cisco Live!

Let's go

#CiscoLive

The bridge to possible

Modern Network Automation and Orchestration at Mass Scale

A Real-World Case Study

Bryn G Pounds (BGP) – Principal Architect Cisco Global Enterprise
@BrynPounds

BRKOPS-2827

Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

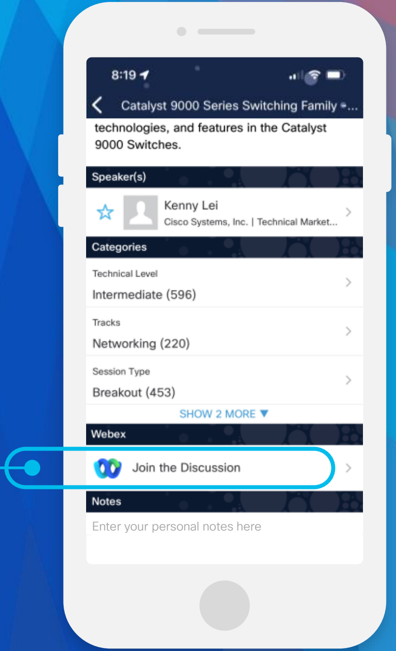
1 Find this session in the Cisco Live Mobile App

2 Click “Join the Discussion”

3 Install the Webex App or go directly to the Webex space

4 Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-2827

Agenda

What does the Journey Look like?

- Network Profile
- The Starting Point *(Technical **AND** Organizational)*
- Tool Selection Process
- What was Built
- Migration from then to now
- MOST IMPORTANT LESSONS LEARNED
- Conclusions

What can grilling teach us about Network Automation?

A LOT!

- Hungry Family Buy in. **Willing to invest** in more than a microwave dinner.
- Traeger? Big Green Egg? **Right tool(s) for the right job(s)**.
- What do we want to grill? Agree on the **success criteria**.
- Reverse Sear – **Changing processes.** Pull when it's done – not after 6 min.
- Is the BBQ steady at 225 degrees? **Visibility – Compliance.**
- Pushing through the stall. **Be patient through change.**
- Resting. See it through to **completion for the agreed results**?
- Satisfied family = **Met or exceeded approval criteria**.

The DIY Network Profile

(Examples of…) The DIY Network Profile

Universities… European Rail Systems…. Web & Service Providers…

30+ Years of Networking

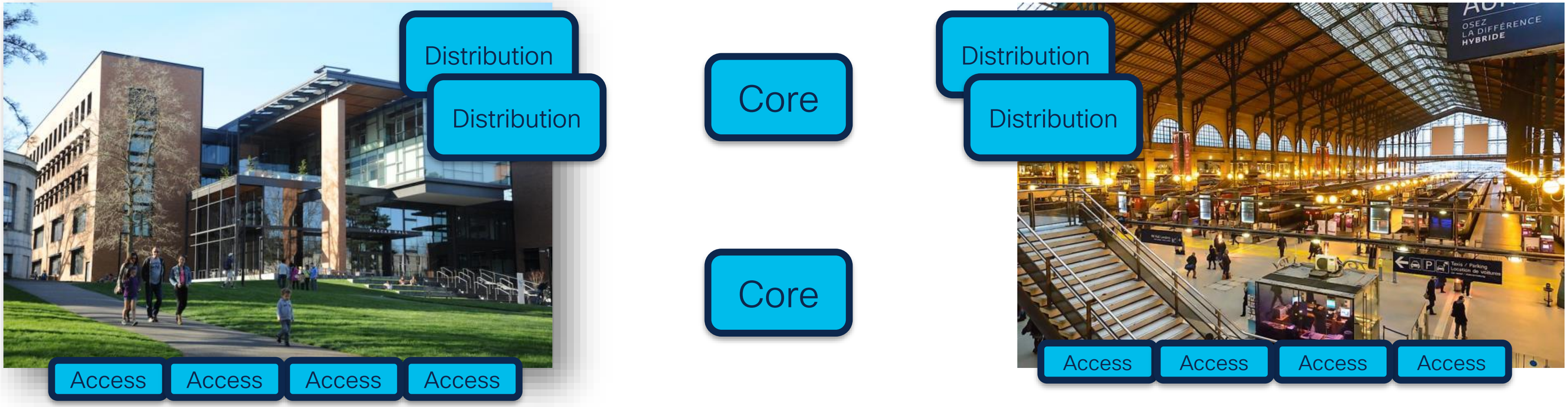
20'ish Schools & 200 buildings, each with "unique" requirements. (…almost like small cities)

- IT Delegation a requirement
- Multiple Vendors a constant
- Diverse Management Tools

4000+ Access Switches
100's of Distribution Switches
16,000 Access Points

Common Designs

Common Core. Distribution to the building / Station.



Distribution
Distribution
Access
Access
Access
Access

Core
Core

Distribution
Distribution
Access
Access
Access
Access

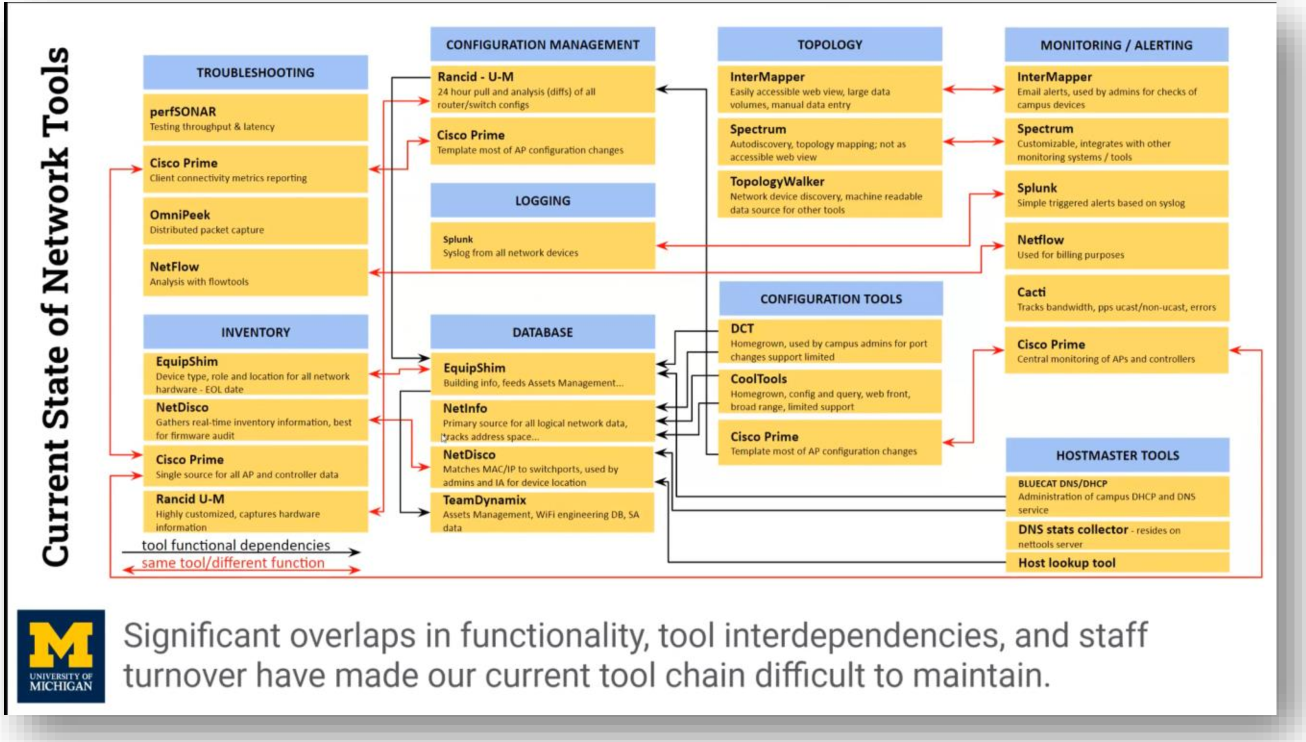
Network Organization: The Starting Point…

- Traditional Network Architecture and Operations Teams
  - Staff manually logging into devices. (Human Error & Config Drift)
  - Staff member would “win the lottery” and leave. (Loss of “tribal knowledge”)
  - Experts spending lots of time on menial tasks, rather that solving “fun” problems
  - **Time spent “configuring network devices”. Not “deploying network services”.**
  - Difficult to control delegated network support where required.

- Minimal Software / Automation / Orchestration Experience

Network Management: Where they Started….

(Don’t worry about trying to understand this)



Current State of Network Tools

TROUBLESHOOTING

- **perfSONAR** Testing throughput & latency
- **Cisco Prime** Client connectivity metrics reporting
- **OmniPeek** Distributed packet capture
- **NetFlow** Analysis with flowtools

INVENTORY

- **EquipShim** Device type, role and location for all network hardware - EOL date
- **NetDisco** Gathers real-time inventory information, best for firmware audit
- **Cisco Prime** Single source for all AP and controller data
- **Rancid U-M** Highly customized, captures hardware information

CONFIGURATION MANAGEMENT

- **Rancid - U-M** 24 hour pull and analysis (diffs) of all router/switch configs
- **Cisco Prime** Template most of AP configuration changes

LOGGING

- **Splunk** Syslog from all network devices

DATABASE

- **EquipShim** Building info, feeds Assets Management…
- **NetInfo** Primary source for all logical network data, tracks address space…
- **NetDisco** Matches MAC/IP to switchports, used by admins and IA for device location
- **TeamDynamix** Assets Management, WiFi engineering DB, SA data

TOPOLOGY

- **InterMapper** Easily accessible web view, large data volumes, manual data entry
- **Spectrum** Autodiscovery, topology mapping; not as accessible web view
- **TopologyWalker** Network device discovery, machine readable data source for other tools

CONFIGURATION TOOLS

- **DCT** Homegrown, used by campus admins for port changes support limited
- **CoolTools** Homegrown, config and query, web front, broad range, limited support
- **Cisco Prime** Template most of AP configuration changes

MONITORING / ALERTING

- **InterMapper** Email alerts, used by admins for checks of campus devices
- **Spectrum** Customizable, integrates with other monitoring systems / tools
- **Splunk** Simple triggered alerts based on syslog
- **Netflow** Used for billing purposes
- **Cacti** Tracks bandwidth, pps ucast/non-ucast, errors
- **Cisco Prime** Central monitoring of APs and controllers

HOSTMASTER TOOLS

- **BLUECAT DNS/DHCP** Administration of campus DHCP and DNS service
- **DNS stats collector** - resides on nettools server
- **Host lookup tool**

tool functional dependencies

same tool/different function

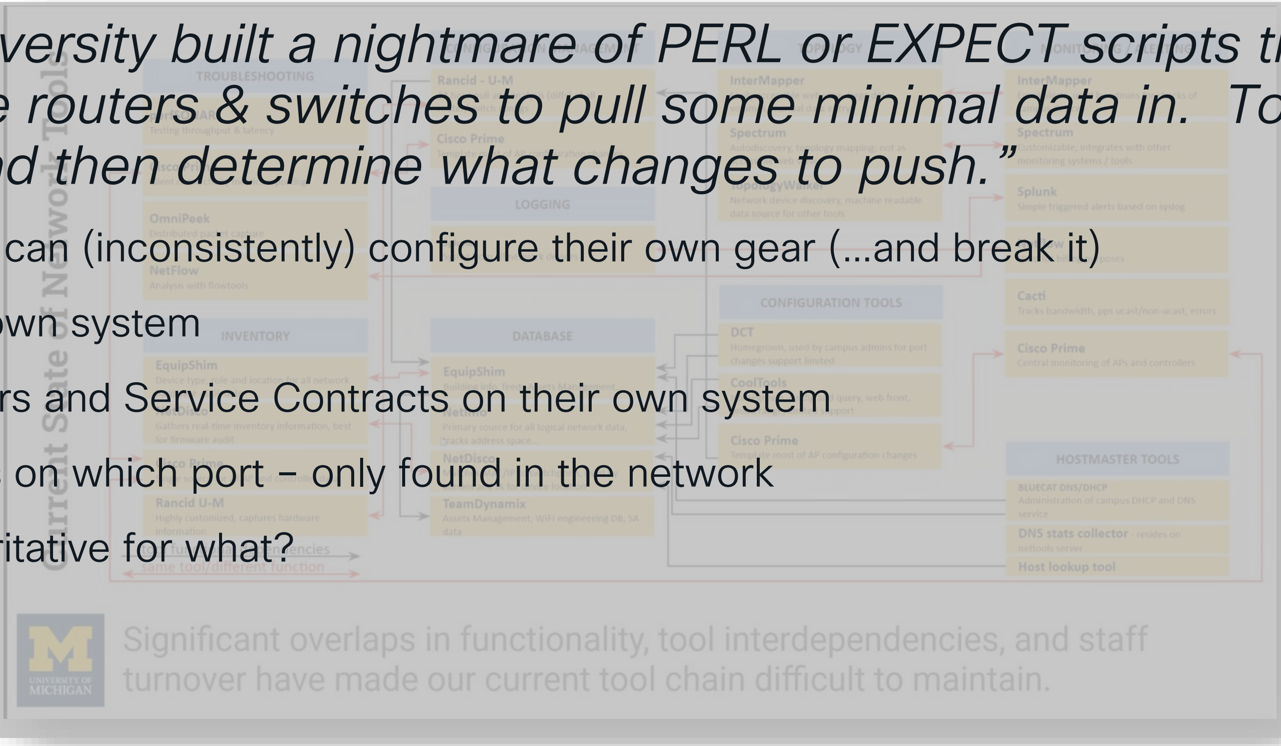
UNIVERSITY OF MICHIGAN

Significant overlaps in functionality, tool interdependencies, and staff turnover have made our current tool chain difficult to maintain.

Network Management: Where they Started….

Network Details spread all over

- *"Every university built a nightmare of PERL or EXPECT scripts that scrape the routers & switches to pull some minimal data in. To classify and then determine what changes to push."*
- Each College can (inconsistently) configure their own gear (…and break it)
- IPAM on it's own system
- Serial Numbers and Service Contracts on their own system
- What VLAN is on which port – only found in the network
- Who is authoritative for what?


Current State of Network Tools
TROUBLESHOOTING
Testing throughput & latency
OmniPeek
Distributed packet capture
NetFlow
Analysis with flowtools
INVENTORY
EquipShim
Device type, role and location for all network
Gathers real-time inventory information, best for firmware audit
Rancid U-M
Highly customized, captures hardware information
same tool/different function
Rancid - U-M
Cisco Prime
LOGGING
DATABASE
EquipShim
Primary source for all logical network data, tracks address space
NetDisco
TeamDynamix
Assets Management, WiFi engineering DB, SA data
InterMapper
Spectrum
Autodiscovery, topology mapping; not as
TopologyWalker
Network device discovery, machine readable data source for other tools
CONFIGURATION TOOLS
DCT
Homegrown, used by campus admins for port changes support limited
CoolTools
Cisco Prime
Template most of AP configuration changes
InterMapper
Spectrum
Customizable, integrates with other monitoring systems / tools
Splunk
Simple triggered alerts based on syslog
Cacti
Tracks bandwidth, pps ucast/non-ucast, errors
Cisco Prime
Central monitoring of APs and controllers
HOSTMASTER TOOLS
BLUECAT DNS/DHCP
Administration of campus DHCP and DNS service
DNS stats collector - resides on netools server
Host lookup tool
UNIVERSITY OF MICHIGAN

Significant overlaps in functionality, tool interdependencies, and staff turnover have made our current tool chain difficult to maintain.

Starting the Journey

Setting the Vision

…and establishing the first tenets.

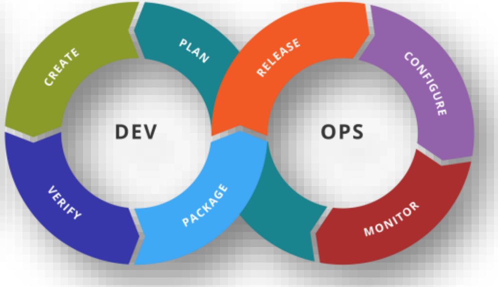
- Leverage Network Automation to **build a better product** (faster).
- Solution needs to be fully trusted by Ops as well as Architecture.
- Ability to delegate individual IT support using same core back end.
- Find the right balance between vendor agnostic automation and the flexibility to leverage specific vendor strengths
- Eliminate fringe & outlaw projects
- Eliminate Config Drift and ensure Config Compliance
- None of this will change daily requirement of a robust 100% uptime network!

Early Moves and Decisions

- **Network Engineers are NOT Software Engineers.**
- Quickly add Software Developers into the network team.
  - Leverage Software Development “best practices” in the network.
- EVERYONE on the team needs to learn baseline software skills
- *(…and given the time to explore and make mistakes in a safe environment)*
- Not looking to reduce staff. Looking to move staff to more “interesting” problems.
- **No one will log onto a router/switch again!**
- Take time to carefully define the problems we want to solve.

Level setting required Skills and Tools

Everyone needs to be comfortable in each of these spaces



Initial Findings

- Defining the problem is often the most difficult part.
- Preferred the model of deploying **abstracted network services**
  - …vs automating the configuration of network devices.
- "Source of Truth" – Is there a *single* source of truth? (Probably not)
- There is rarely such a thing as greenfield.
- **Involve operations early** – they will be supporting what you automate.
- Give everyone enough time to learn new tooling – typically hands on learning. *("What is a code review?")*

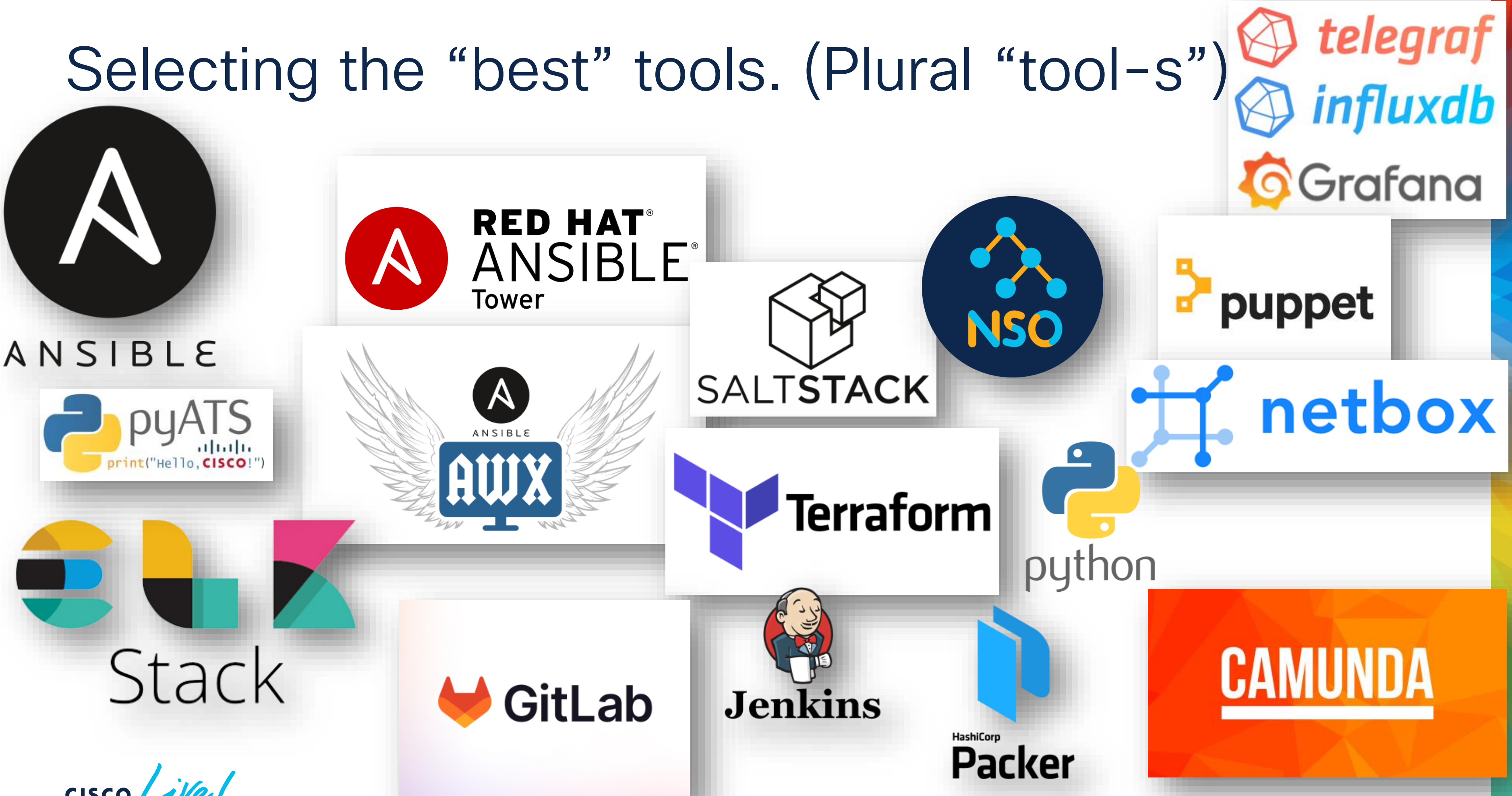
Tool Selection
“Which is better? X or Y?”

The Better Question...

*“Which tools are **better together** for what you need?”*

Often said by those who have implemented large scale network automation

Selecting the “best” tools. (Plural “tool-s”)



Fundamental Questions for Tool Selection

Big Questions….

- *Is your company ready to evolve culturally to achieve this?*
- What are the fundamental problems we are trying to solve?
- Are we configuring boxes, or deploying Network Services?
  - Get out of the mindset of configuring boxes.
- Who will be the “Source of Truth”?
  - Can you get down to a ***single*** source of truth? (I’ve never seen it)
- How early to involve Operations in the Architecture Process?
- How many tools are we willing to integrate?
- Is orchestration the goal? Visibility as well? Telemetry?

Fundamental Questions for Tool Selection

What is Config Compliance? Can there be versions?

- The actual full box config is the intended config?
- Part of the total running config is the intended config for that section? Nobody cares about other parts of the running config. (automated systems access happening)
- A specific feature on box has the intended config for that feature? DNS? NTP? SYSLOG?
- A "version" of a config snippet is running on box.
- The active box code has no known vulnerabilities.
- How to handle Remediation?

Journey through tool evaluation.

Customer Quotes

- Started with ANSIBLE with Tower. Then evaluated SALT.
  - Result: Good tools, although somewhat fragmented.
- Liked NETBOX as "*Source of Truth*" for Infrastructure
  - Device Inventory / VLAN & VRF Assignments / Asset Tracking
- NSO had the advantage of "Network Service Abstraction"
  - Deploy a switchport. Enable BGP Routing. Enable consistent policy.
  - ^^^ What are you really trying to do. Design a Network Service to abstract the CLI config.
- NSO is multi-vendor "*Source of Truth*" for the network configuration.
  - Manages a heterogeneous multi-vendor network. Legacy and new.
  - Verifies network is secure per policy. Detects config drift. Config Consistency.
  - Network friendly CLI enables faster evolution to software skills for network engineers

Campus Wireless

Typically end up with 1 of 2 paths at this point…

- Continue Leading with NSO Automation and Orchestration…
  - Continue with NSO approach – same as switching.
  - IOS-XE NED (Network Element Driver) has solid support for Cisco Catalyst 9800, just like rest of the Catalyst product portfolio.
  - Deploy common network services across wired and wireless ("Name Spaces") with same deployment.
- Lead with Cisco DNA Center. (See **DEVWKS-1004 & DEVWKS-2004**)
  - Easy automation of Cisco Catalyst 9800's and AP's
  - Why did Jimmy's iPhone not associate the the network last Thursday at 4:45PM?
  - Often a lead choice for an Operations centric environment.

Migration from then to now

Best Practices & Lessons Learned

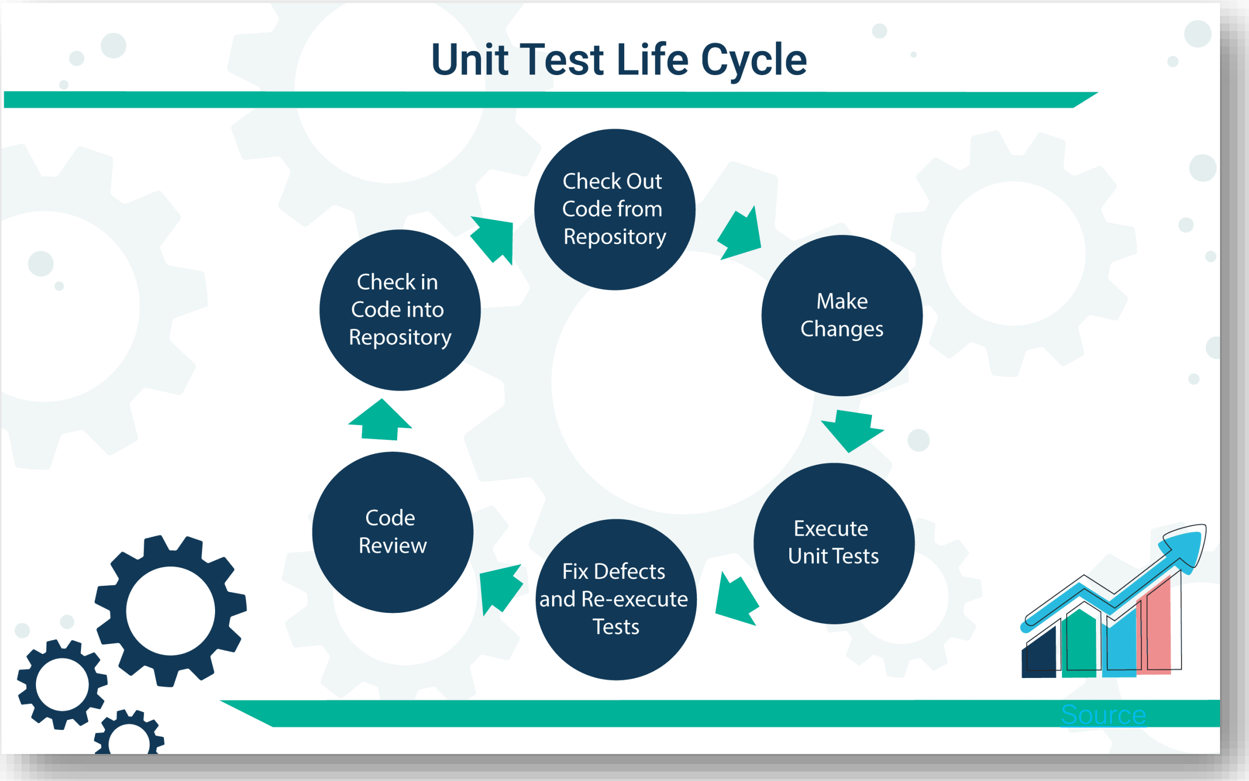
What to migrate from the "old way" to the "new way"?

Several opinions - Happy middle ground seems to be

- Encourage Operations to lead the cultural evolution. No more consoling into boxes, otherwise you're doomed before you begin.
- Migrate early, any nondisruptive services possible to the "new way".
- When you bring a building or station into "new way" automation, leverage this as being the closest you'll ever be to Greenfield. "Measure twice then cut once"
- Migrate the access layer to the "new way". This is where you spend the most time.
- Distribution / Core – Maybe not.
- Leverage NSO "Actions" (more later) to pre-populate NetBox
- Where possible, add communication to/from old tools to leverage one of NSO's interfaces many interface options. Makes it smoother to migrate away from old tools when the time is right
- BEWARE: Open Source ver 1.0 is cool. We're special, so let's modify it. (Now Stuck!)

“Code Review” – The new Network Procedure(s)

Network Code Review are the new norm.



Unit Test Life Cycle
Check Out Code from Repository
Make Changes
Execute Unit Tests
Fix Defects and Re-execute Tests
Code Review
Check in Code into Repository
Source

The Common Solution(s) and “Why NSO”?

(Multiple) Sources of Truth

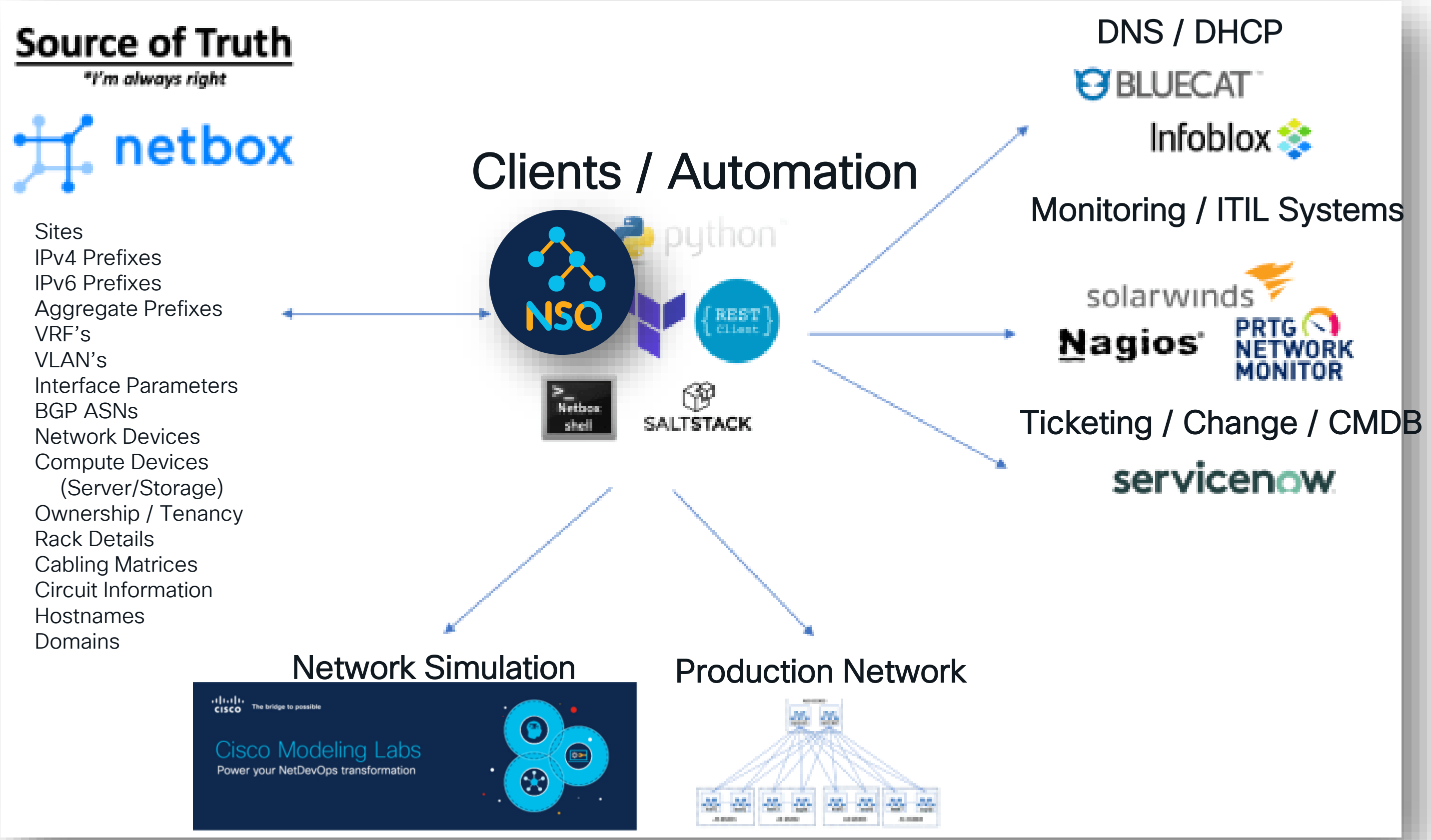
NetBox for DCIM and IPAM

- Device Inventory and categorization
- Asset Tracking
- Prefix, VLAN, and VRF Assignments

NSO: Network Configuration

- “Network Service” config management
- Source of Truth for service data
- Config Drift Notification
- Operational Snapshots
- *Added existing Access switches and all New Network Gear to NSO*

NetBox Summary



Source of Truth

"I'm always right

Sites
IPv4 Prefixes
IPv6 Prefixes
Aggregate Prefixes
VRF's
VLAN's
Interface Parameters
BGP ASNs
Network Devices
Compute Devices
(Server/Storage)
Ownership / Tenancy
Rack Details
Cabling Matrices
Circuit Information
Hostnames
Domains

Clients / Automation

DNS / DHCP

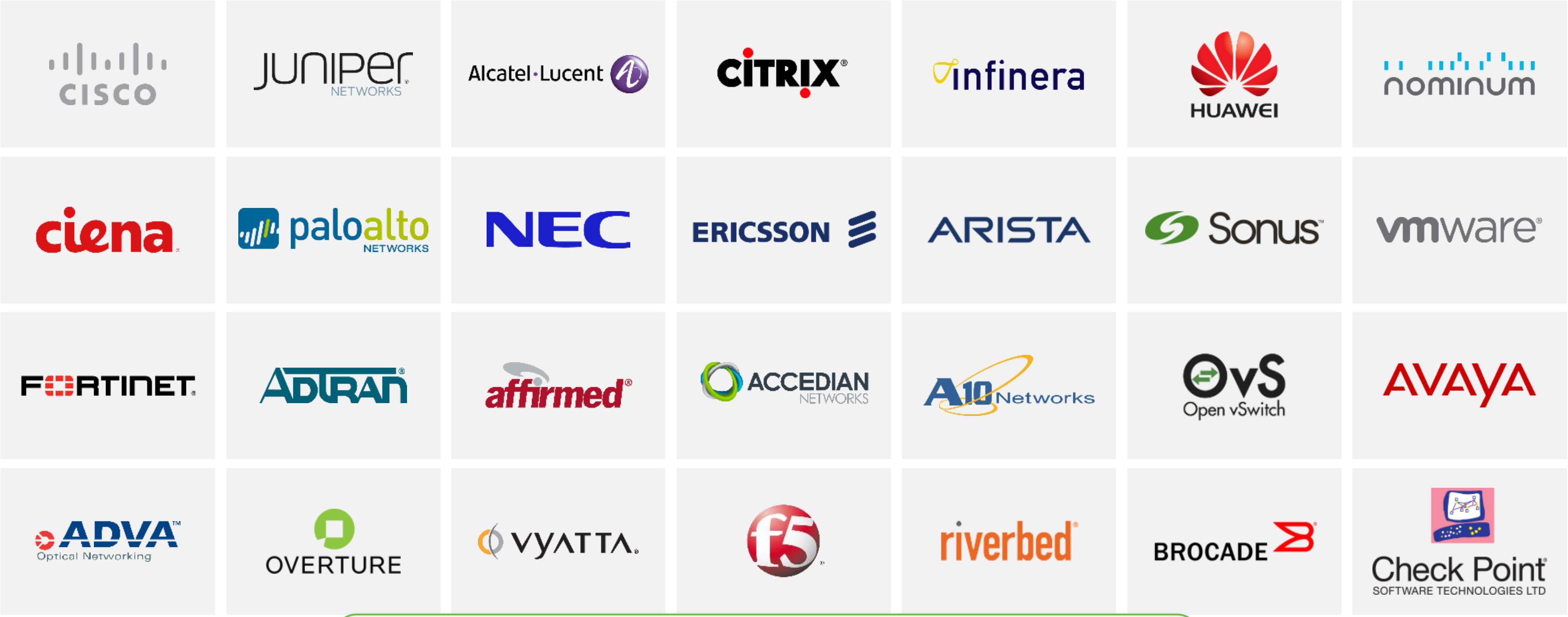
Monitoring / ITIL Systems

Ticketing / Change / CMDB

Network Simulation

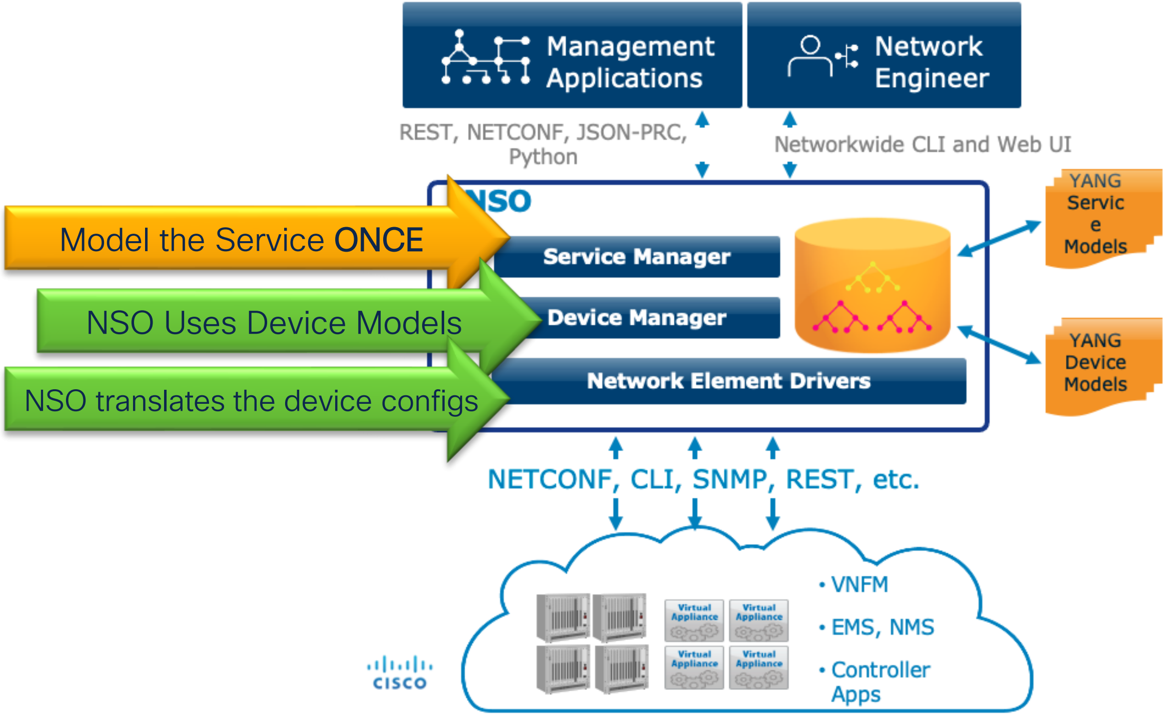
Production Network

NSO Multi Vendor Support



100+ Vendors, 170+ Device Families

NSO Network Service Models



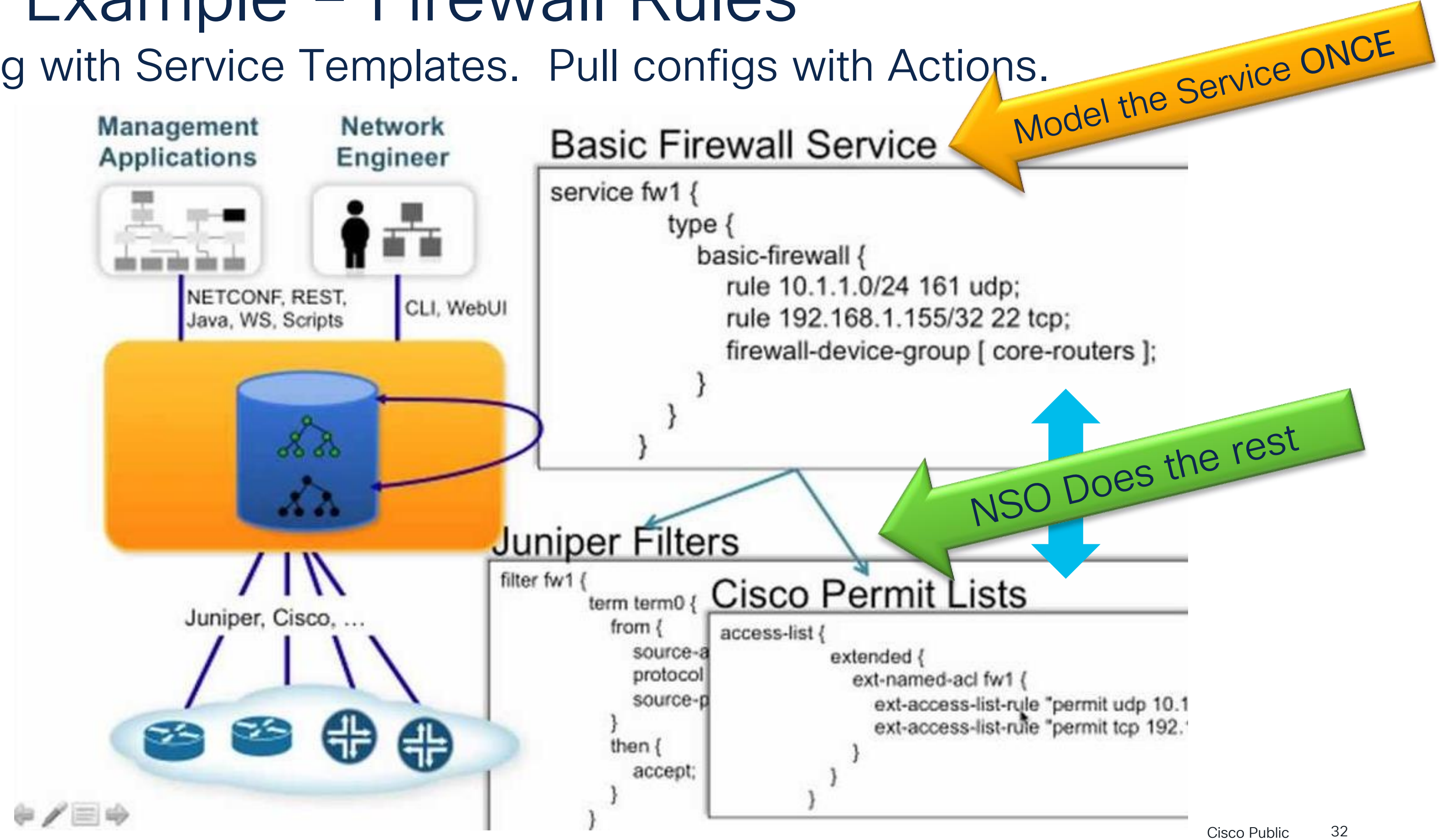
- NETCONF and YANG
- Data models represent:
  - Service instances
  - Network Device configuration
- Active copy of the network config
- Transactional integrity across network
- Single Pane of Glass
- FastMap: rapid network config changes
- Network Element Drivers (NEDs) provide vendor/device abstraction
- Multi-protocol & Multi-vendor

Major Standards Proponent

100 devices in the service. 2 don't deploy, NSO rolls the WHOLE THING back.

Simple Example – Firewall Rules

Push config with Service Templates. Pull configs with Actions.



Model the Service ONCE

NSO Does the rest

Basic Firewall Service

```
service fw1 {
        type {
            basic-firewall {
                rule 10.1.1.0/24 161 udp;
                rule 192.168.1.155/32 22 tcp;
                firewall-device-group [ core-routers ];
            }
        }
    }
```

Juniper Filters

```
filter fw1 {
        term term0 {
          from {
            source-a
            protocol
            source-p
          }
          then {
            accept;
          }
        }
    }
```

Cisco Permit Lists

```
access-list {
        extended {
          ext-named-acl fw1 {
            ext-access-list-rule "permit udp 10.1
            ext-access-list-rule "permit tcp 192.
          }
        }
    }
```

NSO “Actions” – non-configuration steps

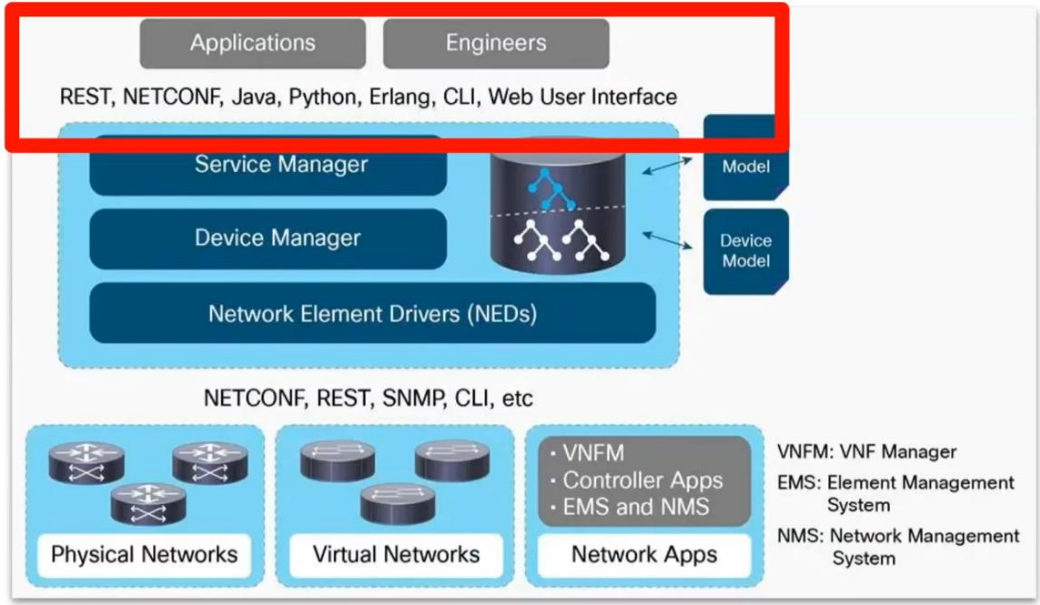
Example: Great for migrating legacy to new systems

- Go to all my switches (or a subset, or a single switch) and discover all the VRF’s and their associated Details. Then see if that VRF exists in NetBox.
  - (Potentially) – then add the VRF details to NetBox, and add the VRF configuration to the switch per defined policy. Thus reconciling the previously unknown network parameters to the “source of truth”.
  - (Potentially) – Then open a service ticket with the details of the previously unknown VRF.
- Check the common services, and reconcile if they are not per policy
- Discover all VLAN’s on a switch(s) and reconcile.
- Discover BGP Routes… OSPF Neighbors… Verify etc…

Same API call: all switches, a subset of switches, or single switch – ***All VENDORS***

NSO’s Programmatic Interfaces

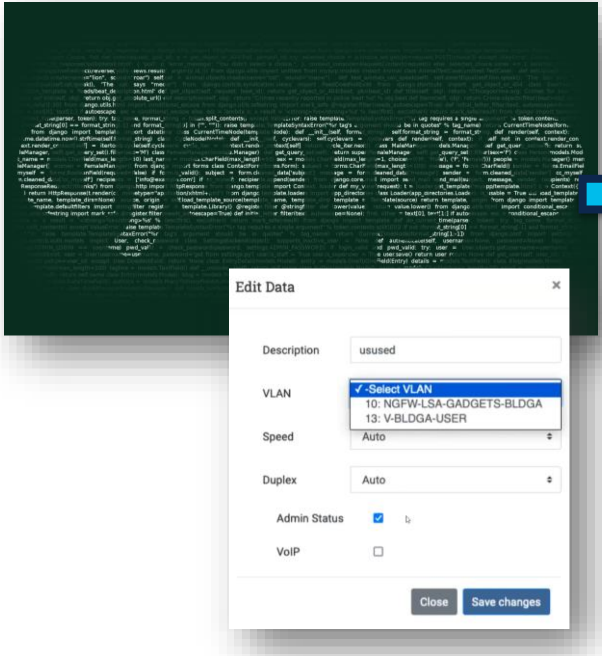
Interface with NSO however you choose


Applications
Engineers
REST, NETCONF, Java, Python, Erlang, CLI, Web User Interface
Service Manager
Device Manager
Network Element Drivers (NEDs)
Model
Device Model
NETCONF, REST, SNMP, CLI, etc
Physical Networks
Virtual Networks
• VNFM
• Controller Apps
• EMS and NMS
Network Apps
VNFM: VNF Manager
EMS: Element Management System
NMS: Network Management System

- REST
- **NETCONF**
- Java
- Python
- Erlang
- CLI
- Web UI

Ability to Front-End common NSO services

Django Calling NSO via NETCONF



Edit Data

Description: usused

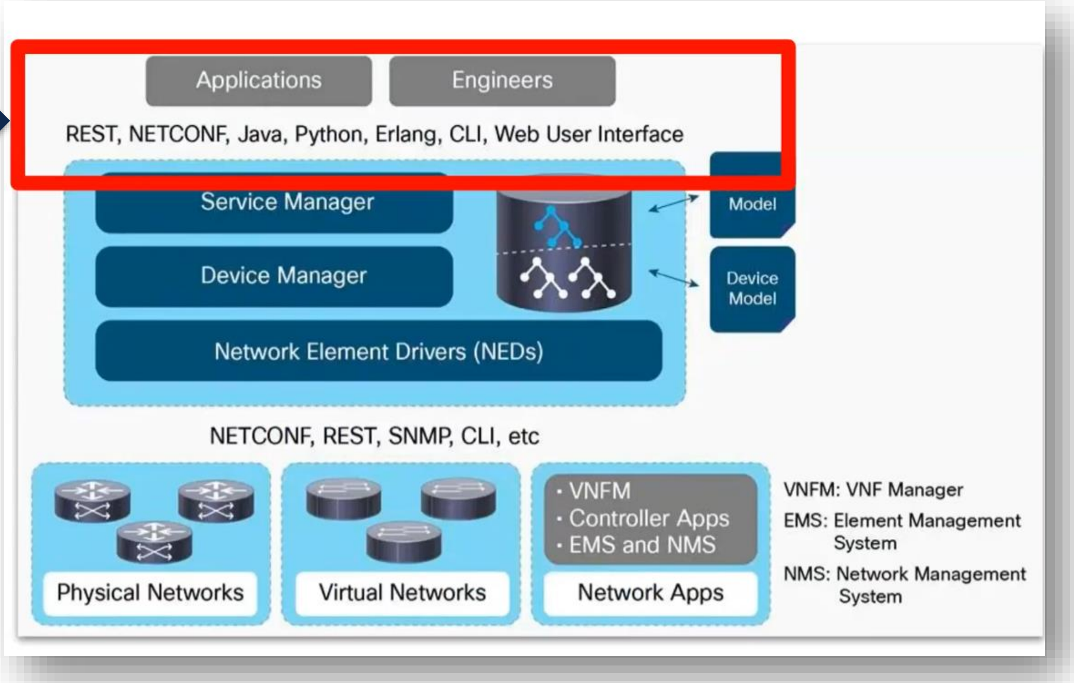
VLAN: ✓ -Select VLAN
- 10: NGFW-LSA-GADGETS-BLDGA
- 13: V-BLDGA-USER

Speed: Auto

Duplex: Auto

Admin Status ☑

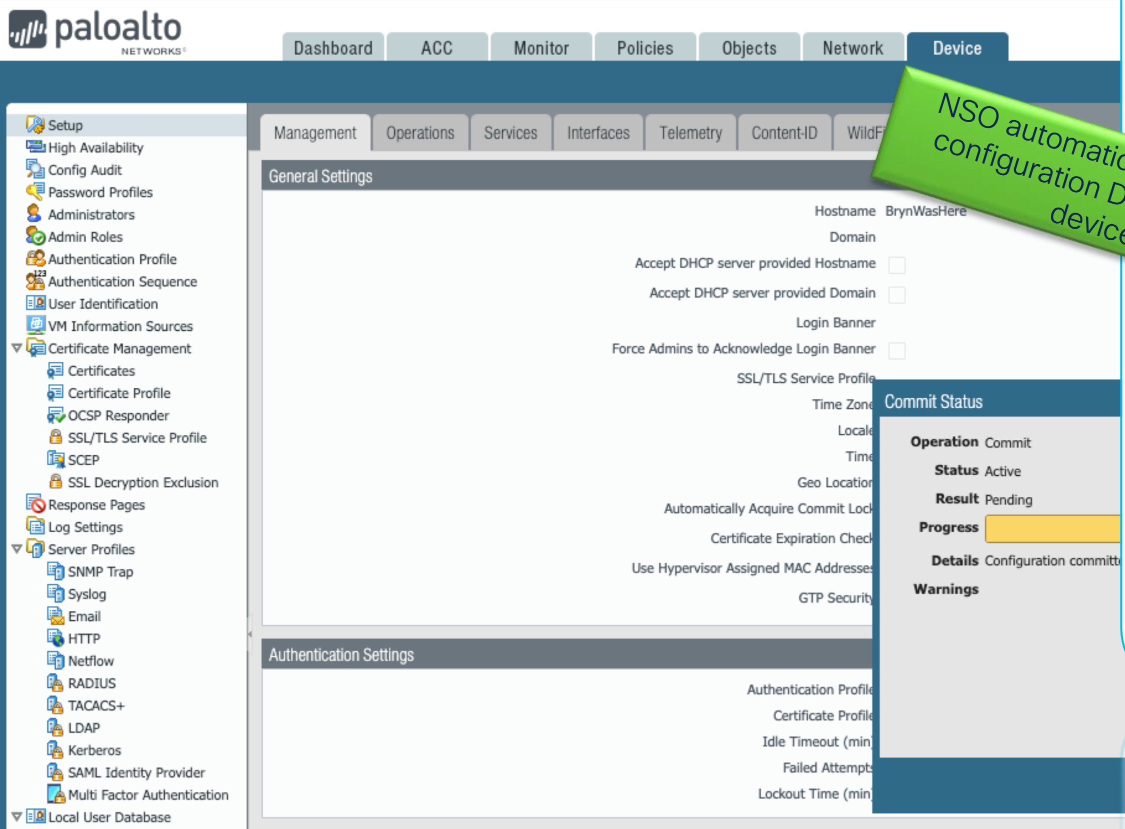
VoIP ☐



Applications
Engineers
REST, NETCONF, Java, Python, Erlang, CLI, Web User Interface
Service Manager
Device Manager
Model
Device Model
Network Element Drivers (NEDs)
NETCONF, REST, SNMP, CLI, etc
Physical Networks
Virtual Networks
· VNFM
· Controller Apps
· EMS and NMS
Network Apps
VNFM: VNF Manager
EMS: Element Management System
NMS: Network Management System

Config Drift via NSO

“Compare Config” example – Palo Alto



General Settings

Hostname BrynWasHere
Domain
Accept DHCP server provided Hostname □
Accept DHCP server provided Domain □
Login Banner
Force Admins to Acknowledge Login Banner □
SSL/TLS Service Profile
Time Zone
Locale
Time
Geo Location
Automatically Acquire Commit Lock
Certificate Expiration Check
Use Hypervisor Assigned MAC Addresses
GTP Security

Authentication Settings

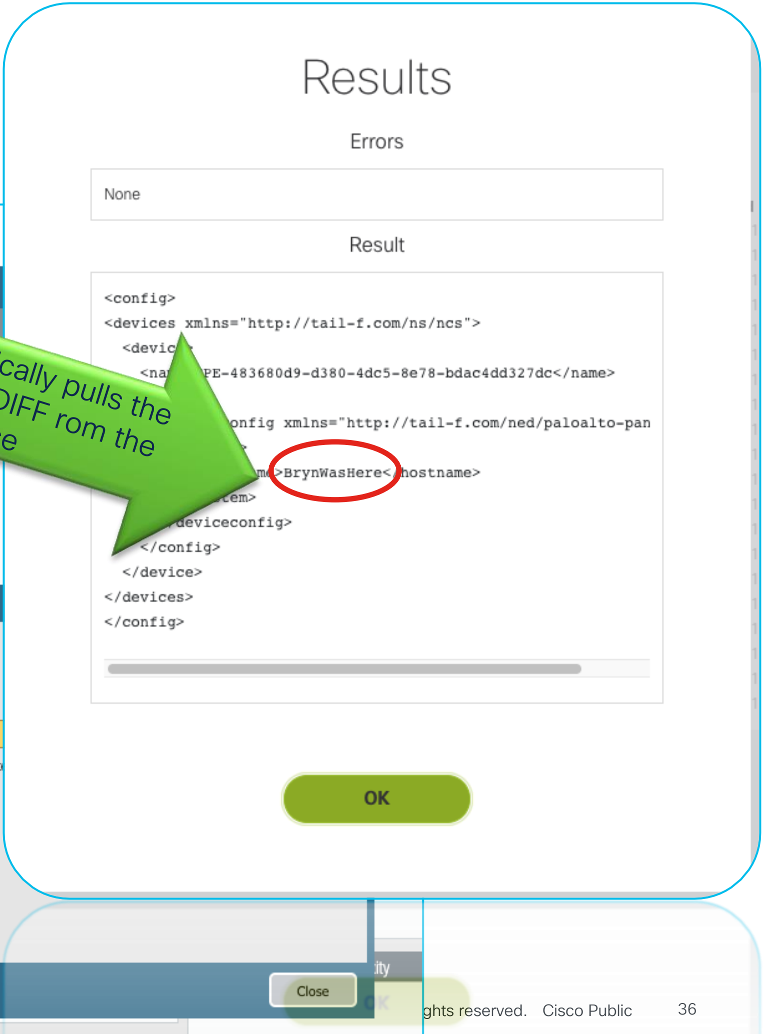
Authentication Profile
Certificate Profile
Idle Timeout (min)
Failed Attempts
Lockout Time (min)

Commit Status

Operation Commit
Status Active
Result Pending
Progress
Details Configuration committ
Warnings

Close

NSO automatically pulls the configuration DIFF rom the device



Results

Errors

None

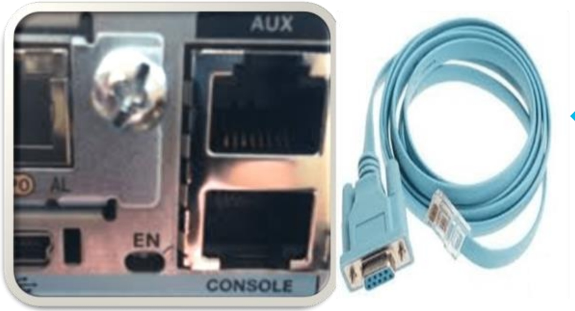
Result

```
<config>
<devices xmlns="http://tail-f.com/ns/ncs">
  <devic
    <na    PE-483680d9-d380-4dc5-8e78-bdac4dd327dc</name>

          onfig xmlns="http://tail-f.com/ned/paloalto-pan

             me>BrynWasHere</hostname>
           tem>
      deviceconfig>
    </config>
  </device>
</devices>
</config>
```

OK

Work Smarter, not Harder. (No Polling)

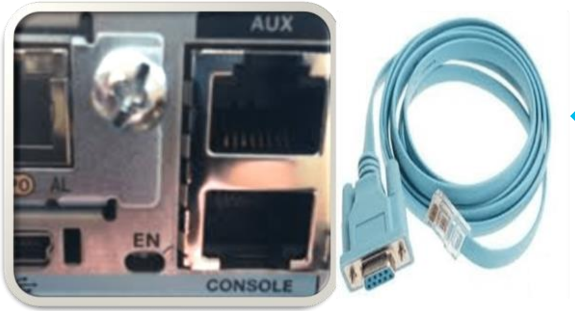
Do I really need to check it every day?



Event Driven. Generate a syslog message when someone logs into a device.

Work Smarter, not Harder. (No Polling)

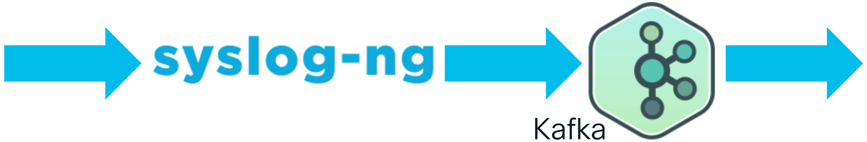
Do I really need to check it every day?



Event Driven. Generate a syslog message when someone logs into a device.

Someone logs into a device.
Syslog is generated

Collect syslog(s) and process
...or put in a messaging bus
...or monitoring your existing collector
...or <whatever>



Kafka
...or <other>

“login” detected and initiate's the NSO compare-config. If DIFF found, send to <whatever>.

MOST IMPORTANT LESSONS LEARNED

MOST IMPORTANT LESSONS

- Be sure you have buy-in from Operations. If you don’t, you will fail.
  - No more consoles. No more SSH'ing into CLI.
- Network Engineers are not Software Developers. Integate your teams EARLY!
  - (Also, Software Developers are not Network Engineers)
  - Time to apply "Unit Test Lifecycle" to the network
- Change your perspective. Network Services – not box configs.
- There is no such thing as a “Single Source of Truth” for everything.
  - Pick 2-3 tools that work well together. No such thing as 1. Don't try 12.
- Modify process to match your preferred software. Not the other way around.
- Decide what "Compliance" really means to your org.
- Work Smarter – Not Harder! 8-)

Conclusions

Final Thoughts

- This “Network Profile” isn’t every network. This is for specific organizations who need / want very specific customized network automation and orchestration.
- It can be done. Give your network engineers "time to make mistakes". Python was made for Network Engineers, who can be "productive" with 1-2 weeks of training.
- Enjoy the ride. Learn a few new skills and build a better network.

Ping me anytime
bryn@cisco.com

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Challenge** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

The bridge to possible

Thank you

#CiscoLive

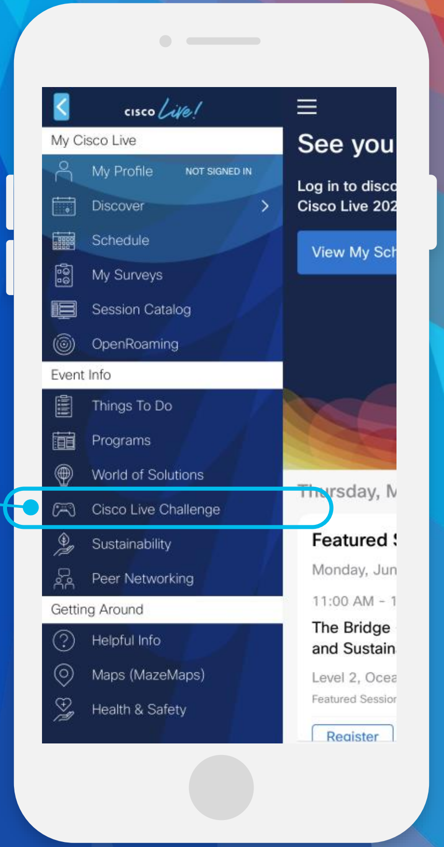
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!

My Cisco Live
- My Profile NOT SIGNED IN
- Discover
- Schedule
- My Surveys
- Session Catalog
- OpenRoaming

Event Info
- Things To Do
- Programs
- World of Solutions
- Cisco Live Challenge
- Sustainability
- Peer Networking

Getting Around
- Helpful Info
- Maps (MazeMaps)
- Health & Safety

See you

Log in to disco
Cisco Live 202

View My Sch

Thursday, M

Featured S
Monday, Jun
11:00 AM - 1
The Bridge
and Sustain
Level 2, Ocea
Featured Sessior
Register

cisco Live!

Let's go

#CiscoLive