst 9K Leadership
- UADP 2.0
- Open IOS-XE
- SD-Access
- X86 CPU & Containers
- Encrypted Traffic Analytics*
- 256 bit MACSEC*
- Trustworthy Systems
- StackWise Virtual
- IEEE1588 & AVB*
- NBAR2
- Model Driven Programmability
- Patching/GIR
- Streaming Telemetry*
Catalyst 9500
Granular Port Densities to Address all Campus Sizes

12Px40G

24Px40G

40Px10G + 8Px10G / 2Px40G
The Journey to the Software Defined Access (SDA)

Secure Foundation
Rapid threat detection and mitigation

Analytics for Assurance
Predictive performance with machine learning

Infrastructure Readiness
Open and Programmable

Policy Based Automation
Simplify, scale network deployment for Cloud, Mobile, IoT

Intent-based Network
Constantly learning, adapting, protecting

Software-Driven Innovation
Cisco Connect 2018

IT's All You

Singapore

27 March 2018

ciscoconnectSG