SD-Access Assurance and Analytics

Karthik Kumar Thatikonda
Technical Leader
Cisco Spark

Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKCRS-2814
Agenda

1. Introduction
   Why do you care?

2. DNA Architecture Overview
   What is SD-Access?

3. DNA Analytics
   What is Network Telemetry?

4. DNA Assurance
   What is SD-Access Assurance?

5. Take-Away
   Next Steps for SD-Access Assurance
Why do you care?
Why SD-Access Assurance?

Need to Troubleshoot user **red** connectivity to a **DHCP server**

50.0.0.1
CLI is the most common troubleshooting tool. It's just a very **bad** troubleshooting tool.

- `show ip dhcp snooping binding`
- `show ip vrf interfaces | inc 1021`
- `show sh lisp vrf Campus | i IID`
- `show lisp instance-id 4099 ipv4 map-cache`
- `show ip cef vrf Campus 50.0.0.1 internal`
- `traceroute 192.168.130.2`
- `ping 192.168.10.1`
- `show cdp nei g1/0/22`
ping 192.168.130.2

... 

Success rate is 0 percent (0/5)

- show ip route 192.168.130.2
- show cdp nei gi1/0/23
- show run int gi1/0/23
interface GigabitEthernet1/0/23
  description border_cp g1/0/15
  no switchport
  ip address 192.168.15.1 255.255.255.252
  ip router isis
  ip access-group test out

Extended IP access list test
  10 deny ip host 192.168.120.1 host 192.168.130.2
Quick Isolation of Network Issues

SD-Access Assurance Reason #1

Connected
Fabric Edge "192.168.120.1" Lost Connectivity to the Co-located Fabric Border and Control Plane 192.168.130.2 in the Physical Network
Total occurrences: 357
Root Cause Issue in few clicks

SD-Access Assurance Reason #2

Set up Path Trace

Source
192.168.120.1
Interface (optional)
Port (optional)

Destination
192.168.130.2
Interface (optional)
Port (optional)

Run New Path Trace

Start
Network Troubleshooting Tool
Pathtrace

Path Trace
To find the location of an issue, perform a path trace between two nodes in your network—a source device and a destination device.

10.30.100.10 (port: not specified) → 10.30.120.10 (port: 9100) [protocol: tcp]

More Details

Run New Path Trace
End to End Visibility across LAN, WLAN and WAN
DNA Architecture
Cisco’s Intent-based Networking

The Network. Intuitive.

Powered by Intent. Informed by Context.
Digital Network Architecture (DNA) DNA Center embracing DNA

DNA Software Capabilities

- Cloud Service Management
- Automation
- Analytics
- Virtualization
- DNA-Ready Physical and Virtual infrastructure
- Security

Insights & Actions
Security & Compliance
Automation & Assurance
Digital Network Architecture (DNA)
DNA Center embracing DNA

DNA Software Capabilities

DNA Center

Automation
Analytics
Virtualization
DNA-Ready Physical and Virtual infrastructure

Automation & Assurance
Security & Compliance
Insights & Actions

DNA - Ready Physical and Virtual infrastructure
Digital Network Architecture (DNA)
DNA Center embracing DNA

DNA Software Capabilities
- Automation & Assurance
- Security & Compliance
- Insights & Actions

DNA Center

Software Defined Access

DNA-Ready Physical and Virtual infrastructure

Security

Virtualization

Analytics

Automation
Digital Network Architecture (DNA)
DNA Center embracing DNA

DNA Software Capabilities
- Cloud Service Management
- Automation
- Analytics
- Virtualization

Software Defined Access
- Catalyst 9000, IOS-XE, Access Points
- Automation & Assurance
- Security & Compliance
- Insights & Actions

Flexible Hardware and Software

Security
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

- **IoT Network**
  - Software-Defined Access (SDA) Extension

- **Employee Network**
  - User Mobility
  - Policy stays with user
SD-Access
Fabric Roles & Terminology

- **DNA Center** – Enterprise SDN Controller provides GUI management and abstraction via Apps that share context
- **Identity Services** – NAC & ID Systems (e.g. ISE) for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – Data Collectors (e.g. NDP) analyze Endpoint to App flows and monitor fabric status
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects APs and Wireless Endpoints to the SDA Fabric
Software Defined Access
Cisco Live Barcelona - Session Map

<table>
<thead>
<tr>
<th>Tuesday (Jan 30)</th>
<th>Wednesday (Jan 31)</th>
<th>Thursday (Feb 01)</th>
<th>Friday (Feb 02)</th>
</tr>
</thead>
<tbody>
<tr>
<td>08:00-11:00</td>
<td>08:00-11:00</td>
<td>08:00-11:00</td>
<td>08:00-11:00</td>
</tr>
<tr>
<td>11:00-13:00</td>
<td>11:00-13:00</td>
<td>11:00-13:00</td>
<td>11:00-13:00</td>
</tr>
<tr>
<td>13:00-15:00</td>
<td>13:00-15:00</td>
<td>13:00-15:00</td>
<td>13:00-15:00</td>
</tr>
<tr>
<td>15:00-18:00</td>
<td>15:00-18:00</td>
<td>15:00-18:00</td>
<td>15:00-18:00</td>
</tr>
<tr>
<td></td>
<td>08:00-11:00</td>
<td></td>
<td>08:00-11:00</td>
</tr>
<tr>
<td></td>
<td>11:00-13:00</td>
<td></td>
<td>11:00-13:00</td>
</tr>
<tr>
<td></td>
<td>13:00-15:00</td>
<td></td>
<td>13:00-15:00</td>
</tr>
<tr>
<td></td>
<td>15:00-18:00</td>
<td></td>
<td>15:00-18:00</td>
</tr>
<tr>
<td>08:00-11:00</td>
<td>08:00-11:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00-13:00</td>
<td>11:00-13:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:00-15:00</td>
<td>13:00-15:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:00-18:00</td>
<td>15:00-18:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>08:00-11:00</td>
<td>08:00-11:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11:00-13:00</td>
<td>11:00-13:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13:00-15:00</td>
<td>13:00-15:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15:00-18:00</td>
<td>15:00-18:00</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**BRKCRS-2810**
Solution Overview

**BRKCRS-2811**
External Connect

**BRKCRS-2816**
Routed Underlay

**BRKCRS-2812**
Migration

**BRKCRS-2815**
Design & Scale

**BRKCRS-2814**
Assurance

**BRKDCN-2489**
DC Integration

**BRKEWN-2020**
Wireless Overview

**BRKEWN-2021**
SDA Wireless Setup

**LTRCRS-2810 (1)**
Hands-On Lab

**LTRCRS-2810 (2)**
Hands-On Lab

Missed One? Sessions are available online @ CiscoLive.com
The DNA Analytics
DNA Center Data Analytics Architecture

Data collection and ingestion

- Network telemetry
  - Router
  - Switch
  - WLC
  - Sensor
  - SNMP
  - NetFlow
  - Syslog
  - Streaming telemetry

Contextual data

- ISE
- AAA
- Topology
- Location
- Policy
- IPAM
- DNS
- DHCP
- Inventory
- PxGrid

Data correlation and analysis

- Complex correlation
- Metadata extraction
- Stream processing

Analytics Engine

Data visualization and action

- Network assurance
- Collector and analytics pipeline SDK
- Data models and restful APIs
- Time series analysis
- System management portal

BRKCRS-2814 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
System Flow

Contextual data → Collector → Distributed Pub-Sub Broker Kafka → Real-time Analytics Engine (Flink, Apache Beam) → Analytics Data Stores (Cassandra, InfluxDB, ELK) → Collectors → Analytics Engine → Applications

- Access
- Collect
- Ingest
- Prepare
- Analyze
- Store and Serve
- Visualize and Act

Network telemetry data

Flow Information: NetFlow, IPFIX, sFlow, NetFlow lite, etc.

N/W State, Operational data, System counts, connection counts, timeouts, etc.

Location, Presence, Identity, Group Info, etc.

Events: Syslog, SNMP Traps, Notifications from controllers, etc.

Controllers, Orchestrator, DBs: Inventory, topology, app identity

Logs, Domain Mgrs: ISE, DNS, MSE, logs, AAA, Traces, etc.

Contextual Data

BRKCRS-2814 © 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
What types of Collection mechanism are used?

**Telemetry**

- **Data Type:** Users, User Group
  - **Data Source:** AD, Cisco ISE
  - **Mechanism:** Pull (API)

- **Data Type:** Topology, Inventory, Configuration, Capabilities
  - **Data Source:** Automation

- **Data Type:** Policy
  - **Data Source:** Cisco ISE
  - **Mechanism:** Subscription through PxGrid

- **Data Type:** IP Address Management, Namespaces
  - **Data Source:** Infoblox, DHCP, DNS
  - **Mechanism:** Pull (API)

- **Data Type:** Wireless Signaling, Roaming data
  - **Data Source:** WLC/AP
  - **Mechanism:** Streaming

- **Data Type:** Flow, Applications
  - **Data Source:** Network Device
  - **Mechanism:** Push

- **Data Type:** SNMP
  - **Data Source:** Network Device
  - **Mechanism:** Pull

- **Data Type:** Syslogs, Traps
  - **Data Source:** Network Device
  - **Mechanism:** Push

**Contextual Telemetry Sources**

**Network Telemetry Sources**

A singular framework for ingestion
Contextual Correlation and Property Graph

Finance

George Baker

Business Applications

App ID: 18

Src IP: 1.1.1.2

Dest Port: 3600

Dest IP: 2.2.2.2

WAN QoS problem here...

Forwarding problem here...

Client density problem here...

SJC-9 2nd Floor

RTP DC

SJC

1.1.1.1

Netflow

AVC

DDI

ISE/Radius

Topology

CMX, DNAC

Device
Power of Analytics and Automation working in sync

DNA Center

Automation

Telemetry, alerts, violations

Assurance and Analytics

Network inventory, topology, and configuration

Network and telemetry configuration

Streaming telemetry & network data
SD-Access - DNA Center
Telemetry Configuration

Telemetry Profile

- Syslog
- NETFLOW
- SYSLOG
- SNMP
- SNMPTRAPS

Capabilities:
- Capable
- Sending

Options:
- SNMP Traps
  - Version: V2C
DNA Assurance is part of DNA Center
DNA Center consists of automation and assurance

Planning, installation and migration
Proactive and predictive network, client and application assurance
Today’s tools are limited and do not address network needs

**Too Many Tools**
- Fragmented visibility
- Closed interfaces / Silo’d views
- Devices queried multiple times
- Different protocols/mechanisms

**Reactive Systems**
- Always playing catch up
- Not designed for analytics
- Inconsistent API architecture
- Specialized knowledge required

**Limited Insights**
- Limited data that is not actionable
- My report vs your report
- No view of state changes
- Lacking context or feedback loop

Rigid | Closed/Proprietary | Lack of Intelligence
Introducing DNA Analytics

Transforming network operations through actionable insights and simplicity

Right Place

End-to-End Visibility
360° view across network
Ability to follow the network path

Correlated Insights
Proactive to get ahead of the problem
Predictive to stay ahead

Right Time

Time Travel
Contextual Graph—Captures network state over time
14 Days history: Record and replay events

Right Action

Guided Remediation
Today—Remediate with user input
Future—Automated remediation
Fabric Assurance
Insights: SDA Use-Cases

Control Plane
- Edge to Control Plane
- Border to Control Plane
- CP performance
- Routing protocols

Data Plane
- Border and Edge connectivity
- Border node health
- Edge node health
- Device to Services (DHCP, DNS, AAA)

Policy Plane
- ISE connectivity
- Border node policy
- Edge node policy

Client Onboarding
- Client / Device DHCP
- Client Authentication
- Client Authorization

Device
- CPU, Memory
- TCAM Tables
- Modules
- Temperature
- Power (POE)

Applications

Services

Clients

Network Infrastructure

Broad

Deep
## Wireless Specific Correlated Insights

<table>
<thead>
<tr>
<th>Client Onboarding</th>
<th>Client Experience</th>
<th>Network Coverage &amp; Capacity</th>
<th>Network Device Monitoring</th>
<th>Application Performance Sensor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Association failures</td>
<td>Throughput analysis</td>
<td>Coverage hole</td>
<td>Availability</td>
<td>Web: HTTP &amp; HTTPS</td>
</tr>
<tr>
<td>Authentication failures</td>
<td>Roaming pattern analysis</td>
<td>AP License Utilization</td>
<td>Crash, AP Join Failure</td>
<td>Email: POP3, IMAP, Outlook</td>
</tr>
<tr>
<td>IP address failure</td>
<td>Sticky client</td>
<td>Client Capacity</td>
<td>High Availability</td>
<td>Web Access</td>
</tr>
<tr>
<td>Client Exclusion</td>
<td>Slow roaming</td>
<td>Radio Utilization</td>
<td>CPU, Memory utilization</td>
<td>File Transfer: FTP &amp; TFTP</td>
</tr>
<tr>
<td>Excessive on-boarding time</td>
<td>Excessive roaming</td>
<td></td>
<td>Flapping AP, Hung Radio</td>
<td>Terminal: Telnet &amp; SSHv2</td>
</tr>
<tr>
<td>Excessive authentication time</td>
<td>RF, Roaming pattern</td>
<td></td>
<td>Power supply failures</td>
<td></td>
</tr>
<tr>
<td>Excessive IP addressing time</td>
<td>Dual band clients prefer 2.4GHz</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AAA, DHCP reachability</td>
<td>Excessive interference</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Total Insights: 66 issues in DNA-C 1.1
Advanced Client Insights– Apple iOS Analytics

1. **Device Profile**
   - Client shares these details
     1. Model e.g. iPhone 7
     2. OS Details e.g. iOS 11

2. **Wi-Fi Analytics**
   - Client shares these details
     1. BSSID
     2. RSSI
     3. Channel #

3. **Assurance**
   - Client shares these details
     Error code for why did it previously disconnected

Support per device-group Policies and Analytics

Insights into the clients view of the network

Provide clarity into the reliability of connectivity
Advanced Client Insights– Apple iOS Analytics

Detailed Client device profile information – device model, OS details

Insights into the clients view of the network – Neighboring Access Points

Provide clarity into the reliability of connectivity – client disassociation details

Capability unique to Cisco Wireless Networks only !!
Proactive Performance Assessment for Wireless

Test your network anywhere at any time

- On-Boarding Tests
  - 802.11 Association
  - 802.11 Authentication & Key Exchange
  - IP Addressing DHCP (IPv4)

- Network tests
  - DNS (IPv4)
  - RADIUS (IPv4)
  - First Hop Router/Default gateway (IPv4)
  - Intranet Host
  - External Host (IPv4)

- Application tests
  - Email: POP3, IMAP, Outlook Web Access (IPv4)
  - File Transfer: FTP (IPv4), TFTP (IPv4)
  - Web: HTTP & HTTPS (IPv4)

Flexible Radio Assignment Algorithm intelligently identifies excessive radios and seamlessly converts those into Sensor mode without client impact.
SD-Access - DNA Center Provision
Fabric Proactive Monitoring

1. Select device to be added to the fabric
2. Select Control Plane Node
3. Select Border Node

Validation

Search Topology
Select Devices to add, remove or identify.
Shift + Click to select multiple.
Fabric Assurance
Monitor Fabric Connectivity

- **IPSLA** tests are run in the network fabric to verify connectivity between Control Plane, Fabric Border, and Fabric Edge nodes.

- **IPSLA** analyzes basic IP service levels for common IP services, to reduce downtime and lower operational costs.

- Includes **path trace** capability as part of troubleshooting steps.

```
ip sla 1
  icmp-echo 192.168.110.1 source-ip 192.168.120.1
  threshold 3
ip sla schedule 1 life forever start-time now
```
Fabric Device 360

**Detail Information**

Click on the Fabric tab to see how Fabric metrics are going:

1. Select Both options
2. Reachability tests are being performed in the Fabric underlay. This is the test results.

### Reachability

<table>
<thead>
<tr>
<th>Destination</th>
<th>Ip Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MapServerBorder - 192.168.130.2 - Underlay</td>
<td>192.168.130.2</td>
<td>Underlay</td>
</tr>
<tr>
<td>MapServerBorder - 192.168.130.1 - Underlay</td>
<td>192.168.130.1</td>
<td>Underlay</td>
</tr>
</tbody>
</table>
Fabric Assurance
Monitor Fabric Connectivity

• **IPSLA** tests are run in the network fabric to verify connectivity between Fabric Border and external services

• Monitor **external services** from fabric in the underlay and overlay network (IPAM, AAA, DHCP, DNS)

• Includes **path trace** capability as part of troubleshooting steps

---

**Example**

```
ip sla 3
  icmp-echo 50.0.0.1 source-ip 7.1.1.5
  vrf Campus
  threshold 3
  ip sla schedule 3 life forever start-time now
```
Fabric Assurance
Monitoring Fabric State - Proactive

- Fabric nodes query Control Plane to resolve host locations, if they don’t have an entry in their local database
- After receiving a map-reply, each fabric node stores those entries in its cache database
- Fabric Assurance tracks the number of requests and state of active cache entries to provide proactive trending analysis

Example

```
FE1# show ip lisp map-cache instance-id 4098
LISP IPv4 Mapping Cache for EID-table vrf Campus (IID 4098), 5 entries

10.2.1.89/32, uptime: 00:05:16, expires: 23:57:59, via map-reply, complete
Locator     Uptime    State     Pri/Wgt
10.2.120.3   00:04:23  up        10/10
```
Health Scores

Site Health Score
- \textit{function} (Client Health Score, Device Health Score)

Client Health Score
- \textit{function} (Onboarding Score, Connectivity Score)

Device Health Score
- \textit{function} (System Health Score, Control Plane Score, Data Plane Score)

Application Health Score
- \textit{function} (Traffic Class, Latency, Packet Loss)
Wired Client Health
Summary: Is the client connected and is the link connection good?

- Connected
  - Throughput issues
    - Link Error
  - Port Up/down
    - Yes/No
  - Authenticated, IP
    - Yes/No
  - Key Services
    - DNS reachable
Fabric Assurance
How Do We Calculate Fabric Network Health Scores?

Collect relevant Key Performance Indicators (KPIs) to determine Device Health

For example: Resources (CPU, DRAM, etc), Link state and errors, Protocol state and errors, Reachability to Control Plane, etc

Fabric Device Health has 3 Categories:
- Control Plane
- Data Plane
- System Health

Fabric Device Score is the Lowest of all Scores

Example

3850-SJC24-3

<table>
<thead>
<tr>
<th></th>
<th>System Health</th>
<th>Data Plane</th>
<th>Control Plane</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10</td>
<td>10</td>
<td>5</td>
</tr>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved.
Fabric Assurance
How Do We Calculate Fabric Network Health Scores?

Fabric Health score is picked from min of each Category Score

Category Score is number of healthy devices in that category to the total number of devices

Fabric Health has 4 Categories:
• Fabric Edge
• Fabric Border
• Fabric Control Plane
• Fabric Wireless

Fabric Domain Score is the Lowest of all four Category Scores

Example

<table>
<thead>
<tr>
<th>Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Wireless</td>
<td>8</td>
</tr>
<tr>
<td>Fabric Edge</td>
<td>10</td>
</tr>
<tr>
<td>Fabric Border</td>
<td>6</td>
</tr>
<tr>
<td>Fabric Control Plane</td>
<td>10</td>
</tr>
</tbody>
</table>

Fabric Network Health: 6
Why Streaming Telemetry?
Individual Transfer Mechanisms Have Challenges

- syslog
- SNMP
- CLI
  - SNMP Poller
  - syslog collector
  - scripts

Scale Issues
Subject to Change
Unstructured
### Streaming Telemetry

Export enriched, consistent and concise data with context from network devices for a better user and operator experience.

<table>
<thead>
<tr>
<th>Periodic or On-Change</th>
<th>Structured Data</th>
<th>Scalable</th>
<th>Reduced CPU Load</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Clock icon" /></td>
<td><img src="image" alt="Molecule icon" /></td>
<td><img src="image" alt="Graph icon" /></td>
<td><img src="image" alt="Download icon" /></td>
</tr>
</tbody>
</table>
5. Streaming Telemetry

Ability to collect many KPIs from devices as close as possible to real time

With Streaming Telemetry we will support collection of many KPIs as close as possible to real time

Subscription

Publication
- Periodic or on-change
- Structured data
- Priority subscriptions
- Customized to recipient
- XML or JSON encoding
- NETCONF or HTTP/2 transport
- Increased scale
- Reduced CPU and bandwidth consumption
Getting Started Workflow
DNA Assurance - Getting Started Workflow

- DNA Center Install
  - On-Premise Single Node
  - Cloud Tethered for App Updates

- Network Device Discovery
  - CDP IP Address Range

- Network Design & Provision
  - Create Network Hierarchy (Sites)
  - Assign Device to Sites
  - Provision Telemetry Configuration

Ready for DNA Assurance!
Getting Started Workflow – Network Discovery

Discovery

New Discovery

Discovery Name: SFO-Branch

Add Credentials

Username*

Password*

Confirm Password*

Enable Password

Confirm Enable Password

Save as global settings

Settings will be used for this specific Discovery job only

Add Credentials:

CLI
- Cisco

SNMPv2C READ
- snmp

SNMPv2C WRITE
No credentials to display

SNMP V3
No credentials to display

Discovered%s
WiredDNAC
Range 10.30.255.1-10.30.25...

OtherWired
Range 10.11.255.1-10.11.25...
Getting Started Workflow – Network Design
# Getting Started Workflow – Assign Device to Sites

## Device Inventory

<table>
<thead>
<tr>
<th>Device</th>
<th>Address</th>
<th>Site</th>
<th>Serial Number</th>
<th>Uptime</th>
<th>OS Version</th>
<th>OS Image</th>
<th>Sync Status</th>
<th>Last Provision</th>
<th>Provision Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMS-AP3862-34</td>
<td>10.11.19.1</td>
<td>...MS/AMS-Level3</td>
<td>FCW2136NCCJ</td>
<td>15 days, 11:45:00.840</td>
<td>8.5.110.0</td>
<td>Not Available</td>
<td>Managed</td>
<td>-</td>
<td>Not Provisioned</td>
</tr>
<tr>
<td>AMS-ASR1K-NET</td>
<td>10.11.255.2</td>
<td>...MS/AMS-Level3</td>
<td>FOX1817GSM2</td>
<td>45 days, 19:51:29.15</td>
<td>15.5(352)</td>
<td>asr1002x-univ...Tag Golden</td>
<td>Managed</td>
<td>-</td>
<td>Not Provisioned</td>
</tr>
<tr>
<td>AMS-SW3650.test.com</td>
<td>10.11.255.100</td>
<td>...MS/AMS-Level3</td>
<td>FDO1852E264</td>
<td>139 days, 10:16:58.88</td>
<td>03.06.0SE</td>
<td>packages.conf Tag Golden</td>
<td>Managed</td>
<td>-</td>
<td>Not Provisioned</td>
</tr>
<tr>
<td>ASR1K-CORE1</td>
<td>10.0.255.42</td>
<td>...DC/DC-Level1</td>
<td>FOX1521G55N</td>
<td>130 days, 10:09:03.84</td>
<td>15.5(352)</td>
<td>asr1000rp1-ad...Tag Golden</td>
<td>Partial Collection Failure</td>
<td>-</td>
<td>Not Provisioned</td>
</tr>
<tr>
<td>ASR1K-CORE2</td>
<td>10.0.255.52</td>
<td>...DC/DC-Level1</td>
<td>FOX1521G55M</td>
<td>131 days, 10:20:44.51</td>
<td>15.5(352)</td>
<td>asr1000rp1-ad...Tag Golden</td>
<td>Partial Collection Failure</td>
<td>-</td>
<td>Not Provisioned</td>
</tr>
</tbody>
</table>

**Filter**

Select **Assign Device to Site**

**Actions**

- Provision
Getting Started Workflow – Telemetry Configuration

Telemetry Assessment and Configuration

Sites Hierarchy
- Global
  - Canada
  - TO
  - Mexico
  - Netherlands
  - USA

Device Inventory

Telemetry

OS Version | OS Image | Sync Status | Last Provision | Provision Status
---|---|---|---|---
8.5.110.0 | Not Available | Managed | - | Not Provisioned
15.5E052 | wrt1092x-univ-Tag Goldfin | Managed | - | Not Provisioned
03.66.06E | packages.conf Tag Goldfin | Managed | - | Not Provisioned
14.5E052 | wrt10900p1-ad... Tag Goldfin | Partial Collection Failure | - | Not Provisioned
15.5E052 | wrt10900p1-ad... Tag Goldfin | Partial Collection Failure | - | Not Provisioned
Getting Started Workflow

Overall Health

Overall Health Summary

NETWORk
89%
Healthy Devices

View Network Health

NETWORK DEVICES
Core 100% Healthy Devices
Access 100% Healthy Devices
Distribution 100% Healthy Devices
Router 89% Healthy Devices
Wireless 37% Healthy Devices

CLiENT
86%
Healthy Clients

View Client Health

CLIENTS
Wireless 62% Healthy Clients
Wired 100% Healthy Clients

Ready for DNA Assurance!
End-to-end visibility – Overall Health

**Overall Health Summary**

<table>
<thead>
<tr>
<th>NETWORK</th>
<th>CLIENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>40%</td>
<td>55%</td>
</tr>
</tbody>
</table>

- **Top 10 Issues (3)**
  - Dec 06, 2017 12:00:00 to Dec 07, 2017 12:00:00
  - Onboarding
  - Clients Failing DHCP Attempts Because DHCP IP Addressing Tims Out at "Global/USA/SM-SM-Level1"
  - Total occurrences: 42

**Site/Building/Floor**

- **Network Health (% Healthy Devices)**
  - All Sites: 52%
  - Wireless: 52%
  - Client: 52%
  - Issues #: 52
  - Clients #: 5,232
  - Network Devices #: 5,232
  - Bandwidth Usage: 65%

- **San Jose**
  - 27%: Core
  - 24%: Wired
  - 72%: Wireless
  - 25
  - 2,777
  - 777
  - 75%

- **Building**
  - 13%
  - Distribution
  - 13%
  - Wired
  - 12
  - 162
  - 162
  - 62%

- **Building**
  - 28%
  - Access
  - 29%
  - Wireless
  - 5
  - 459
  - 459
  - 57%

- **Building**
  - 36%
  - Access
  - 36%
  - Wireless
  - 4
  - 622
  - 622
  - 42%

- **Building**
  - 42%
  - Access
  - 42%
  - Wireless
  - 8
  - 320
  - 320
  - 63%

**Quick drill down to a site or Toggle between Geo, List or Topology View**

**Where in the world and on which site most serious issues are happening**

**Overall health summary of network and clients**

**Top 10 Global Insights**
End-to-end visibility – Network/Client Health

- Client Health Summary
- Onboarding, RF and Client Profile info

- Network Health Summary
- Control, Data, Policy Plane and Health info
End-to-end visibility – 360 views of users & devices

- Single location for all user information and every user device
- History of performance for each user device
- Proactive identification of any issues affecting user’s experience

- Single location for all user device related user information
  - Connectivity graph with health score of all device on the path
  - Application performance
  - Device KPIs
Network Time Travel – Go back in time to understand the network state when issue occurred

- History shows critical events
- Identifies when issues occurred!

- Rewind time to when the issue occurred
- All the information on the user or network device 360 changes to the selected time!
Path Trace – Troubleshoot issues along the network path

- Run `pathtrace` from source to destination to quickly get key performance statistics for each device along the network path.
- Identify ACLs that may be blocking or affecting the traffic flow.

Client 360

Issues (1)
Connected
This client is exhibiting sticky behavior on "LA-Corporate3" and "LA-AP1615-32" 2.4 GHz.
Test occurrences: 1

Onboarding
12:00:17 12:00:20 UT

Path Trace
To find the location of an issue, perform a path trace between two nodes in your network – a source and a destination.

More Details

GigabitEthernet1/0/24

Ingress details
- GigabitEthernet1/0/24
- Used VLAN: N/A
- Admin status: N/A
- Input Queue Drops: N/A
- Input Queue Count: N/A
- Input Rate: N/A
- Output Drop: N/A
- Output Queue Count: N/A
- Output Rate: N/A
- Input Queue Max Depth: N/A
- Matched ACE Result: N/A

ACL Name: standard_acl_r1_ac2_4
ACL Result: DENY
Matching ACE Rule: 10 deny 221.3.25.14
Matching ACE Result: DENY
Insights with Guided Remediation Actions

Clients Failing DHCP Attempts Because DHCP IP Addressing Timed Out at "Global/USA/SM/SM-Level1".

- Guided Actions to help remediate issues quickly
- Detailed drill downs to identify the impact quickly

Description
Clients located in "Global/USA/SM/SM-Level1" timed out and have not been assigned an IP address from the DHCP server.

Impact
- Location: 1 building
- Clients: 4 Wireless Clients

Suggested Actions (6)
1. Verify that the DHCP scope is configured correctly. Best Practice - Design an IP address pool that is two to three times larger than the expected number of users.
2. Reduce the DHCP lease time. Best practice - DHCP lease time for high-density, high mobile environment is 10-30 min.
Proactive Insights - Sensors

Create sensor test schedule and define the applications and test to run

- Sensor tests raise issues/insights
- Detailed results shown at the floor level
Platform
DNAC 1.1 Platform:
Scale and Hardware specification

**Scale:** Single Node

- Centralized deployment, cloud tethered
- 1 RU Small form factor
- 2 x 10Gbps Data links
- Built in Network Telemetry collection (FNF, SNMP, Syslog)
- Built in Contextual connectors (ISE/PxGrid, IPAM, Location)
- HA (3 Node, Automation), RBAC, Backup/Restore, Scheduler, APIs
- 64-bit x86 Processors
- Solid State Disks in RAID10
- Hardware MRAID Controller
- Dual PSU

**Single Appliance for DNAC (Automation + Assurance)**

- 5,000 -> 4K Aps + 1K Network Devices
- 25,000 -> Clients/Hosts
## DNA Assurance Platform Support (Release 1.1)

### CAT2K / CAT3K / CAT4K Switches

<table>
<thead>
<tr>
<th>CAT2K</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2960-L</td>
<td>IOS 15.2(2)E7</td>
<td>IOS 15.2(1)E</td>
</tr>
<tr>
<td>C2960-P</td>
<td>IOS 15.2(2)E7</td>
<td>IOS 15.2(1)E</td>
</tr>
<tr>
<td>C2960-C</td>
<td>IOS 15.2(2)E8</td>
<td>IOS 15.2(1)E</td>
</tr>
<tr>
<td>C2960-CPD</td>
<td>IOS 15.2(2)E7</td>
<td>IOS 15.2(1)E</td>
</tr>
<tr>
<td>C2960-X Stack</td>
<td>IOS 15.2(2)E6</td>
<td>IOS ≥ 12.1</td>
</tr>
<tr>
<td>C2960-XR</td>
<td>IOS 15.2(2)E6</td>
<td>IOS ≥ 12.1</td>
</tr>
<tr>
<td>C2960-XR Stack</td>
<td>IOS 15.2(2)E6</td>
<td>IOS ≥ 12.1</td>
</tr>
<tr>
<td>C2960-CX</td>
<td>IOS 15.2(4)E3</td>
<td>IOS 2 or 12.1</td>
</tr>
</tbody>
</table>

### CAT3K

<table>
<thead>
<tr>
<th>CAT3K</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3650-CX</td>
<td>IOS 15.2(0)E</td>
<td>All Versions</td>
</tr>
<tr>
<td>C3650 (Copper)</td>
<td>IOS-XE 16.6.1</td>
<td>All Versions</td>
</tr>
<tr>
<td>C3650-Stack</td>
<td>IOS-XE 16.6.1</td>
<td>All Versions</td>
</tr>
<tr>
<td>C3650/Copper(Fiber)</td>
<td>IOS-XE 16.6.1</td>
<td>All Versions</td>
</tr>
<tr>
<td>C3850-Stack (Copper/Fiber)</td>
<td>IOS-XE 16.6.1</td>
<td>All Versions</td>
</tr>
</tbody>
</table>

### CAT4K

<table>
<thead>
<tr>
<th>CAT4K</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C4500-X</td>
<td>IOS-XE 3.10E</td>
<td>All Versions</td>
</tr>
<tr>
<td>C4500-E (SUP 7E)</td>
<td>IOS-XE 3.10E</td>
<td>All Versions</td>
</tr>
<tr>
<td>C4500R+E (SUP 7E)</td>
<td>IOS-XE 3.10E</td>
<td>All Versions</td>
</tr>
<tr>
<td>C4500E</td>
<td>IOS-XE 3.10E</td>
<td>All Versions</td>
</tr>
<tr>
<td>C4507R+E (SUP 8E)</td>
<td>IOS-XE 3.10E</td>
<td>All Versions</td>
</tr>
<tr>
<td>C4510R+E (Sup 8E)</td>
<td>IOS-XE 3.10E</td>
<td>All Versions</td>
</tr>
</tbody>
</table>

### Cisco Meraki Devices

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Cisco Meraki Devices</td>
<td>All Versions</td>
<td>All Versions</td>
</tr>
</tbody>
</table>

### CAT9K / CAT6K / N7K Switches

<table>
<thead>
<tr>
<th>CAT9K</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C9300</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9300 Stack</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9400-LC-48UX</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9400-LC-24XS</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9400 (Sup1XL)</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9400 (Sup1LE)</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9500</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
<tr>
<td>C9500 Stack</td>
<td>IOS-XE 16.6.2</td>
<td>IOS-XE 16.6.1</td>
</tr>
</tbody>
</table>

### CAT6K

<table>
<thead>
<tr>
<th>CAT6K</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>C6400E (Sup 2T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6504E (Sup 2T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6506E (Sup 2T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6509E (Sup 2T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6513E (Sup 2T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6807-X (Sup 2T/6T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6840-X (Sup 2T/6T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
<tr>
<td>C6880-X (Sup 2T/6T)</td>
<td>IOS 15.5.1</td>
<td>≥ 12.2</td>
</tr>
</tbody>
</table>

### Wireless Controllers / APs

<table>
<thead>
<tr>
<th>Wireless</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>WLC (53xx, 55xx, 85xx)</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
<tr>
<td>AP 1700</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
<tr>
<td>AP 1800</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
<tr>
<td>AP 2700</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
<tr>
<td>AP 2800</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
<tr>
<td>AP 3700</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
<tr>
<td>AP 3800</td>
<td>AireOS 8.5 MR1</td>
<td>AireOS 8.5 MR1</td>
</tr>
</tbody>
</table>

### ASR / ISR / CSRv Routers

<table>
<thead>
<tr>
<th>ASR / ISR / CSRv Routers</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISR 4K</td>
<td>IOS-XE 3.16</td>
<td>IOS-XE 3.9</td>
</tr>
<tr>
<td>ISR 4221</td>
<td>IOS-XE 16.4</td>
<td>IOS-XE 16.4</td>
</tr>
<tr>
<td>ISR 4351</td>
<td>IOS-XE 3.16</td>
<td>IOS-XE 3.30</td>
</tr>
<tr>
<td>ISR 4451-X</td>
<td>IOS-XE 3.16</td>
<td>IOS-XE 3.9</td>
</tr>
<tr>
<td>ISR 1K (Selected PIDs Only)</td>
<td>Recommend ed OS</td>
<td>Minimum OS</td>
</tr>
<tr>
<td>ASR 1001-X</td>
<td>IOS-XE 18.3.5</td>
<td>IOS-XE 3.12.0</td>
</tr>
<tr>
<td>ASR 1002-X</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.7.0</td>
</tr>
<tr>
<td>ASR 1006-X (RP2)</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.16.0</td>
</tr>
<tr>
<td>ASR 1006-X (RP3)</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.16.0</td>
</tr>
<tr>
<td>ASR 1009-X (RP2)</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.16.0</td>
</tr>
<tr>
<td>ASR 1009-X (RP3)</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.16.0</td>
</tr>
<tr>
<td>ASR 1001-HX</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.16.3</td>
</tr>
<tr>
<td>ASR 1002-HX</td>
<td>IOS-XE 16.3.5</td>
<td>IOS-XE 3.16.3</td>
</tr>
</tbody>
</table>

### UCS on ISR43xx

<table>
<thead>
<tr>
<th>UCS on ISR43xx</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>UCS 840</td>
<td>UCS 840</td>
<td>UCS 840</td>
</tr>
<tr>
<td>UCS 820</td>
<td>UCS 820</td>
<td>UCS 820</td>
</tr>
<tr>
<td>UCS 220</td>
<td>UCS 220</td>
<td>UCS 220</td>
</tr>
</tbody>
</table>

### Virtual Router

<table>
<thead>
<tr>
<th>Virtual Router</th>
<th>Recommended OS</th>
<th>Minimum OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSRv</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>ISRv</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>ASA v</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>vWAAS</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>ENCS 5400</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>ENCS 5100</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>UCS-C220</td>
<td>WIP</td>
<td>WIP</td>
</tr>
<tr>
<td>UCSE on ISR43xx</td>
<td>WIP</td>
<td>WIP</td>
</tr>
</tbody>
</table>

© 2018 Cisco and/or its affiliates. All rights reserved. Cisco Public
DNAC 1.1 Data Retention

- Data storage for 5000 devices, 25,000 clients
- Customizable retention policy
- Storage monitoring and alerting
- Provide meaningful assurance troubleshooting, issues and trending dashboard data

- KPIs, Metrics: 14 days
- Relationship Graph: 14 days
- Events/Alarms: 14 days
- Issues: 14 days

Backup (To external storage)

Purge
## DNA Assurance Scalability (DNA Center v1.1)

<table>
<thead>
<tr>
<th>Capacity</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>25K</td>
<td>Clients / Endpoints</td>
</tr>
<tr>
<td>4K</td>
<td>Access Points</td>
</tr>
<tr>
<td>1000</td>
<td>Switches/Routers/WLC</td>
</tr>
<tr>
<td>20</td>
<td>Sites</td>
</tr>
</tbody>
</table>
Conclusion
## Old Approach

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reactive: Traditional monitoring based on network element KPFs</td>
</tr>
<tr>
<td>Network Unaware</td>
</tr>
<tr>
<td>Closed Interfaces &amp; Developer Inefficiencies</td>
</tr>
<tr>
<td>Use case specific monolithic architecture</td>
</tr>
<tr>
<td>Rigid Network Telemetry</td>
</tr>
</tbody>
</table>

## DNA Approach

<table>
<thead>
<tr>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proactive: True Assurance based on deeper correlation across all entities</td>
</tr>
<tr>
<td>Network and Context Aware - deeper insights through Analytics</td>
</tr>
<tr>
<td>Open interfaces with adaptive APIs and ITSM Integration framework</td>
</tr>
<tr>
<td>Hyper-distributed multi-tenant &amp; cloud first secure architecture</td>
</tr>
<tr>
<td>Micro services based agile modern network telemetry collection capabilities</td>
</tr>
</tbody>
</table>

The Network that Scales for the Digital Business
SD-Access Support
Fabric ready platforms for your digital ready network

Switching
- Catalyst 9400
- Catalyst 9500
- Catalyst 4500E
- Catalyst 6800
- Catalyst 3650 and 3850
- Nexus 7700

Routing
- ASR-1000-X
- ASR-1000-HX
- ISR 4430
- ISR 4450
- ISRv/CSRv

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

Extended
- CDB
- 3560-CX
- IE (2K/3K/4K/5K)

* with Caveats
What to Do Next?

- Get SD-Access Capable Devices with DNA Advantage OS License
- Get DNA Center Appliances with DNA Center Software
- Cisco Services can help you to Test - Migrate - Deploy

Refresh your Hardware & Software
 Deploy the DNA Center
 Engage with Cisco Services
SD-Access - Cisco on Cisco
Live SD-Access Deployment @ Cisco Systems

750 Wired & Wireless users

2 Fabric Border Control-Plane Nodes
7 Fabric Edge Nodes
98 Fabric Access Points
3 Virtual Networks
16 Scalable Groups
2 Wireless SSIDs
8 Address Pools

Built and managed by the Cisco Engineering team, in conjunction with Cisco IT Services
Questions?
Use Cisco Spark to communicate with the speaker after the session

How
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install Spark or go directly to the space
4. Enter messages/questions in the space

cs.co/ciscolivebot#BRKCRS-2814
• Please complete your Online Session Evaluations after each session

• Complete 4 Session Evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt

• All surveys can be completed via the Cisco Live Mobile App or the Communication Stations

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at www.ciscolive.com/global/on-demand-library/.
Continue Your Education

• Demos in the Cisco campus
• Walk-in Self-Paced Labs
• Tech Circle
• Meet the Engineer 1:1 meetings
• Related sessions
Thank you